

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE
BEOGRAD

MASTER STUDIJE

STUDIJSKI PROGRAM:
SAVREMENE INFORMACIONE TEHNOLOGIJE

MASTER RAD

KRIPTOGRAFSKI ASPEKTI ZAŠTITE OPTIČKIH TELEKOMUNIKACIONIH MREŽA

MENTOR:
Prof. dr Mladen Veinović

STUDENT:
Lazar Aščerić
Br. indeksa: 410060/2010

BEOGRAD, 2011

Zahvaljujem se:

- Svojoj porodici, čija su brojna odricanja uložena u ovaj rad,
- Mentoru prof. dr. Mladenu Veinoviću, na iscrpnom vođenju i konsultacijama u toku pisanja rada,
- Ministarstvu odbrane RS, na finansijskoj podršci za vreme školovanja.

Lazar Ašćerić

SAŽETAK

Optičke telekomunikacione mreže, zbog sve većih zahteva za informacionim kapacitetom, danas su u velikoj meri poprimile širokopojasni karakter, kako u svom transportnom tako i u pristupnom delu. Ogromna većina telekomunikacionog saobraćaja u transportnim mrežama realizuje se preko optičkih vlakana, a dominantni standardi su SDH/SONET i Carrier Ethernet paketski prenos. Podrška na optičkom nivou obezbeđena je primenom WDM tehnologije multipleksiranja. WDM sistemi se pod određenim uslovima mogu koristiti i za direktan prenos IP-a, što vodi ka razvoju savremenih potpuno optičkih mreža. Zbog visokih bitskih brzina kao i brojnih pretnji i napada na ove mreže, bez obzira na primenjene tehnologije, razvoj i implementacija sistema zaštite podataka u njima zahteva posebnu pažnju.

U radu je prikazana analiza problema bezbednosti i zaštita podataka u optičkim telekomunikacionim mrežama sa akcentom na kriptografska rešenja bazirana na simetričnim kriptografskim sistemima. Analizirane su moguće pretnje i oblici ugrožavanja optičkih mreža. Navedeni su neki simetrični i asimetrični kriptografski algoritmi koji se mogu primeniti pri zaštiti, a kao poseban problem analizirano je upravljanje ključevima. Izneta su neka dostupna komercijalna rešenja za zaštitu, analizirana je njihova pouzdanost, izvršeno poređenje stranih i domaćih rešenja i predložen mogući načini implementacije u konkretan telekomunikacioni sistem.

Ključne reči: bezbednost, zaštita, kriptografija, algoritam, ključ, mreža.

ABSTRACT

Optical telecommunication networks, due to increasing demands for information capacity, are now largely assumed the character of broadband, both in its transport and in the access part. The vast majority of telecommunications traffic in transportation networks is realized through optical fibers, and the dominant standards are SDH/SONET and Carrier Ethernet packet. Support on the optical level is provided using WDM multiplexing technology. WDM systems, under certain conditions may be used for direct transmission of IP, which leads to the development of modern fully optical networks. Due to the high bit rates as well as numerous threats and attacks on the network, regardless of the applied technology, development and implementation of data protection in them require special attention.

This paper presents the analysis of problems of security and data protection in the optical telecommunications networks with a focus on cryptographic solutions based on symmetric cryptographic systems. We analyzed the possible forms of threats and attacks of optical networks. Some symmetric and asymmetric cryptographic algorithms which can be applied for protection are presented by this paper, and key management has been analyzed as a particular problem. This paper expressed some available commercial solutions for protection, analyzed their reliability, made comparison of foreign and domestic solutions and suggested possible ways of implementing the specific telecommunication system.

Keywords: security, protection, cryptography, algorithms, key, network.

SPISAK SLIKA I TABELA

Slika 1. Način vremenskog multipleks. prema evropskoj, američkoj i japanskoj hijerarhiji - 11 -

Slika 2. Struktura STM-1 signala ..... - 13 -

Slika 3. Osnovna struktura multipleksiranja za SDH standard ..... - 14 -

Slika 4. Označavanje faznog pomeraja VC-4 rama u odnosu na STM-1 ram ..... - 16 -

Slika 5. Vrste i funkcije pointera u ETSI strukturi multipleksiranja ..... - 18 -

Slika 6. Vrste SDH multipleksera i njihove funkcionalnosti ..... - 20 -

Slika 7. Delovi Ethernet frejma ..... - 22 -

Slika 8. Evolucaja Etherneta iz LAN-a u Metro i transportnu mrežu ..... - 25 -

Slika 9. Slabljenje u optičkom vlaknu i optički prozori ..... - 29 -

Slika 10. Princip funkcionisanja xWDM sistema ..... - 31 -

Slika 11. Model kriptografskog sistema ..... - 37 -

Slika 12. Tipovi zaštite komunikacija ..... - 43 -

Slika 13. Algoritam DES ..... - 46 -

Slika 14. Operacije u jednoj rundi DES ..... - 47 -

Slika 15. Runda AES-a ..... - 50 -

Slika 16. Princip asimetričnog šifrovanja ..... - 52 -

Slika 17. Faze kriptološkog ključa ..... - 55 -

Slika 18. Razmena ključeva korišćenjem KDC ..... - 58 -

Slika 19. Protokol Needham-Schroeder ..... - 60 -

Slika 20 Otička telekomunikaciona mreža državnih organa ..... - 62 -

Slika 21 Implementacija kripto uređaja u optičku telekomunikacionu mrežu ..... - 69 -

Slika 22. SMC 1100 ..... - 72 -

Slika 23. Specijalni uređaji Čajavec a.d. ..... - 74 -

Tabela 1. Binarni protoci u SDH standardu ..... - 12 -

Tabela 2. Podređeni i nadređeni ramovi u ETSI strukturi multipleksiranja ..... - 17 -

Tabela 3. Zahtevi za kašnjenje, džiter, raspoloživost i tačnost sinhronizacije u Carrier Ethernet, SDH i mreži mobilne telefonije ..... - 27 -

Tabela 4. Bitske brzina u mreži ..... - 62 -

Tabela 5. HC-84xx i HC-85xx uređaji Crypto AG ..... - 71 -

SADRŽAJ

1. UVOD ..... - 6 -

1.1 UVODNE NAPOMENE I KONTEKST ISTRAŽIVANJA ..... - 6 -
1.2 METODOLOGIJA ISTRAŽIVAČKOG PROJEKTA ..... - 7 -
1.2.1 PREDMET ISTRAŽIVANJA ..... - 7 -
1.2.2 CILJEVI I ZADACI ISTRAŽIVANJA ..... - 7 -
1.2.3 ISTRAŽIVAČKE HIPOTEZE ..... - 8 -
1.2.4 METODE ISTRAŽIVANJA I TOK ISTRAŽIVAČKOG PROCESA ..... - 8 -

2. PREGLED TEHNOLOGIJA U OPTIČKIM TELEKOMUNIKACIJAMA ..... - 10 -

2.1 SDH/SONET ..... - 10 -
2.1.1 RAZLOZI ZA UVOĐENJE SDH ..... - 10 -
2.1.1.1 Načini vremenskog multipleksiranja ..... - 10 -
2.1.1.2 Ograničenja PDH tehnike ..... - 11 -
2.1.2 BINARNI PROTOCI U SDH ..... - 12 -
2.1.3 OSNOVNA STRUKTURA STM-1 ..... - 13 -
2.1.4 STRUKTURA MULTIPLEKSIRANJA ..... - 14 -
2.1.4.1 Mapiranje u virtuelni kontejner ..... - 14 -
2.1.4.2 Uloga pointera i fazno izravnanje ..... - 15 -
2.1.5 ŠTA JE MOGUĆE MAPIRATI U SDH ..... - 18 -
2.1.5.1 PDH pritoke ..... - 18 -
2.1.5.2 ATM ćelije ..... - 19 -
2.1.5.3 Ethernet over SDH ..... - 19 -
2.1.6 ELEMENTI SDH MREŽE ..... - 20 -
2.2 CARRIER ETHERNET ..... - 21 -
2.2.1 STRUKTURA ETHERNET RAMA I TIPOVI ETHERNETA ..... - 22 -
2.2.1.1 Struktura Ethernet rama ..... - 22 -
2.2.1.2 Tipovi Etherneta ..... - 23 -
2.2.2 PRIMENA ETHERNETA U TRANSPORTNIM MREŽAMA ..... - 24 -
2.2.2.1 Evolucija ka Carrier Ethernetu ..... - 24 -
2.2.2.2 Poređenje sa SDH ..... - 25 -
2.3 OPTIČKE MREŽE SA xWDM MULTIPLEKSIRANJEM ..... - 28 -
2.3.1 PROSTIRANJE SIGNALA KROZ OPTIČKO VLAKNO ..... - 28 -
2.3.1.1 Optičko vlakno kao svetlovod ..... - 28 -
2.3.1.2 Hromatska i polarizaciona disperzija i nelinearnost ..... - 30 -
2.3.2 STRUKTURA xWDM SISTEMA ..... - 30 -
2.3.2.1 Optički predajnici i prijemnici ..... - 31 -
2.3.2.2 Optički pojačavači ..... - 32 -
2.3.2.3 Optičko multipleksiranje i demultipleksiranje ..... - 33 -
2.3.2.4 Optički add/drop multiplekseri (OADM) ..... - 34 -
2.3.2.5 Optički kroskonektori (OXC) ..... - 34 -
2.3.3 VRSTE WDM ..... - 34 -
2.3.3.1 Coarse WDM ..... - 35 -
2.3.3.2 Dense WDM ..... - 35 -

3. KRIPTOGRAFSKI SISTEMI ..... - 37 -

3.1 KRIPTOGRAFIJA U SAVREMENIM TELEKOMUNIKACIJAMA ..... - 37 -
3.1.1 OSNOVNI TERMINI ..... - 37 -
3.1.1.1 Šifrovanje i dešifrovanje ..... - 37 -
3.1.1.2 Kritptografski algoritmi i ključevi ..... - 38 -

3.1.2 ISTORIJAT I NAMENA KRIPTOGRAFIJE - 39 -
3.1.3 ANALIZA PRETNJI I NAPADA - 40 -
3.2 KRIPTOGRAFSKI ALGORITMI - 42 -
3.2.1 TIPOVI ZAŠTIĆENIH KOMUNIKACIJA - 43 -
3.2.1.1 Link encryption - 43 -
3.2.1.2 End to end encryption - 44 -
3.2.2 SIMETRIČNI KRIPTOGRAFSKI ALGORITMI - 44 -
3.2.2.1 Principi simetrične kriptografije - 44 -
3.2.2.2 DES - 46 -
3.2.2.3 Triple DES - 48 -
3.2.2.4 AES - 48 -
3.2.2.5 Ostali simetrični algoritmi - 50 -
3.2.2.6 Režimi rada simetričnih algoritama - 51 -
3.2.3 ASIMETRIČNI KRIPTOGRAFSKI ALGORITMI - 51 -
3.2.3.1 Javni i tajni ključ - 51 -
3.2.3.2 RSA - 52 -
3.2.4 HIBRIDNI SISTEMI - 53 -
3.3 UPRAVLJANJE KRIPTOGRAFSKIM KLJUČEVIMA - 54 -
3.3.1 FAZE KRIPTOLOŠKIH KLJUČEVA - 54 -
3.3.1.1 Generisanje ključeva - 55 -
3.3.1.2 Distribucija ključeva - 56 -
3.3.1.3 Zamena i uništenje ključeva - 57 -
3.3.2 PROTOKOLI ZA RAZMENU KLJUČEVA - 57 -
3.3.2.1 KDC - 57 -
3.3.2.2 DiffieHellman-ova eksponencijalna razmena ključeva - 58 -
3.3.2.3 Needham-Schroeder protokol - 59 -

4. IMPLEMENTACIJA KRIPTOGRAFSKOG SISTEMA U OPTIČKU TELEKOMUNIKACIONU MREŽU - 61 -

4.1 ANALIZA KOMUNIKACIONIH KARAKTERISTIKA - 61 -
4.1.1 MODEL MREŽE - 61 -
4.1.2 BITSKE BRZINE - 62 -
4.1.3 OSTALE KARAKTERISTIKE - 63 -
4.2 ZAHTEVI ZA KRIPTO UREĐAJIMA - 63 -
4.3 PROJEKTOVANJE SISTEMA ZAŠTITE - 64 -
4.3.1 ANALIZA SISTEMA ZAŠTITE - 65 -
4.3.2 OBLIKOVANJE SISTEMA ZAŠTITE - 66 -
4.3.3 IMPLEMENTACIJA SISTEMA ZAŠTITE - 68 -
4.4 PREGLED DOSTUPNIH REŠENJA NA TRŽIŠTU - 69 -
4.4.1 CRYPTO AG - 70 -
4.4.1.1 Karakteristike uređaja - 71 -
4.4.1.2 Security management - 72 -
4.4.2 MOGUĆA DOMAĆA REŠENJA - 73 -
4.4.3 OSTALA PRIMENLJIVA REŠENJA - 74 -

5. ZAKLJUČAK - 76 -

LITERATURA - 78 -

1. UVOD

Današnja dešavanja na opštoj geopolitičkoj sceni kao i istorijski događaji u našem okruženju stvaraju potrebu za dubljim razmatranjem pojmova suvereniteta i nacionalne bezbednosti. Ovo izuzetno široko i važno pitanje, pored niza drugih elemenata, mora uzeti u obzir bezbednost informacija koje se koriste pri donošenju odluka bitnih za funkcionisanje sistema odbrane, sektora bezbednosti i diplomatije. Profesionalni sistemi kao što su vojska, policija i bezbednosne službe ne bi smele da se oslone na potpuno spoljna bezbednosna rešenja već je neminovno usmeravanje sredstava i resursa na interni razvoj kako bi se postigla kontrola nad svim parametrima koji čine sistem zaštite. Razvoj sistema zaštite, takođe predstavlja široko i važno pitanje čiji je segment u optičkim telekomunikacijama iznet u ovom radu.

1.1 UVODNE NAPOMENE I KONTEKST ISTRAŽIVANJA

Optički sistemi prenosa danas zauzimaju centralno mesto u telekomunikacionim sistemima. Oko četiri petine ukupnog telekomunikacionog saobraćaja u transportnim mrežama obavlja se preko optičkih spojnih puteva [15]. Razlog za to krije se u velikoj propusnoj moći optičkih vlakana. Ttrenutno razvijene WDM tehnike multipleksiranja optičkih signala po talasnim dužinama omogućavaju da se po jednom optičkom vlaknu istovremeno prenese od nekoliko desetina do čak nekoliko stotina kanala, svaki od njih na različitoj talasnoj dužini. Primenom standardnih STM-64 SDH ili 10 Gb Ethernet signala, omogućavaju se brzine prenosa koje prevazilaze red veličina 1Tbit/s. Ovakav prenos se, uz adekvatno postavljene regeneratorske stanice, može realizovati na udaljenostima i do nekoliko hiljada kilometara.

U pogledu kapaciteta, svaku telekomunikacionu mrežu možemo podeliti na njen transportni deo, kroz koji se ostvaruje veliki bitski protok i prenos informacija na velika rastojanja (*long-haul* mreža), koja kao svoj niži nivo obuhvata široko-oblasnu (WAN) i regionalnu (MAN) mrežu, i pristupni deo, kroz koji se ostvaruje protok nižeg intenziteta na relativno kratkim rastojanjima i do krajnjih korisnika. Pored toga što su neprikosnovene u transprtnom delu sistema, optičke mreže sve više preuzimaju i ulogu pristupnih. Tome je uveliko doprineo razvoj Etherneta i mogućnosti njegovog prilagođenja za prenos po optičkom vlaknu na veće udaljenosti, a ne samo u okviru lokalnih mreža (LAN).

Imajući u vidu da podaci koji se prenose putem optičkih mreža danas mogu imati izuzetno veliku vrednost, u svim profesionalnim sistemima, donošenje odluka i uspeh u poslovanju uveliko zavise od sposobnosti sistema da osigura bezbednost tih podataka. S obzirom na obim korišćenja optičkih telekomunikacionih mreža kao baza informacionim sistemima na prenosnom putu, neophodno je razmatrati zaštitu podataka na tom nivou.

Optičke širokopojasne mreže, kao jezgra računarskih mreža, predstavljaju krajnje nebezbednu sredinu u pogledu prenosa podataka. One su, u prvom redu, projektovane da savladaju velike udaljenosti i obezbede dovoljan protok, dok su bezbednosni moduli retkost u njihovoj arhitekturi. Iz tog razloga većina korisnika pribegava modelu zaštite podataka na višim slojevima. Međutim, pojedini profesionalni sistemi, kao što su državni organi (vojska, policija, dipomatija, bezbednosne agencije i sl.), zahtevaju sveobuhvatniji sistem zaštite koji se, i pored bezbednosnih rešenja na višim slojevima, ne bi smeo realizovati bez kriptografije na prvom i drugom sloju OSI modela. U ovom radu biće razmatran taj problem i izneto jedno od mogućih rešenja koje podrazumeva korišćenje gotovih proizvoda uz opciono dodavanje sopstvenih parametara, kao i sopstveni način organizacije i funkcionisanja sistema zaštite.

Kriptografska zaštita telekomunikacionog sistema uopšte, mogla bi se definisati kao sprečavanje neovlašćene strane ili napadača da dođe do tajnih informacija, koje se posredstvom tog sistema prenose, u jasnoj formi. Tehnike i algoritmi kojima se to postiže su raznovrsni i biće detaljno opisani u ovom radu.

1.2 METODOLOGIJA ISTRAŽIVAČKOG PROJEKTA

1.2.1 PREDMET ISTRAŽIVANJA

U ovom radu predmet istraživanja je kriptografska zaštita podataka u optičkim telekomunikacionim mrežama i način implementacije kriptografskih sistema u optičke mreže pri posebnim uslovima eksploatacije sa posebnim osvrtom na gotova domaća i strana kriptografska rešenja. Činjenica da se optički prenos podataka masovno koristi u pristupnim i transportnim telekomunikacionim mrežama i potrebe profesionalnih sistema za kriptografskim rešenjima visokih bezbednosnih karakteristika, čini ovu oblast izuzetno širokom za istraživanja. Ovaj rad je pokušaj da se doprinese potpunijem shvatanju značaja kriptografske zaštite podataka na spojnom putu.

1.2.2 CILJEVI I ZADACI ISTRAŽIVANJA

Naučni cilj rada je sistematizacija znanja o optičkim telekomunikacionim mrežama i kriptografskim sistemima, utvrđivanje problema pri implementaciji pojedinih kriptografskih rešenja u telekomunikacioni sistem i načina njihovog prevazilaženja te ukazivanje na prednosti i nedostatke primenjenih rešenja i mogućnost odabira konkretnog rešenja na bazi izvršenih analiza.

Društveni cilj rada je udovoljavanje bezbednosnim potrebama korisnika telekomunikacionih mreža u profesionalnim sistemima, ukazivanje na ugrožavanje bezbednosti telekomunikacionih servisa koje optičke mreže pružaju i skretanje pažnje državnim institucijama nadležnim za zaštitu informacija na neminovnost ulaganja u razvoj sopstvenih kriptografskih rešenja.

Zadaci rada su definisanje postupaka i metoda iznalaženja najcelishodnijeg rešenja za kriptografsku zaštitu podataka u optičkim telekomunikacionim mrežama, uzimajući pri tome u obzir sve bitne karakteristike mreže i kriptografske parametre, a posebno topologiju mreže, brzinu prenosa, kriptografski algoritam, kriptografske ključeve i menadžment ključeva.

1.2.3 ISTRAŽIVAČKE HIPOTEZE

Opšta hipoteza:

Bezbednost podataka pri prenosu kroz telekomunikacionu mrežu u profesionalnim sistemima je jedan od ključnih elemenata za uspešno poslovanje i donošenje odluka, pogotovo ako se radi o podacima značajnim za funkcionisanje državnih organa. Sistem zaštite podataka na prenosnom putu baziran na kriptografskim rešenjima predstavlja najvažniji segment te bezbednosti.

Posebne hipoteze:

Savremene telekomunikacione mreže moraju imati veliki informacioni kapacitet kako bi obezbedile brz prenos podataka za sve zahtevnije servise. Optičko multipleksiranje talasnih dužina (xWDM) predstavalja najefikasniji način za dostizanje željenog kapaciteta.

Visoke bitske brzine koje egzistiraju u optičkim mrežama predstavljaju ogroman izazov za projektovanje i implementaciju sistema zaštite.

Prilikom projektovanja sistema zaštite od izuzetnog je značaja ostvarivanje što većeg nivoa kontrole nad kriptološkim parametrima koji čine sistem zaštite. Razvoj sopstvenih rešenja zahteva ogromno vreme i sredstva, a primena komercijalnih rešenja ne omogućava dovoljnu kontrolu nad tim parametrima.

1.2.4 METODE ISTRAŽIVANJA I TOK ISTRAŽIVAČKOG PROCESA

Kako bi se zadovoljila objektivnost, opštost i sistematičnost, a imajući u vidu specifičnost istraživanja, u radu su primenjene sledeće metode:

- Metoda deskripcije,
- Komparativna metoda,
- Metoda analize,
- Metoda sinteze,
- Metoda modelovanja.

Metoda deskripcije je postupak opisivanja činjenica, procesa i predmeta te njihovih empirijskih potvrđivanja odnosa i veza.

Komparativna metoda podrazumeva upoređivanje sličnih ili srodnih činjenica, pojava, procesa i odnosa, odnosno urvrđivanje njihove sličnosti u ponašanju i intenzitetu kao i razlika među njima.

Metoda analize je postupak naučnog istraživanja i objašnjavanja stvarnosti putem rasčlanjivanja složenih misaonih tvorevina na njihove jednostavne delove i elemente, kao i izračunavanje svakog dela za sebe i u odnosu na druge delove.

Metoda sinteze je suprotna od metode analize i podrazumeva spajanje jednostavnijih lako proverljivih misaonih tvorevina u složenije.

Modelovanje u ovom radu ima za cilj da se putem aproksimacije zamišljenog sistema lakše razumeju i objasne njegovi kompleksni delovi i prikaže predloženo rešenje problema.

Nakon metodoloških smernica, datih u uvodnom delu, drugi deo rada posvećen je telekomunikacionim tehnologijama (SDH/SONET, Carrier Ethernet i xWDM) na kojima se zasnivaju savremeni telekomunikacioni servisi u optičkim mrežama.

U trećem delu, pored teorijskih osnova o kriptografiji uopšte, kriptografskim sistemima i algoritmima koji su opisani, razmatra se menadžment ključeva i problemi koji se u vezi sa tim javljaju. Takođe su navedene moguće pretnje i napadi na telekomunikacioni sistem u pogledu ugrožavanja tajnih podataka.

Na bazi iznetih teorijskih osnova, u četvrtom delu, na modelu telekomunikacione mreže koji je predstavljen, izvršena je analiza i dat predlog rešenja. Identifikovani su problemi pri implementaciji, mogući načini njihovog prevazilaženja i izvršeno poređenje rešenja dostupnih na tržištu.

U zaključnom delu sumirani su rezultati i dodatno naglašene prednosti i nedostaci primenjenih rešenja u vidu daljih pravaca razvoja.

2. PREGLED TEHNOLOGIJA U OPTIČKIM TELEKOMUNIKACIJAMA

2.1 SDH/SONET

Sa pojavom potrebe za standardizacijom protoka, njihovim povećanjem i prevazilaženjem razlika u interfejsima i načinima multipleksiranja počelo je stvaranje nove tehnike. Godine 1985. predlog Bellcorda prihvaćen je za novi standard pod nazivom SONET. ITU-T proširuje SONET i nakon usaglašavanja 1988. nastaje SDH. Usvojene su tri osnovne SDH preporuke (G.707, G.708 i G.709) u kojima su definisani protoci, elementi, principi multipleksiranja, struktura ramova i struktura multipleksiranja.

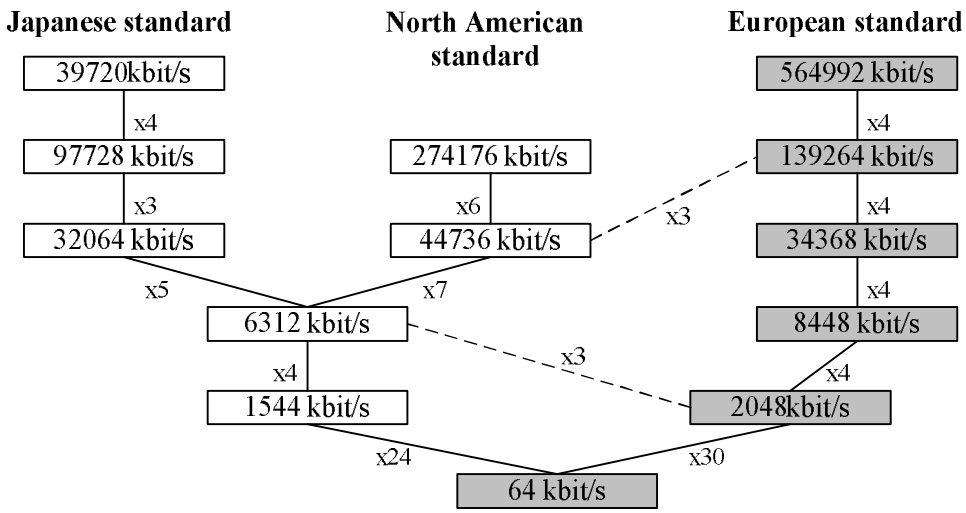
Sinhrone digitalne mreže SONET (*Synchronous Optical Networking* - po američkom ANSI standardu) ili SDH (*Synchronous Digital Hierarchy* - po evropskom ETSI standardu) često koriste različite termine za opisivanje istih funkcija i procesa. Ovo može da dovede do konfuzije i preteranih nepotrebnih razlika. Uz nekoliko izuzetaka, SDH se može posmatrati kao nadskup za SONET, te ćemo u nastavku posmatrati uglavnom ETSI standard, a ANSI ćemo pominjati samo u delovim u kojima je zbog boljeg razumevanja potrebno izvršiti poređenje sa istim.

2.1.1 RAZLOZI ZA UVOĐENJE SDH

2.1.1.1 Načini vremenskog multipleksiranja

Prema ITU-T (*International Telecommunication Union*) preporuci G-702 definisane su evropska i američka hijerarhije vremenskog multipleksiranja. One su bazirane na različitim primarnim digitalnim protocima, evropska na 2.048 kbit/s, a američka na protoku od 1.544 kbit/s u koje je moguće, na sličan način, multipleksirati 30 odnosno 24 kanala kapaciteta 64 kbit/s. Pored primarnih digitalnih signala 2.048 kbit/s i 1.544 kbit/s (ili E-1 - 2 Mbit/s i T-1 - 1,5 Mbit/s, kako se češće označavaju), radi daljeg povećanja iskorišćenja transmisionog puta, definisani su i sekundarni – E-2 (T-2), tercijalni – E-3 (T-3), kvartarni – E-4 (T-4) i kvintarni – E-5 (T-5) digitalni signali. Oni se dobijaju multipleksiranjem određenog broja signala iz predhodnog hijerarhijskog nivoa. Prikaz pomenutih hijerarhija, uključujući i japansku, koja nije zvanično definisana od strane ITU-T a razvijana je paralelno sa američkom, dat je na slici 1.

Ovakva šarolikost u brzinama prenosa pojavila se sa početkom digitalizacije zbog komercijalne izolovanosti regiona u svetu, ali je to kasnije, internacionalizacijom digitalnih komunikacija, bio i još uvek ostao veliki problem. On je delimično rešen definisanjem tzv. mešovite hijerarhije vremenskog multipleksiranja (2048-6312-44736-139264) koja je na slici 1 označena isprekidanim linijama.



Slika 1. Način vremenskog multipleksiranja prema evropskoj, američkoj i japanskoj hijerarhiji

Dobijanje digitalnog signala višeg reda vrši se multipleksiranjem određenog broja digitalnih signala iz prethodnog hijerarhijskog nivoa, uz njihovo dovođenje na zajednički takt. To se vrši korišćenjem neke od metoda izravnavanja (*Justification*), koje zavisno od brzine takta pritočnog signala može biti pozitivno, negativno i nulto. Izravnanje je postupak kontrolisane promene protoka pritočnog digitalnog signala ubacivanjem ili izdvajanjem bita u cilju njegovog usaglašavanja sa nekim drugim, raličitim protokom, bez gubitka informacije. Nakon dovođenja pritočnih signala na zajednički takt, vrši se njihovo multipleksiranje "bit po bit".

2.1.1.2 Ograničenja PDH tehnike

Pri formiranju digitalnih signala, postoje sinhrono i asinhrono (pleziohrono) vremensko multipleksiranje. Svi napred navedeni načini vremenskog multipleksiranja predstavljaju pleziohrono multipleksiranje na kome se zasniva PDH (*Plesiochronous Digital Hierarchy*) tehnologija.

PDH mreže nastale su kao alternativa analognim sistemima prenosa i kao odgovor na potrebe POTS (*Plain Old Telephon Service*) i kao takve nisu bile prilagođene zahtevima novijih servisa, posebno prenosu podataka u računarskim mrežama. Osnovni nedostaci PDH tehnike su sledeći:

- Nemogućnost identifikacije pojedinačnih kanala ili signala nižih protoka iz viših hijerarhijskih digitalnih signala. Primera radi ukoliko bi se vršilo odgranjavanje signala E-1 iz E-4, neophodno je signal od 140 Mbit/s demultipleksirati preko nivoa 34 Mbit/s i 8 Mbit/s do nivoa 2 Mbit/s, a zatim, posle izvršenog odgranjavanja izvršiti ponovo multipleksiranje obrnutim redosledom.
- Postojanje tri različite PDH hijerarhije u upotrebi širom sveta, što je uz veliku šarolikost interfejsa predstavljalo veliki problem u internacionalnim komunikacijama.
- Nedovoljan kapacitet rezervisan za prenos informacija potrebnih za nadgledanje i upravljanje mrežom.

- Ne postoji standardom definisan signal protoka većeg od 140 Mbit/s u Evropi i 45 Mbit/s u Americi, što za savremene servise predstavlja nezamislivo mali informacioni kapacitet.
- Ne postoji globalni standard za optičke interfejse digitalnih signala PDH hijerarhije, što onemogućava komunikaciju na optičkom nivou između PDH uređaja različitih proizvođača.
- Problemi sa povezivanjem opreme različitih proizvođača, najčešće zbog različite implementacije funkcija upravljanja mrežom.

2.1.2 BINARNI PROTOCI U SDH

Osnovni nivo u SDH predstavlja signal protoka 155.520 kbit/s i naziva se STM-1 (*Sinchronous Transport Module 1*). Ovaj protok je izabran iz dva razloga. Prvi je mogućnost prihvatanja PDH signala, nivoa E1 do E4, a drugi kompatibilnost sa tada već razvijenim američkim standardom SONET čiji osnovni nivo ima protok 51.840 kbit/s (STS-1 - *Synchronous Transport Signal 1*), a STS-3 protok od 3 x 51.840 kbit/s = 155.520 kbit/s.

Protoci signala na višim hijerarhijskim nivoima SDH formiraju se kao celobrojni umnožak binarnog protoka STM-1 signala. Prikaz do sada razvijenih binarnih protoka u SDH standardu dat je u tabeli 1. U prvoj koloni prikazan je odgovarajući nivo optičkog prenosnog signala OC-N. Oznaka STM-0 predstavlja de fakto naziv koji su uveli pojedini proizvođači za protok STS-1 sa aspekta SDH.

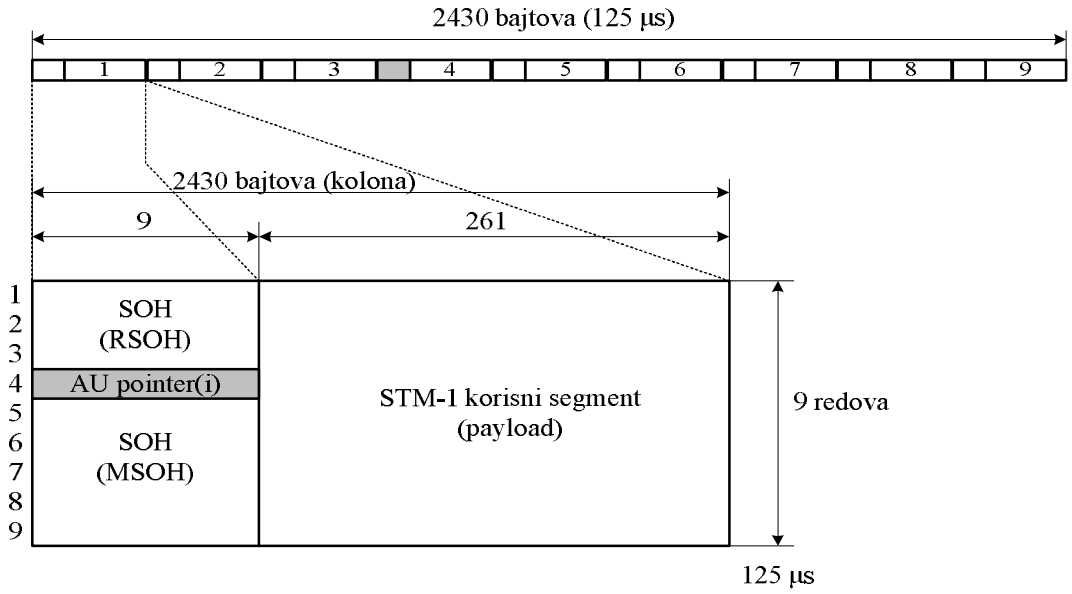
SONET/SDH Designations and bandwidths				
SONET Optical Carrier Level	**SONET Frame Format**	**SDH level and Frame Format**	**Payload bandwidth (kbit/s)**	**Line Rate (kbit/s)**
OC-1	STS-1	STM-0	50,112	51,840
OC-3	STS-3	STM-1	150,336	155,520
OC-12	STS-12	STM-4	601,344	622,080
OC-24	STS-24	–	1,202,688	1,244,160
OC-48	STS-48	STM-16	2,405,376	2,488,320
OC-192	STS-192	STM-64	9,621,504	9,953,280
OC-768	STS-768	STM-256	38,486,016	39,813,120

Tabela 1. Binarni protoci u SDH standardu

Linkovi sa protocima STM-1 i STM-4 namenjeni su, na primer, za povezivanje udaljenih LAN mreža na internet ili više LAN mreža u jednu Intranet mrežu. Internet provajderi, zbog potrebe za velikom brzinom prenosa podataka, koriste jednu ili više STM-16 ili STM-64 konekcija, dok se signali višeg reda koriste za internet okosnice kao i za povezivanje velikih telekomunikacionih mreža na internacionalnom nivou. Pored prenosa podataka iz računarskih mreža, mapiranjem Etherneta, o čemu će kasnije biti više reči, signali SDH hijerarhije su transparentni i za prenos govornih telefonskih kanala pa je u javnim telefonskim mrežama (PSTN - *Public Switched Telephone Network*) SDH u masovnoj upotrebi.

2.1.3 OSNOVNA STRUKTURA STM-1

STM-1 ram (slika 2) ima dužinu 2430 bajtova i izdeljen je u 9 jednakih segmenata koji, kada se poređaju jedan ispod drugog daju matrični izgled rama. Tako predstavljen STM-1 ram ima 9 redova po 270 bajtova. Prenos se vrši red po red, pri čemu poslednji bajt reda prethodi prvom bajtu sledećeg reda. Ram STM-1 signala, kao i ramovi svih STM-N signala, traje 125 μs, što znači da se ponavlja sa učestanošću 8000 Hz. Odgovarajući binarni protok je 155.520 kbit/s (2430 x 8 x 8000), što predstavlja osnovni binarni protok u SDH standardu. Uočava se da svaki bajt predstavlja protok od 64 kbit/s.



Slika 2. Struktura STM-1 signala

U opštem slučaju, STM-N ram ima 9 redova sa po N x 270 bajtova i takođe traje 125 μs. Samim tim se dobija da protok STM-N signala iznosi N x 155.520 kbit/s.

STM-N ram ima tri zone:

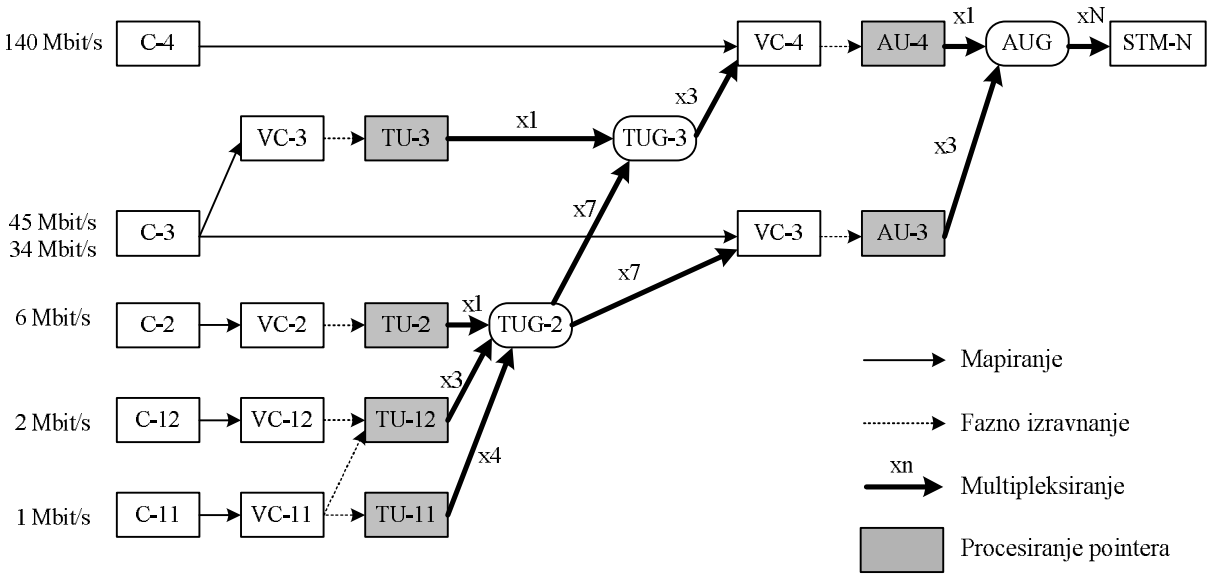
- zaglavlje sekcije (SOH - *Section Over Head*) koje je podeljeno u dve podzone, i to zaglavlje regeneratorske sekcije (RSOH - *Regenerator Selection Over Head*) i zaglavlje multipleksne sekcije (MSOH - *Multiplex Section Over Head*),
- AU pointer i

- korisni segment (*STM-N payload*).

Svaka zona ima svoju ulogu u obradi signala, a ta uloga se svodi na što efikasnije postupke smeštanja pritočnih signala u SDH hijerarhiju na predaji i prepoznavanje istih na prijemnoj strani.

2.1.4 STRUKTURA MULTIPLEKSIRANJA

Struktura multipleksiranja SDH signala prikazana je na slici 3.



Slika 3. Osnovna struktura multipleksiranja za SDH standard

Suština SDH multipleksiranja zasniva se na tri grupe procedura, i to: mapiranje pritočnog signala u virtuelni kontejner, fazno izravnanje dodavanjem pointera i multipleksiranje.

2.1.4.1 Mapiranje u virtuelni kontejner

Virtuelni kontejner VC-n (n = 1X, 2, 3, 4) (VC - *Virtual Container*) je informaciona struktura koja je predviđena za podržavanje veze na sloju puta u SDH mrežama. To je u osnovi digitalni signal koga čini niz uzastopno generisanih ramova, a osnovna funkcija mu je smeštanje pritočnih signala u jedinstvenu informacionu strukturu radi lakše dalje obrade. Postoji pet standardnih VC, a to su: VC-11, VC-12, VC-2, VC-3 i VC-4. Prva cifra u oznaci VC, označava hijerarhijski nivo pritočnog PDH signala, a druga, ukoliko postoji, označava da za taj hijerarhijski nivo PDH signala postoje dva različita VC, poseban za američki, a poseban za evropski standard. Primećujemo da ne postoji VC za smeštanje E-2 signala, a da za signale E-3 i T-3 postoji jedinstven VC-3, što je dogovoreno pre samog definisanja standarda.

Virtuelni kontejneri, zavisno od toga da li su namenjeni samo za smeštanje određenog pritočnog signala ili i VC nižeg hijerarhijskog nivoa, mogu biti VC višeg i VC nižeg reda. Svaki VC, pored korisnog segmenta u koji se smeštaju pritočni signali, ima i svoj servisni deo koji označavamo sa POH (*Path Over Head*) ili zaglavlje puta. Uloga POH je da prenosi kontrolne informacije koje, između ostalog, služe za nadgledanja ispravnog transporta korisnog segmenta virtuelnog kontejnera od mesta njegovog formiranja do mesta rasformiranja. Virtuelni kontejneri VC-3 i VC-4 imaju jednake strukture zaglavlja puta pa se taj POH označava kao VC-3/VC-4 POH dok virtuelni kontejneri VC- 11, VC-12 i VC-2 imaju drugi tip zaglavlja puta koji se označava kao VC-1/VC-2 POH.

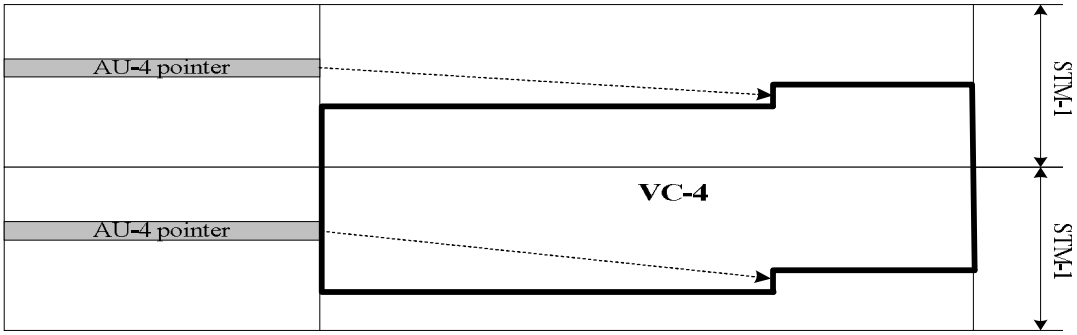
Kada se korisni segment koristi za smeštanje pritoke, tj. ako se radi o VC nižeg reda, taj korisni segment se tada naziva kontejner (C - *Container*). Postupak koji se realizuje na ulazu u SDH mrežu i koji podrazumeva adaptaciju i smeštanje pritočnog signala u odgovarajući VC, tačnije u njegov C, naziva se mapiranje (*mapping*). Dakle, pritočni signal se mapira u C, dodaje se POH i dobija se VC, čiji se sadržaj ne menja sve do izlaska iz SDH mreže.

2.1.4.2 Uloga pointera i fazno izravnanje

Rešavanje problema direktne identifikacije pritočnih signala u zbirnom STM-N signalu, koji se često navodi kao problem njihove vidljivosti, uslov je da bi se omogućilo njihovo jednostavno odgranjavanje, fleksibilno rutiranje i efikasno nadgledanje. Taj problem se u SDH tehnici svodi na problem vidljivosti virtuelnih kontejnera koji se prenose unutar STM-N signala. Da bi se obezbedio jednostavan pristup VC-u kao signalu, nije dovoljno u svakom trenutku imati informaciju o tome u kom delu korisnog segmenta STM-N rama se on prenosi, već i informaciju o tome gde je početak i kraj svakog njegovog rama. Naravno, dovoljno je samo znati početak VC rama, jer je njegov kraj jednoznačno definisan njegovom dužinom, ali i početkom sledećeg VC rama. Rešenje tog problema videlo se u tome da se početak svakog virtuelnog kontejnera definiše relativno, tj. u odnosu na neku referentnu poziciju u zoni korisnog segmenta STM-N rama namenjenoj za prenos posmatranog virtuelnog kontejnera. S obzirom na to da se virtuelni kontejneri nižeg reda prvo smeštaju u odgovarajući virtuelni kontejner višeg reda (u Evropi je to VC-4), da bi se odredio početak rama VC nižeg reda neophodno je prvo odrediti početak rama VC višeg reda. Referentna pozicija u odnosu na koju se definiše početak VC-4 definisana je samom identifikacijom početka STM-N rama.

Početak STM-N rama jednoznačno je definisan signalom sinhronizacije STM-N rama koji se prenosi u prvih nekoliko bajtova RSOH. Logično je da se informacija o tome koliko je početak posmatranog VC-4 pomeren u odnosu na tu referentnu poziciju mora čuvati na nekoj lokaciji u STM-N ramu koja ne pripada korisnom segmentu STM-N rama. Odlučeno je da se za čuvanje te informacije rezerviše zona u prvih Nx9 bajtova četvrtog reda STM-N rama koji se naziva zona AU-pointera (za STM-1 će biti svega 9 bajtova).

U toj zoni se prenosi N AU-4 pointera, od kojih svaki nosi informaciju o relativnom faznom pomeraju početka odgovarajućeg VC-4 rama u odnosu na odgovarajuću referentnu poziciju u korisnom segmentu STM-N signala. Ovo ćemo najlakše objasniti na primeru STM-1 rama. U korisnom segmentu STM-1 signala prenosi se samo jedan VC-4 signal. Prema tome, u zoni AU pointera nalazi se samo jedan AU-4 pointer. Pošto protok VC-4 odgovara protoku korisnog segmenta STM-1 signala i ram VC-4 takođe traje 125 μs, broj bajtova VC-4 rama jednak je broju bajtova korisnog segmenta STM-1 signala.



Slika 4. Označavanje faznog pomeraja VC-4 rama u odnosu na STM-1 ram

Međutim, kao što je poznato, početak VC-4 se može nalaziti na bilo kom bajtu korisnog segmenta STM-1 rama (slika 4). Kao referentna pozicija u korisnom segmentu STM-1 rama izabrana je pozicija prvog bajta korisnog segmenta koji se prenosi iza AU-4 pointera. Dakle, u AU-4 pointeru se nalazi informacija o položaju prvog bajta VC-4 rama u odnosu na pomenuti referentni bajt. AU-4 pointer posmatranog STM-1 rama može da "pokaže" na bilo koji položaj VC-4 rama u zoni koja se nalazi između pomenutog referentnog bajta tekućeg STM-1 rama i odgovarajućeg referentnog bajta u narednom STM-1 ramu.

Deo korisnog segmenta STM-N rama namenjen za smeštanje jednog VC-4 i pridruženi AU-4 pointer čine informacionu strukturu koja se naziva AU-4 (*Administrative Unit 4*). Konkretno, u slučaju STM-1 rama, administrativnu jedinicu čini ceo korisni segment STM-1 rama i AU-4 pointer. Zaključujemo da AU-4 predstavlja strukturu koju čini fazno izravnati VC-4 i odgovarajući AU-4 pointer. U ETSI strukturi multipleksiranja AU-4 istovremeno predstavlja i AUG (*Administrative Group Unit*). U STM-N ramu se formira N ovakvih struktura. One su u STM-N ramu (N=4, 16, 64, 256) multipleksirane "bajt po bajt", čime se dobijaju SDH signali viših hijerarhijskih nivoa.

Definisanjem početka svakog VC-4 unutar STM-N rama, učinili smo ih sada lako vidljivim. Ukoliko je u VC-4 mapirana neka pritoka, recimo protoka 140 kbit/s, njena vidljivost je osigurana. Međutim, ukoliko se u VC-4 prenose virtuelni kontejneri nižeg reda (VC-1X, VC-2 i VC-3), ti signali još uvek nisu vidljivi. Sada sledi slična logika kao i u prethodnom slučaju. Na isti način na koji smo vršili fazno izravnavanje VC-4 unutar STM-N rama, vršićemo fazno izravnavanje svih VC nižeg reda unutar VC-4 rama.

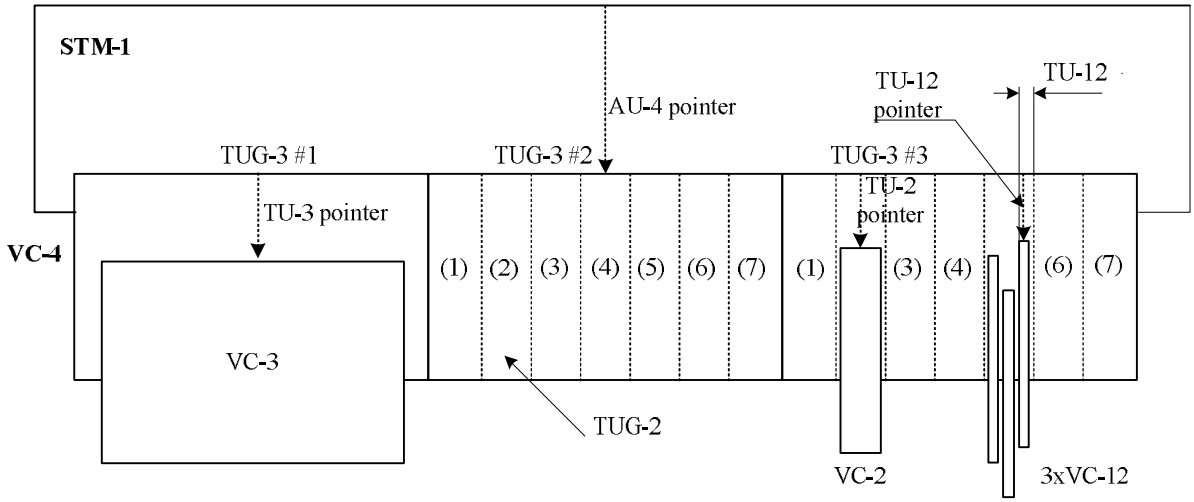
Imajući u vidu da se STM-N i VC koriste kao oznake i za ram i za signal, podređeni ram se može nazivati i ramom podređenog signala, a nadređeni ram ramom nadređenog signala. U tabeli 2 date su sve moguće kombinacije "podređeni ram - nadređeni ram" u ETSI strukturi multipleksiranja.

Podređeni ram	**Nadređeni ram**	**Naziv pointera**
VC-4	STM-N (N=1,4,16,64,256)	AU-4 pointer
VC-3	VC-4	TU-3 pointer
VC-2	VC-4	TU-3 pointer
VC-12	VC-4	TU-3 pointer

Tabela 2. Podređeni i nadređeni ramovi u ETSI strukturi multipleksiranja

Informacija o tome da li se VC-4 koristi za direktno smeštanje pritoke ili za smeštanje virtuelnih kontejnera nižeg reda prenosi se u njegovom zaglavlju puta (POH). Ukoliko je u pitanju drugi slučaj, onda se pored POH u njegovom ramu definišu još neke lokacije koje nisu predviđene za smeštanje virtuelnih kontejnera nižeg reda, tj. lokacija čiji je položaj određen samom identifikacijom početka VC-4 rama (pomoću AU-4 pointera). U tim lokacijama, kojih ima onoliko koliko se virtuelnih kontejnera nižeg reda prenosi u posmatranom VC-4, prenose se TU-pointeri koji ukazuju na relativni fazni pomeraj odgovarajućeg rama virtuelnog kontejnera nižeg reda u odnosu na neku referentnu poziciju u zoni korisnog segmenta VC-4 namenjenoj za prenos posmatranog VC nižeg reda. Fazni pomeraj virtuelnih kontejnera nižeg reda simbolično je prikazan na slici 5.

Generalno, fazni pomeraj podređenog rama u odnosu na nadređeni ram predstavlja položaj prvog bajta podređenog rama (bajta na koji ukazuje pointer) u odnosu na referentni bajt u nadređenom ramu. Pri tome su za vrednost pointera značajni samo oni bajtovi nadređenog rama u koje se smeštaju bajtovi datog podređenog rama. Postupak u kome se generiše odgovarajući pointer naziva se fazno izravnavanje (*Aligning*). Deo korisnog segmenta VC-4 rama namenjen za smeštanje jednog VC-n rama (n=1X, 2, 3) i pripadajući TU-pointer čini informacionu strukturu koja se naziva pritočna jedinica (TU - *Tributary Unit*). Na slici 9 možemo prepoznati sve informacione strukture koje se mogu pronaći unutar jednog VC-4 kada on prenosi virtuelne kontejnere nižeg reda.



Slika 5. Vrste i funkcije pointera u ETSI strukturi multipleksiranja

Grupa od tri TU-12 multipleksirane "bajt po bajt" naziva se TUG-2 (*Tribunary Unit Group 2*) tj. grupa pritočnih jedinica 2. Umesto tri TU-2, TUG-2 može činiti jedna TU-2. TUG-3 (*Tribunary Unit Group 3*) je struktura koju čini sedam TUG-2 multipleksiranih "bajt po bajt". Umesto sedam TUG-2, TUG-3 može činiti jedna TU-3.

2.1.5 ŠTA JE MOGUĆE MAPIRATI U SDH

Pošto se shvati način "ubacivanja" pritočnih signala u SDH hijerarhiju, potrebno je pokazati koji su to pritočni signali i na koji način funkcioniše njihovo mapiranje.

2.1.5.1 PDH pritoke

Kao što se vidi na slici 3, od evropskih PDH signala mogu se mapirati E-1, E-3 i E-4 u odgovarajući VC. Mapiranje u osnovi može biti asinhrono, sinhrono mapiranje bita i sinhrono mapiranje bajtova. Pošto svaki SDH uređaj ima sopstveni generator takta, koji je sinhronizovan sa delom ili kompletnom SDH mrežom, zavisno od toga da li ptitočni PDH signal odstupa od tog takta ili je sinhronizovan sa njim, primenjuje se odgovarajući način mapiranja.

PDH signali višeg reda uvek se mapiraju asinhrono, dok se primarni signal može mapirati asinhrono ili sinhronim mapiranjem bajtova. Sinhrono mapiranje bajtova, pored toga što zahteva postojanje sinhronizma između uređaja u kom se generiše pritočni PDH signal i SDH uređaja, zahteva i da ram PDH signala bude organizovan preko bajtova. Prednost sinhronog mapiranja bajtova je ta što se u okviru signala 2.048 kbit/s u svakom trenutku može direktno pristupiti signalima 64 kbit/s i Nx64 kbit/s. To je moguće zato što se sinhronim mapiranjem svaki TS (*Time Slot*) rama primarnog PDH signala smešta na unapred definisanu poziciju rama VC-1X.

2.1.5.2 ATM ćelije

Za razliku od izvora koji generišu digitalne signale konstantnog protoka, kao što je slučaj kod PDH, postoje i izvori promenljivog protoka. Takvi signali se radi lakšeg prenosa pakuju u ATM (*Asynchronous Transfer Mode*) ćelije. ATM predstavlja neki vid vremenskog multipleksiranja, ali takav u kome se kapaciteti sistema penosa više ne dodeljuju u fiksnim vremenskim intervalima već u skladu sa trenutnom aktivnošću izvora signala. ATM ćelija se sastoji od 53 bajta od kojih prvih 5 čini zaglavlje, a preostalih 48 korisni segment.

ATM ćelije se mapiraju u VC-4, tačnije C-4 tako što se bajtovi ćelija jedan za drugim smeštaju u bajtove C-4. Pri tome se vrši poravnavanje granica bajtova ćelija sa granicama bajtova C-4 Obzirom da kapacitet C-4 iznosi 2.430 bajtova, što nije celobrojni umnožak dužine ATM ćelije, dozvoljeno je da se poslednja ćelija u C-4 ramu završi u sledećem po redu C-4 ramu. Mapiranje ATM ćelija u VC-4-Xc vrši se na sličan način kao i u VC-4. I u ovom slučaju dozvoljeno je da poslednja ćelija u C-4 ramu završi u sledećem po redu C-4 ramu. VC-4-Xc je oznaka za virtuelni kontejner nastao udruživanjem više VC-4 (ukupno X VC-4). Odgovarajući kontejner (C-4-Xc) ima X puta veći kapacitet od C-4.

2.1.5.3 Ethernet over SDH

Kada govorimo o digitalnim signalima promenljivog protoka, najčešće mislimo na Ethernet pakete u okviru različitih računarskih mreža. SDH tehnologija je uvođenjem GFP (*Generic Framing Procedure*, ITU-T G.7041), VCAT (*Virutal Concatenation*, ITU-T G.707) i LCAS (*Link Capacity Adjustment Scheme*, ITU-T G.7042) procedura postala tehnologija koja omogućava efikasno, transparentno, granularno i dinamički promenljivo, po zauzetom kapacitetu, prenošenje paketskog saobraćaja. Na taj način dobija se objedinjen sistem za prenos TDM i Ethernet saobraćaja.

GFP definiše generički mehanizam za adaptaciju sa viših protokolskih slojeva na protokol SDH mreže. Standardom su definisana dva radna režima: prenos paketa (GFP-F - *Frame Maped GFP*) i prenos univerzalnog toka podataka (GFP-T – *Transparent GFP*). Za enkapsulaciju Ethernet paketa u SDH ramove koristi se GFP-F, pri čemu se otklanjaju nepotrebna zaglavlja Ethernet rama (preambula i deo koji razgraničava ramove), a potom se enkapsulira u GFP ram. Veličina zaglavlja GFP rama je fiksna i u sebi nosi informaciju o dužini rama, kao i 16-bitnu sekvencu za detekciju i ispravljanje grešaka u zaglavlju.

VCAT ili virtuelna konkatenacija omogućava udruživanje više SDH kanala u jedan kanal radi formiranja kapaciteta linka koji će odgovarati zahtevima saobraćaja podataka klijenta. To je upravljački, planski orjentisan mehanizam kojim je omogućeno povezivanje dva ili više VC-n u jednu celinu, virtuelno povezanu grupu (VCG - *Virtually Concatenated Group*) koja se kroz SDH mrežu prenosi potpuno nezavisno. Upotreba VCAT mehanizma omogućava efikasnije i fleksibilnije korišćenje SDH mreža za prenos paketski orijentisanog saobraćaja.

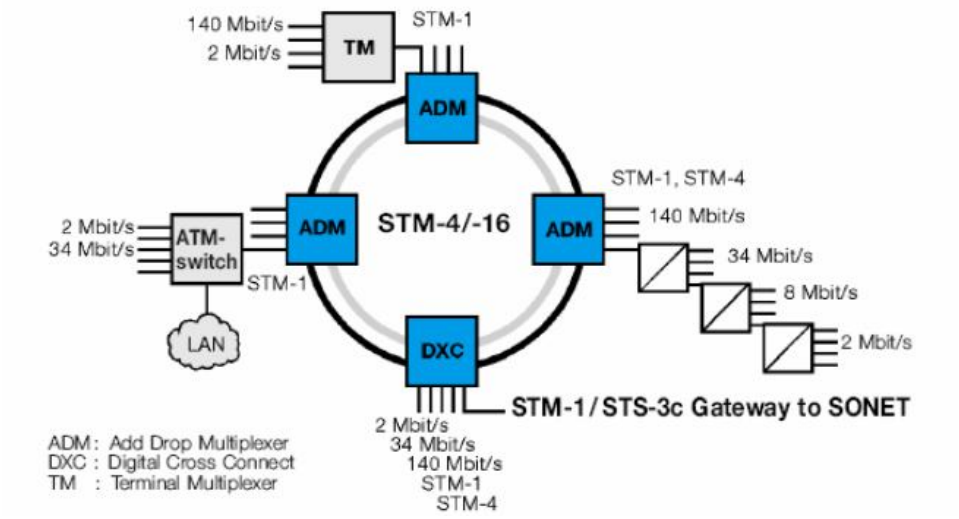
LCAS predstavlja proširanje VCAT mehanizma. Ova procedura obezbeđuje postepenu promenu kapaciteta virtuelnog linka, dodavanjem ili oduzimanjem kapaciteta koji čini virtuelni link, bez gubitka paketskog saobraćaja. Ovo je jako bitno s obzirom na vremensku neujednačenost protoka paketskog saobraćaja.

Kombinacija SDH sa GFP, VCAT i LCAS obezbeđuje mrežnu okosnicu za istovremeni prenos TDM servisa i paketskog saobraćaja, što je veoma čest zahtev u telekomunikacionim mrežama.

2.1.6 ELEMENTI SDH MREŽE

Pod elementima SDH mreže podrazumevamo sve multipleksne uređaje bazirne na SDH (SDH multiplekseri), u kojima su obično integrisane i funkcije sinhronih uređaja za prospajanje i sinhronih linijskih uređaja. Za sinhrone multipleksere je karakteristično da imaju izrazito modularnu strukturu. Jednostavnim dodavanjem modula ili samim preprogramiranjem uređaja, moguće je, ne samo povećati kapacitet, već i kvalitativno promeniti njegovu funkciju. Ovoj osobini SDH uređaja još širi smisao daje činjenica da svi proizvođači opreme teže da unificiraju funkcionalne celine istog tipa za ceo spektar svojih SDH uređaja. Za sva SDH multipleksne uređaje karakteristično je i da se nadgledanje, kontrola i upravljanje njihovim radom vrši daljinski, pomoću TMN (*Telecommunication Management Network*), a preko odgovarajućih međuspojeva.

Osnovne funkcionalnosti SDH multipleksera su ADM (*Add/Drop Multiplexing*) i DXC (*Digital Cross Connect*). Njihov tipični način primene prikazan je na slici 6.



Slika 6. Vrste SDH multipleksera i njihove funkcionalnosti

Shodno funkcijama SDH multipleksera kao i potrebama za pokrivenost servisima, moguće je realizovati različite konfiguracije SDH mreža. Postoje sledeće konfiguracije: konfiguracija tačka - tačka, add/drop konfiguracija, prstenasta struktura, hub konfiguracija i mešovita konfiguracija.

Konfiguracije tačka-tačka mogu se koristiti za ostvarivanje veze većeg kapaciteta kad god je SDH rešenje u pogledu cene konkurentno drugim sistemima prenosa.

Add/drop konfiguracija, tzv. konfiguracija lanca, može se koristiti u svim slučajevima kada su čvorovi raspoređeni duž nekog pravca. Usputni čvor preuzima saobraćaj od drugih čvorova (koji je njemu namenjen) odgranjavanjem iz zbirnog signala, a saobraćaj drugim čvorovima upućuje zauzimanjem slobodnih kapaciteta u zbirnom signalu. Drugim rečima, svaki usputni čvor možemo shvatiti kao regenerator za zbirni STM-N signal, koji ima mogućnost odgranjavanja i ponovnog zauzimanja.

Prstenasta struktura je, u stvari, zatvorena linearna konfiguracija u delovima mreže, koji zahtevaju vrlo visoku raspoloživost, veoma je preporučljivo koristiti tzv. samoizlečive prstenaste strukture (*Self-Healing Ring Structures*). Takve strukture su sposobne da se rekonstruišu samostalno, bez ikakve intervencije spoljašnjeg sistema za upravljanje mrežom, pa se u slučaju ispada pojedine trase (npr. prekida kabla) ili čvora unutar prstena, brzim rutiranjem saobraćaja obezbeđuje kontinuitet servisa. Postoje brojni metodi za realizaciju zaštite od prekida saobraćaja, kod ove, ali i kod ostalih konfiguracija SDH mreže.

Hub konfiguracija podrazumeva korišćenjem sinhronih interfejsa na pritočnoj strani multipleksera. Time se eliminiše potreba za vezivanjem multipleksera "leđa u leđa". Na taj način posmatrani multiplekser postaje hub-multiplekser koji vrši koncentraciju saobraćaja u prostornom odnosno geografskom smislu. Hub-multiplesker se obično nalazi u centru zvezdaste strukture neke SDH podmreže.

Mešovita konfiguracija se najčešće koristi, a predstavlja slučaj kada sve navedene strukture koegzistiraju u jednoj SDH mreži.

2.2 CARRIER ETHERNET

Ethernet tehnologija prenosa pruža veliki propusni opseg po relativno niskoj ceni, jednostavna je za korišćenje i podržava multipoint konfiguracije mreža. Iz tih razloga, od svoje prve standardizacije početkom osamdesetih godina do danas, predstavlja „de fakto" nosioca servisa u LAN mrežama. Međutim, iako je Ethernet tradicionalno tehnologija lokalnih mreža, njegov permanentni razvoj doveo je do penetracije Etherneta do nivoa regionalnih i gradskih mreža, dok su poslednja istraživanja i potreba za standardizacijom doveli do razvoja 100 Gb Etherneta, koji bi u bliskoj budućnosti mogao da postane tehnologija izbora i ozbiljan konkurent ostalim tehnologijama koje se primenjuju u transportnom delu mreže, prvenstveno SDH/SONET tehnologiji.

2.2.1 STRUKTURA ETHERNET RAMA I TIPOVI ETHERNETA

2.2.1.1 Struktura Ethernet rama

Slika 7 pokazuje format Ethernet rama, odnosno frejma (*frame*). Ovaj osnovni format ostao je nepromenjen u dužem vremenskom periodu uprkos brzom razvoju Etherneta i drugačijoj tehnologiji izrade fizičkih slojeva. Ethernet je višemedijumska tehnologija zato što operiše na različitim medijima pri različitim brzinama. Ethernet uređaji se dizajniraju sa vrlo jasno definisanim interfejsom između MAC (*Media Access Control*) i fizičkog podsloja Etherneta. Slojeviti pristup dozvoljava fizičkom sloju da se razvija nezavisno od MAC podsloja. Ethernet frejmovi predstavljaju format podataka za MAC sloj. To je uobičajena specifikacija za formate MAC frejmova koji dozvoljavaju Ethernet proizvode različitih brzina. Zapravo, Ethernet komutatori su obično konstruisani od portova različitih brzina i tipova prenosnog medija.

7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes
Preamble	*SDF*	*DA*	*SA*	*Length/ Type*	*Packet*	*FCS*

Slika 7. Delovi Ethernet frejma

Nepromenljivi format dozvoljava svakoj generaciji Etherneta da bude kompatibilna sa prethodnim generacijama, tako da korisnik ne mora unapređivati softver viših slojeva OSI modela i aplikacije kada je brzina mreže povećana. Ovo je odigralo veliku ulogu pri obezbeđivanju uspeha Etherneta.

U opštem slučaju, Ethernet ram ima sledeće delove:

- Preambula - 7 bajtova (*Preamble*) – Čini je niz: “10101010…" Ovim kodom se vrši sinhronizacija komunikacije i upozorava se prijemna stanica da pristiže frejm.
- Razgraničavač - 1 bajt (SDF - *Start of frame delimiter*) - Predstavlja kod “10101011” nakon koga sledi odredišna adresa.
- Odredišna adresa - 6 bajtova (DA - *Destination address*) - Određuje koja stanica treba da primi frejm.
- Adresa izvora - 6 bajtova (SA - *Source address*) - Adresa uređaja koji šalje frejm.
- Dužina/tip - 2 bajta (*Length/Type*) - Polje zaduženo za reprezentaciju dužine korisnog polja. Pošto je dozvoljena maksimalna veličina korisnog dela frejma (polja za podatke) samo 1.500 bajtova, vrednost dužina/tip iznad 1.536 predstavlja tip eternet frejmova. Često se koristi kao predstavnik protokola gornjih slojeva ili kao tip upravljačkih informacija sadržanih u delu za podatke.

- Paket - 46-1.500 bajtova (*Packet*) - Polje u kojem su sadržani podaci, a ako je dužine korisnih podataka manje od 46 bajtova, ostatak se popunjava „prazninama“.
- Sekvenca za proveru frejma - 4 bajta (FCS - *Frame Check Sequence*) - Upisuje se rezultat algoritma CRC primenjenog na frejmu, u cilju prepoznavanja oštećenja paketa pri fizičkom prenosu.

Teži se da Ethernet frejmovi sadrže minimum upravljačkih informacija. Jednostavnija struktura frejma pomaže da i mrežna oprema bude manje složenija i jeftinija. Ipak, kako infrastrukturne mreže nastavljaju da rastu i održavanje Etherneta postaje sve važnije. Originalni format frejma sa minimalnim dodatnim dizajnom nije više dovoljan. Ekspanzija Ethernet frejmova pažljivo se uvedi kako bi dopustila njegov rast uz minimizaciju uticaja na postojeće proizvode.

2.2.1.2 Tipovi Etherneta

Na različitim stepenima tehnološkog razvoja, postoje različiti tipovi Etherneta. Oni se, u većoj ili manjoj meri koristi i danas. Najčešće korišćeni su:

- Ethernet na 10 Mbit/s,
- Brzi Ethernet (*Fast Ethernet)*,
- Gigabitni Ethernet (*Gigabit Ethernet*),
- 10-Gigabitni Ethernet (10-*Gigabit Ethernet*),
- 40- i 100- *Gigabit Ethernet*.

Ethernet na 10 Mbit/s sastoji se od 4 osnovna oblika:

- 10Base5 ili široki Ethernet, na debelom koaksijalnom kablu (9,5 mm) i impedanse 50Ω,
- 10Base2 ili tanki Ethernet na tankom koaksijalnom kablu (0,48 mm) i impedanse 50Ω,
- 10Base-T, na UTP kablovima sa uprednim paricama i
- 10Base-F, prva verzija Ethernet tehnologije na optičkom vlaknu.

Svi podtipovi Etherneta na 10Mbit/s koristili su tzv. Manchester kod, takođe poznat kao fazno kodiranje.

Fast Ethernet ima brzinu 100 Mbit/s. Nastao je kao napredna verzija standardnog 10Base-T. Kao rezultat unapređivanja razvijena su tri odvojena standarda fizičkog sloja: 100Base-TX, 100Base-T4 i 100Base-T2. Do poboljšanja je došlo tako što se koristi naprednija tehnika kodiranja podataka tzv. 8B6T. Najpopularnije implementacije *Fast Etherneta* su:

- 100Base-TX na kablovima sa upredenim paricama kategorije 5 i
- 100Base-FX sa optičkim vlaknima.

Gigabit Ethernet je tehnologija koja omogućava prenos brzinama od 1000 Mbit/s. Potpuno je kompatibilan sa prethodnim Ethernet mrežama i omogućava jednostavnu migraciju ka većim brzinama prenosa. Mreže mogu da povećavaju performanse bez zamene postojećeg ožičenja, protokola i aplikacija. Razvijeni standardi su:

- 1000Base-T - Koristi UTP kabl kat. 5, sa sva četiri para parica uz kodiranje 4D-PAM5,
- 1000Base-CX - STP kabl sa 2 parice, kodiranje 8B/10B,

- 1000Base-SX - višerežimsko optičko vlakno, laserska svetlost talasne dužine 800 nm i dometa do 550 m i
- 1000Base-LX - jednorežimsko optičko vlakno, talasne dužine 1300 nm i dometa do 5 km.

10-*Gigabit Ethernet* definiše verziju sa nominalnom propusnom moći od 10 Gbit/s, deset puta većim od *Gigabit Ethernet*. Proteklih nekoliko godina objavljeni su sledeći standardi:

- 802.3ae – 2002 – standard koji definiše sisteme za rad po optičkom vlaknu – SR, LR, ER i LX4,
- 802.3ak – 2004 – 10 Gb Ethernet na bakarnim kablovima - CX4,
- 802.3an – 2006 – definiše 10GBASE-T sistem na upredenim paricama i 10GBASE-LRM optički sistem i
- 802.3ap – 2007 – dva nova sistema na bakarnim kablovima – KR i KX4.

10-Gigabitni Ethernet podržava samo komunikaciju u potpunom dupleksu koristeći pri tome bakarne STP i UTP kablove kategorija 6a i 7 i optička vlakna. On koristi novi PCS način kodiranja (64B66B) sa samo 3% dodatnog saobraćaja.

Najveća promena, u odnosu na prethodne tipove Etherneta, se ogleda u tome što je eliminisan metod CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), jer 10-Gigabitni Ethernet koristi samo full-duplex mod, što znači da detekcija kolizije nije neophodna.

40- i 100- *Gigabit Ethernet* su ratifikovani od strane IEEE u junu 2010 [14], a podržavaju slanje Ethernet linkova u potpunom dupleksu preko više 10 Gbit/s linkova ili STM-256. Najverovatniji tokovi sledećih viših hijerarhijskih nivoa, a zavisno od brzine razvoja prenosa po optičkom vlaknu, biće 400Gb-Ethernet i 1Tb-Ethernet.

2.2.2 PRIMENA ETHERNETA U TRANSPORTNIM MREŽAMA

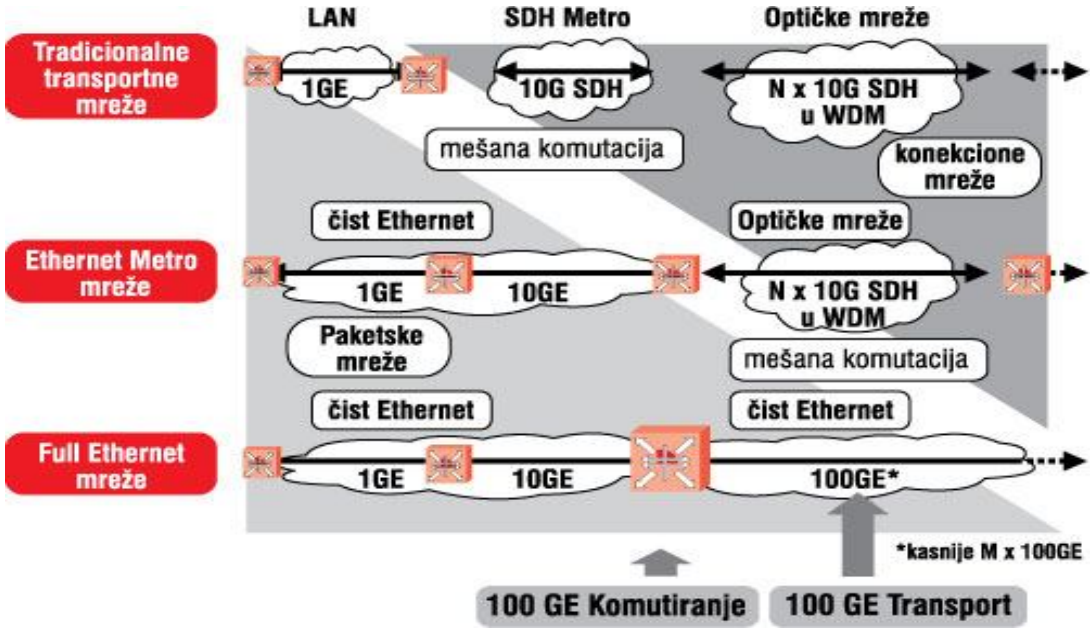
2.2.2.1 Evolucija ka Carrier Ethernetu

Carrier Ethernet koristi Ethernet kao osnovnu tehnologiju, a zatim joj dodaje određene osobine i funkcije kako bi dobio rezultantne proizvode koje bi pozicionirao u transportne mreže. Na slici 8 simbolično je prikazan prelazak Etherneta iz LAN-a na transportni nivo [15].

Metro Ethernet Forum (MEF) definisao je pet atributa koji razlikuju Carrier Ethernet od LAN Ethernet-a:

- Postojanje standardizovanih servisa,
- Skalabilnost,
- Pouzdanost,
- Kvalitet servisa i
- Upravljanje servisima.

Takođe su definisani i tipovi servisa (*E-Line, E-LAN i E-Tree*), parametri servisa i test procedure. Međutim, mnogo veći problem predstavlja suštinsko izrastanje LAN Etherneta u metro, nacionalne i globalne mreže.



Slika 8. Evolucaja Etherneta iz LAN-a u Metro i transportnu mrežu

U evoluciji ka Carrier Ethernet-u krenulo se od poznatog načina razdvajanja Ethernet broadcast domena VLAN (*Virtual Local Area Network*) tagovima, ali je problem bio u nedostatku transparentnosti za VLAN tagove krajnjih korisnika. Sledeći korak je bilo dodavanje posebnog transportnog S-VLAN taga, što se brzo pokazalo kao neadekvatno zbog malog broja mogućih vrednosti u situacijama sa više desetina hiljada korisnika i preopterećenosti MAC *forwarding* tabela. Trenutno rešenje podrazumeva enkapsulaciju korisničkog Ethernet rama u novi *backbone* Carrier Ethernet ram, sa posebnim B-DA i B-SA MAC adresama iz relativno malog skupa adresa koje pripadaju samoj transportnoj mreži i dodatnim B-TAG i I-TAG poljima za definisanje *backbone* VLAN taga, tipa servisa i prioriteta.

2.2.2.2 Poređenje sa SDH

Uticaj tradicionalnih transportnih tehnologija na Carrier Ethernet je značajan. SDH tehnologija je postavile visoke standarde po pitanju pouzdanosti, brze dijagnostike kvarova i kontinuiranog praćenja performansi. Zbog toga je Carrier Ethernet morao biti proširen čitavim nizom novih funkcija, od kojih su mnoge standardizovane po ugledu na SONET/SDH. Rešenja za probleme koji su sprečavali široku primenu LAN Etherneta u mrežama telekomunikacionih operatera su pronađena, velikim delom, po ugledu na SONET/SDH. To je i logično pošto su u pitanju isti problemi koje je trebalo prevazići.

Jedan od najčešće navođenih razloga, za izbor Carrier Ethernet plaforme je, da je logično da saobraćaj koji nastane kao Ethernet treba da se prenosi kao Ethernet. To bi bilo u potpunosti tačno da je u pitanju *native* Ethernet transport, tj. da se korisnički saobraćaj može dodati ili izdvojiti u svakoj tački transportne mreže, bez potrebe za uvođenjem posebnih *edge* funkcionalnosti. Carrier Ethernet *edge* uređaji moraju da efektivno mapiraju ili enkapsuliraju korisnički saobraćaj u *backbone* MAC pakete. Sa stanovišta operatera, razlika između GFP mapiranja koje se koristi u SDH mrežama i mapiranja u novi *backbone* MAC paket nije velika. U oba slučaja neophodno je postojanje funkcionalnih blokova za adaptaciju kako bi se korisnički saobraćaj prilagodio za prenos kroz transportnu mrežu.

Drugi problematični argument je navođenje opšte zastupljenosti LAN Etherneta kao i niske cene i troškova održavanja Carrier Ethernet opreme. Kao što je već pokazano, LAN Ethernet je neadekvatan za primenu u transportnim mrežama. Carrier Ethernet podrazumeva dizajniranje i proizvodnju novih tipova uređaja, sa čestim i značajnim ulaganjima u podršku za nove preporuke, pošto je standardizacija mnogih aspekata još uvek u toku. Dok cena opreme uglavnom zavisi od marketinške politike proizvođača i ne mora direktno da odražava uložena sredstva, dodatna obuka za upotrebu i održavanje je neizbežna. Carrier Ethernet jeste zasnovan na LAN Ethernet tehnologiji, ali preuzima mnoge koncepte iz SDH, tako da je period prilagođavanja neophodan bez obzira na prethodno iskustvo operatera i korisnika.

Dodatni faktor vezan za poređenje cene Carrier Etherneta i SONET/SDH tehnologije je potrošnja električne energije. SDH uređaji troše između jedne četvrtine i jedne polovine električne energije manje od Carrier Ethernet uređaja pri istoj količini prenesenog saobraćaja [17]. Veća potrošnja električne energije Carrier Ethernet uređaja posledica je činjenice da je obrada toka Carrier Ethernet paketa znatno zahtevnija od obrade SDH signala na istim brzinama prenosa. Pored uštede električne energije, koja će biti sve bitnija stavka u budžetu operatera telekomunikacionih mreža, korišćenje energetski efikasnije opreme je u skladu i sa *Green Networks* konceptom koji je sve prisutniji.

Fleksibilnost po pitanju propusnog opsega takođe je argument za diskusiju. Dimenzije virtuelnih kontejnera kod SDH, originalno namenjenih prenosu PDH pritoka, zaista nisu prilagođene prenosu Ethernet saobraćaja, ali je uvođenje VCAT i LCAS mehanizama umnogome prevazišlo ove probleme, donoseći granularnost paketskog prenosa na nivou kapaciteta jednog VC-12 kontejnera. Sa druge strane, Carrier Ethernet je izgubio nešto od fleksibilnosti dodavanjem kontrolnih mehanizama za zaštitu saobraćaja i specifičnih tipova servisa (npr. prenos E1 PDH signala) koji ne tolerišu odbacivanje paketa ili varijacije u kašnjenju.

U Carrier Ethernet mreži, kao i u SDH mreži, vrši se potpuna enkapsulacija pritočnog Ethernet saobraćaja i njegov prenos duž prethodno određene putanje. Jedino što prenošeni signali vide je uticaj koji je transportna mreža imala na njih sa stanovišta kašnjenja, džitera (varijacije kašnjenja), raspoloživosti veze i garancije propusnog opsega. Iz tog razloga potrebno je izvršiti poređenje za ove dve tehnologije. Tabela 3 [17] prikazuje garantovane vrednosti kašnjenja, džitera i raspoloživosti u Carrier Ethernet mreži i SDH mreži.

<table>
<tr><th>Parametar</th><th>Carrier Ethernet</th><th>SDH</th><th>Zahtev kod Mobile Backhaul mreže</th></tr>
<tr><td>Kašnjenje</td><td>< 25ms</td><td>< 100 μs</td><td>< 5 ms</td></tr>
<tr><td>Džiter</td><td>< 10 ms</td><td>< 3.2 μs</td><td>1 ms</td></tr>
<tr><td>Raspoloživost</td><td>99.95%
< 263 min./god.</td><td>99.999%
< 5.3 min./god.</td><td>99.999%
< 5.3 min./god.</td></tr>
<tr><td rowspan="2">Tačnost sinhronizacije mreže</td><td>< 50 ppb *</td><td>< 50 ppb *</td><td rowspan="2">50ppb</td></tr>
<tr><td colspan="2">* postiže se korišćenjem kvalitetnih oscilatora</td></tr>
</table>

Tabela 3. Zahtevi za kašnjenje, džiter, raspoloživost i tačnost sinhronizacije u Carrier Ethernet, SDH i mreži mobilne telefonije

Poređenja radi, u tabeli 3 su dati i zahtevano trajanje kašnjenja, džiter i raspoloživost u mreži mobilne telefonije tzv *Mobile Backhaul* telekomunikacionoj mreži baznih stanica mobilne telefonije i kontrolera baznih stanica. Kontroleri baznih stanica su sa druge strane povezani sa komutacionim centrima mobilne telefonije. *Mobile Backhaul* mreža predstavlja tipičnu telekomunikacionu mrežu sa naglim porastom paketskog saobraćaja te porastom potrebe za većim propusnim opsegom raspoloživošću, a bez tolerancije na visoke vrednosti kašnjenja i džitera. Poređenjem trajanja kašnjenja, džitera i vremena koje mreža provede u neispravnom stanju u SDH mrežama je za nekoliko redova veličine manje u odnosu na vrednosti ovih parametara u Carrier Ethernet mrežama. Poređenjem vrednosti u prvoj i trećoj koloni tabele 3, vidi se da Carrier Ethernet specifikacije ni po jednom od prikazanih kriterijuma ne zadovoljavaju zahteve mobilne telefonije. Pojedini proizvođači Carrier Ethernet opreme deklarišu znatno manje vrednosti ovih granica, čime se uklapaju u zahteve mreža za koje isporučuju uređaje. Ipak, visoke vrednosti ovih granica definisane od strane MEF, govore da postizanje vrednosti kašnjenja, džitera i raspoloživosti poredivih sa onima koje nude SDH mreže još nisu dostižne.

Prema napred navedenim argumentima u korist jedne i druge tehnologije prenosa, može se zaključiti da migracija Etherneta od LAN ka transportnom nivou ide postepeno, a da će SONET/SDH sistemi, i pored nedovoljne fleksibilnosti, uz odgovarajuća prilagođavanja paketskom saobraćaju ostati i dalje u upotrebi.

2.3 OPTIČKE MREŽE SA xWDM MULTIPLEKSIRANJEM

Bez obzira da li u sistemu prenosa koristimo SONET/SDH, Carrier Ethernet, konbinaciju obe tehnologije ili nešto sasvim četvrto, u nastojanju da budemo konkurentni na tržištu telekomunikacionih usluga, suočićemo se sa problemima obezbeđenja dovoljnog propusnog opsega u tom sistemu. Odgovor na ove probleme daje WDM (*Wavelength-Division Multiplexing*) talasno multipleksiranje. WDM danas omogućava prenos od 16 do 160 informacionih signala različitih protokola i različitih bitskih brzina na različitim talasnim dužinama kroz jedno optičko vlakno. Eksperimentiše se sa sistemima koji bi prenosili nekoliko stotina, pa i do hiljadu talasnih dužina istovremeno.

WDM je, u stvari, samo jedan u nizu xDM tehnologija (x = F, T, C i W) koja vrši multipleksiranje optičkih signala po parametru talasne dužine. Drugim rečima, više različitih optičkih signala različitih talasnih dužina se prenosi kroz jedno optičko vlakno, a pošto različite talasne dužine ne predstavljaju ništa drugo do različitih frekvencija, onda je WDM u suštini FDM (*Frequency Division Multiplexing)*. Jedinu, ali veoma značajnu razliku donose specifičnosti koje ovoj tehnici daju optički signali i optička vlakna umesto električnih signala i koaksijalnih kablova kod FDM.

2.3.1 PROSTIRANJE SIGNALA KROZ OPTIČKO VLAKNO

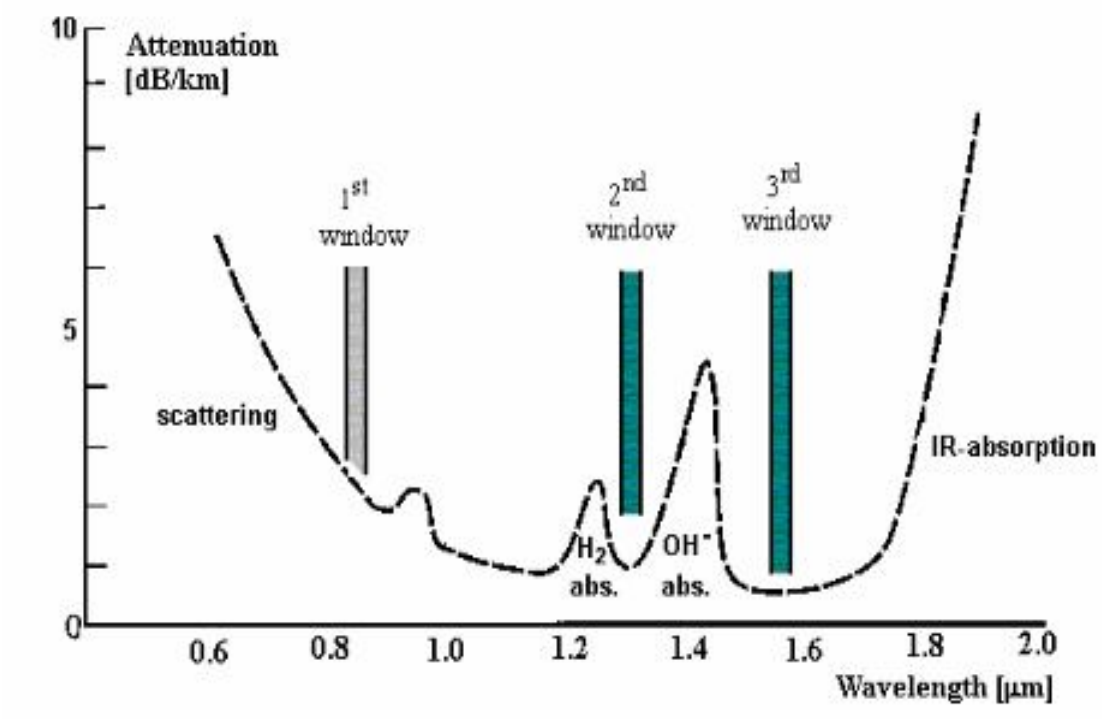
2.3.1.1 Optičko vlakno kao svetlovod

Pošto se prostiranje svetlosti kroz optičko vlakno zasniva na totalnoj refleksiji koja je uslovljena različitim indeksima prelamanja kod jezgra i omotača, neophodno je analizirati optičku snagu signala koji se prostire tj. njeno slabljenje i tzv. optičke prozore u kojima su slavljenja najmanja.

Slabljenje optičke snage u vlaknu uzrokovano je različitim faktorima koj mogu biti unutrašnji i spoljašnji. Unutrašnji uzrok je postojanje inherentnih nečistoća koje uzrokuju apsorpciju svetlosti u materijalu zbog interakcije fotona sa molekularnim nečistoćama u staklu, premeštanja elektrona, te prelaska elektrona između energetskih nivoa. Kada foton naiđe na nečistoću on se rasprši ili apsorbuje. Spoljašnji uticaji su posledica savijanja vlakna zbog čega se menja put koji svetlost prolazi, što je naročito izraženo kod multimodnih vlakana.

Slabljenje usled raspršenje svetlosti na nehomogenostima i nečistoćama u materijalu koje su odlika materijala ili nastaju pri proizvodnji vlakna, kao pojava naziva se *Rayleighovo* raspršenje, a emitovana svetlost *Tyndallova* svetlost. Faktoru slabljenja najviše doprinosi koeficijent prigušenja zbog *Rayleighovog* raspršenja, čak 96%. Ono je posebno izraženo od 700 nm do 1000 nm, s tim da prema većim talasnim dužinama opada. Međutim na većim talasnim dužinama (iznad 1700 nm) snaga je ograničena sa infracrvenom svetlošću, tj. postoji infracrvena apsorpcija, dok ispod 800 nm počinje rasti uticaj ultraljubičastog zračenja.

Na slici 9 prikazano je slabljenje u funkciji talasne dužine, koje predstavlja zbir svih, unutrašnjih i spoljnih uticaja. Ekstremi koji su dobijeni na rezultanoj krivi posledica su postojanja hidroksilnih molekula (OH) u vlaknu, a koji su posledica vlage. Ovi molekuli uzrokuju jako rezonantno slabljenje, a ne mogu se u potpunosti izbeći proizvodnim procesom. Osnovni mod im je na 2730 nm, a viši harmonici su na 950 i 1380 nm. Postojanje vlage kritično je na spojevima i konektorima te kod upotrebe vlakana treba voditi računa da isto ne dođe u dodir sa vlagom.



Slika 9. Slabljenje u optičkom vlaknu i optički prozori

Da bi se minimizirali negativni uticaji na optičku snagu, konstruisana su tri optička prozora koja se koriste u optičkim vlaknima:

- u pojasu oko 850 nm (I prozor),
- u pojasu oko 1300 nm (II prozor) i
- u pojasu oko 1550 nm (III prozor).

Minimum prigušenja za prvi prozor iznosi oko 2 dB/km, za drugi 0,5 dB/km, i za treći 0,2 dB/km. U početku je najviše korišćen prvi prozor, iako to nije optimalno rešenje, ali su postojali drugi problemi na drugom i trećem prozoru. Prvi prozor se danas i dalje koristi, ito zbog jeftine realizacije, dok se češće koriste opsezi oko druog i trećeg. Danas se već proizvedena optička vlakna sa slabljenjem koje se bliži teoretskom, te se granice između optičkih prozora postepeno zamagljuju.

2.3.1.2 Hromatska i polarizaciona disperzija i nelinearnost

WDM sistemi se prilikom transmisije svetlosti kroz optičko vlakno susreću sa još nekim izazovima. To su hromatska i polarizaciona disperzija i nelineranost.

Zbog toga WDM koristi isključivo monomodna vlakna u trećem (oko 1550 nm) gde je najmanje slabljenje signala, a pomeranje tačke nulte disperzije na željenu talasnu dužinu obezbeđuje se specijalnim metodama konstrukcije optičkih vlakana. Time su problemi slabljenja i hromatske i polarizacione disperzije praktično rešivi.

Veliki broj korišćenih kanala pri multipleksiranju uzrokuje povećanje intenziteta svetlosti u vlaknu, a time i pojavu nelinearnih efekata. Oni su posledica stimulisanog *Briluenovog* (SBS) ili *Ramanovog* (SRS) rasejanja, bilo fluktuacije indeksa prelamanja ili mešanje četiri talasa (FWM). Svi ovi efekti izazvaju degradaciju korisnog signala. Problem SBS se može ublažiti, dok SRS još nije reešiv i može predstavljati fundamentalnu granicu kapaciteta budućih optičkih sistema. Što se tiče pojave preslušavanja optičkih kanala, što je posledica FWM-a, ovaj efekat se može smanjiti tako što će postojati mala hromatska disperzija u celom opsegu. Zbog toga su realizovana vlakna sa smanjenim nagibom disperzione krive u celom opsegu talasnih dužina, koji je od interesa. Da bi se generalno umanjili nelinearni efekti ide se ka konstrukciji optičkih vlakana sa velikom efektivnom površinom (recimo okruženjem jezgra vlakna prstenom od materijala sa velikim indeksom prelamanja), čime bi se smanjila ukupna snaga optičkog signala kroz monomodna vlakna, ali tako da disperzija ostane i dalje kontrolisana.

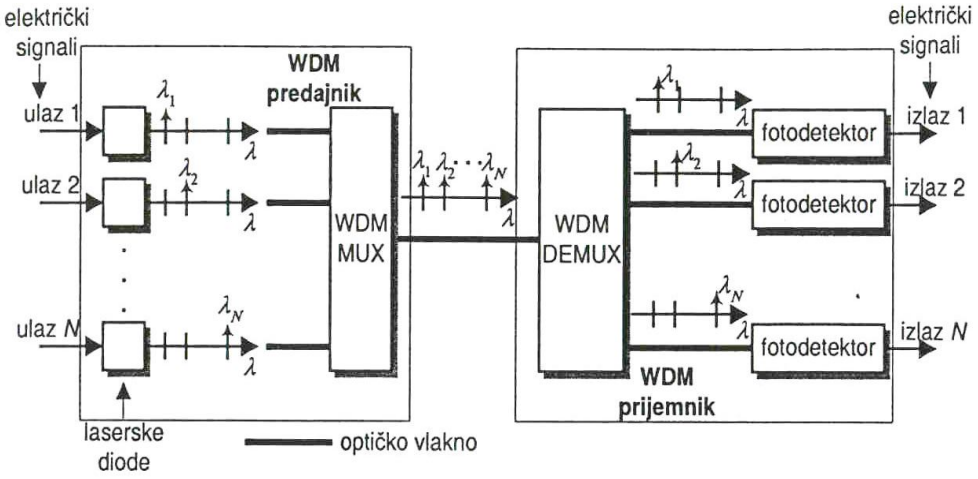
2.3.2 STRUKTURA xWDM SISTEMA

Princip rada xWDM sistema (slika 10) zasniva se na istovremenom prostiranju više svetlosnih talasa različitih boja (tj. talasnih dužina) kroz jedno optičko vlakno pri čemu raspoloživa širina frekvetnog opsega iznosi nekoliko THz.

Za xWDM sisteme karakteristične su sledeće veličine, na koje treba obratiti pažnju pri izboru elemenata tog sistema:

- Umetnuti gubici (*inserction loss*), koji predstavljaju gubitke na optičkom signalu zbog umetnutog WDM uređaja.
- Širina kanala (*channel width*), tj. spektralna širina pojedinog lasera. Od njegovih dimenzija direktno zavisi broj kanala koje je moguće preneti. Mogu se izražavati u nm ili kHz, a zadovoljavajuća vrednost je oko 100 kHz.
- Preslušavanje između kanala (*cross talk*), predstavlja mešanja pojedinih kanala u WDM multiplekseru. To je nelinearna pojava kao posledica nelinearnog međutalasnog mešanja.

WDM sistem se na predajnoj strani sastoji od elektrooptičkog konvertora tj. optičkog predajnika i WDM multipleksera, a na prijemnoj strani od WDM demultipleksera i optičkog prijemnika odnosno optoelektričnog konvertora.



Slika 10. Princip funkcionisanja xWDM sistema

Osnovne funkcije xWDM sistema su:

- Generisanje signala – izvor tj. predajni laser predajnika mora biti podešen tako da emituje svjetlost, unutar uskog zadanog opsega, koja predstavlja nosioca informacija.
- Kombinovanje signala - WDM sistemi koriste multipleksere (*MUX*) da bi kombinovali talase. Pri tome se javlja gubitak signala, vezan za multipleksiranje, koji može biti nadoknađen uz pomoć optičkih pojačavača.
- Emitovanje signala - efekat preslušavanja, degradacija i gubitak optičke snage se moraju uzeti u obzir prilikom prenosa optičkim vlaknima.
- Razdvajanje primljenih signala - na prijemnoj strani multipleksirani signali se moraju razdvojiti pomoću demultipleksera (*DEMUX*).
- Prijem signala – prenešeni signal se prima (detektuje) preko fotodetektora prijemnika.

2.3.2.1 Optički predajnici i prijemnici

Optički predajnici i prijemnici su vitalni delovi svakog optičkog prenosnog sistema. Za WDM je karakteristično da zahteva kvalitetne komponente, veoma uskog spektra zračenja, pa su standardne neupotrebljive.

Optički predajnici su u osnovi, izvori svetlosti koji, na osnovu ulaznog električnog signala, određenog intenziteta i frekvencije, emituju svetlost. Najčešće su u upotrebi laserske i LED diode. Što se tiče karakteristika, laserske diode imaju uži spektar zračenja, veću snagu na ulazu u vlakno i relativno veliku sposobnost modulacije, dok su LED diode prostije za izradu, jeftinije su i temperaturno nisu zavisne.

Pored svetlosnog izvora koji napaja optičko vlakno, u sebi imaju i modulator koji vrši modulaciju generisane svetlosti ulaznim binarnim signalom. Modulacija se najčešće vrši promenom intenziteta svetlosti koja se šalje na ulaz optičkog vlakna. U cilju efikasnog multipleksiranja xWDM sistemi optičkim predajnicima nameću sledeće specifične zahteve:

- Tačno definisana vrednost talsne dužine i izuzetno uska širina spektralne linije izvora,

- Mogućnost promene talasne dužine zračenja,
- Snaga izvora treba da bude dovoljno velika da može da se postigne željena vrednost verovatnoće greške,
- Neophodno je izvršiti efikasno fokusiranje svetlosti izvora, kako bi se optičko vlakno pobudilo dovoljnom optičkom snagom,
- Predajnik treba da generiše signal linearnih karakteristika kako bi se sprečili viši harmonici i intermodulaciona izobličenja,
- Velike brzine modulacije, kako bi se iskoristile prednosti optičkih vlakana,
- Fizičke karakteristike predajnika treba da budu usaglašene sa korišćenim optičkim vlaknom, tj. da imaju zadovoljavajuće dimezije i težinu kao i malu zavisnost od temperature.

Obezbeđenje ovih zahteva omogućava tehnologija integrisane optike kojom se realizuju hibridni sistemi u kojima je integrisan poluprovodnički laser sa sistemom za spoljašnju modulaciju i integrisanim elektronskim kolima. U fazi razvoja su mikro elektromehanički sistemi u realizaciji spoljašnje modulacije koji će obezbediti velike brzine signala. Danas su atraktivni modulatori bazirani na principu *Mah-Cenderovog* interferometa, realizovani u tehnologiji integrisane optike, integrisani sa laserskim čipom. Njima se postižu protoci veći od 100 Gbit/s.

Optički prijemnici su fotodetektori, koji primaju optički signal iz vlakna a na svom izlazu daju adekvatan električni signal. U upotrebi su fotodiode i fototranzistori.

Parametri koji su bitni u karakterizaciji optičkih prijemnika su: spektralni odziv, osetljivost, propusni opseg, dinamički opseg i šum. U skladu sa zahtevima koje postavljaju WDM sistemi, moguće je izvršti optimizaciju konstrukcije i uslova polarizacije fotodetektora, uzimajući u obzir nelinearne i nestacionarne efekte kod ovih elemenata.

2.3.2.2 Optički pojačavači

Pojačanje optičkog signala razlikuje se od pojačanja električnog u tome što može da se pojačava samo snagu signala bez obnavljanja njegovog oblika. Ovaj tip pojačanja obezbjeđuje potpunu transparentnost podataka, odnosno proces pojačanja je potpuno nezavisan od formata modulacije signala. Međutim njihova mana je da se optički šum pojačava sa korisnim optičkim signalom. Optički pojačavači koriste principe stimulisane emisije, slično kao i laseri, te unose i šum spontane emisije. Postoje tri osnovna tipa optičkih pojačavača:

- Poluprovodnički pojačavači bazirani na višestrukim kvantnim jamama, imaju veću širinu opsega i veće zasićenje pojačanja, omogućavaju kraće vreeme uključivanja i isključivanja, ali su više osjetljivi na polarizaciju. Poluprovodnički pojačavači mogu da dostignu pojačanja od 25dB i širinu opsega od 40nm. Njihova prednost je mogućnost integracije sa drugim komponentama.

- Optički pojačavači bazirani na dopiranim vlaknima, EDFA (*Erbium-Dopped Fibre Amplifier*), obezbjeđuju pojačanje za talasne dužine između 1525 nm i 1560 nm. Tipično pojačanje je oko 25dB. Za oblast oko 1300 nm, veliku pažnju privlače pojačavači bazirani na fluoridnim vlaknima dopiranim prazeodimijumom, (PDFFA - *Praseodymium-Dopde Fluoride Fiber Amplifier*). Ovi pojačavači imaju malo preslušavanje i šum, rade u opsegu od 1280 nm do1330 nm sa pojačanjem od oko 40dB. WDM u kombinaciji sa EDFA pojačavačima predstavlja izbor bez konkurencije za velike udaljenosti i velike brzine prenosa. Ograničenje ovih optičkih pojačavača je nejednak spektar pojačanja.
- Ramanovi pojačavači rade po principu nelinearnog *Ramanovog* rasejanja i moguće ih je primeniti na svim opsezima talasnih dužina što zavisi samo od talasne dužine pobudnog lasera. Kod njih se pojačanje ostvaruje rasejanjem u postojećem transmisionom vlaknu.

2.3.2.3 Optičko multipleksiranje i demultipleksiranje

Optički multiplekser prihvata skup optičkih signala različitih talasnih dužina sa više ulaznih vlakana i kombinuje ih u jedinstven optički signal. Ovu funkciju obavlja tako što ulazne optičke signale prostorno razdvojene, iz više optičkih vlakana, kroz optičko sočivo, dovodi na modulacioni optički element (spektralni filtar, prizmu, rešetku, AWG (*Arrayed Waveguide Grating*) rešetku ili dr.) na kome se obavljaju procesi refrakcije, difrakcije ili interferencije, koji zavise od talasne dužine ulazne svetlosti. Snopove svetlosti nakon ovog procesa objedinjuje drugo sočivo koje napaja izlazno optičko vlakno.

Proces demultipleksiranja je obrnut i predstavlja prostorno razdvajanje višekomponentnog optičkog signala sa različitim talasnim dužinama na bazi pomenutih procesa. Demultipleksiranje se vrši pre nego što snop svetlosti dospe na opto-električnu konverziju, jer su fotodetektori, koji vrše ovu funkciju, širokopojasni uređaji koji ne mogu selektivno da detektuju signal jedne talasne dužine.

Danas u upotrebi brojne tehnike multipleksiranja - demultipleksiranja, a najvažnije su sledeće:

- Filteri tankog filma,
- (De)multipleksiranje na bazi prizme,
- Difrakciona Bragova rešetka,
- Mreža indeksiranih varijabli talasovoda (AWG) i
- Interliver periodični filteri i frekvencijski renderi.

Razlikuju se aktivni i pasivni optički de/multiplekseri. Pasivni se baziraju na optičkim komponentama kao što su prizma, difrakciona rešetka i spektralni filtri, a aktivni su, u osnovi, kombinacija pasivnih komponenti i podesivih detektora, od kojih je svaki detektor podešen na određenu talasnu dužinu.

Ključni parametri WDM multipleksera su: centralna frekvencija, unutrašnji gubici, propusni opseg i preslušavanje kanala. Kod demultipleksera nužno je voditi računa da se postigne maksimalno razdvajanje optičkih kanala, a da pri tome preslušavanje bude minimalno.

2.3.2.4 Optički add/drop multiplekseri (OADM)

Jedan od osnovnih zahteva za optičku transportnu mrežu je njena dobra struktura. U WDM postoje slične mrežne arhitekture kao i u SDH (ring, mesh, itd.), podržane sličnim mrežnim elementima. Prema tome i funkcionalnosti tih arhitektura analogne su SDH i postižu se primenom optičkih add/drop multipleksera (OADM) i optičkih kroskonektora (OXC). Ovaj koncept optičkih mreža podrazumeva mogućnost da operater ima optički pristup saobraćaju u različitim čvorovima mreže.

Iz skupa optičkih kanala koji ulaze u OADM čvor mreže izdvaja se željeni kanal, a ostali saobraćaj, koji se ne izdvaja, odvija se neometano. Željeni optički kanal koji se izdvaja može da radi na različitim protocima. Postoji nekoliko generacija OADM. Prva generacija su uređaji kod kojih se dodaje ili oduzima unapred određena talasna dužina. Kod poslednjih generacije ova radna talasna dužina se može dinamički birati. Kod njih se takođe može dodati ili izdvojiti jedan ili više kanala istovremeno. Za njihovu realizaciju koriste se podesivi filtri (tankoslojni filteri, optoakustični filteri, matrične talasovodne rešetke i Bragova rešetka na bazi fibera) i laseri sa promjenljivom talasnom dužinom.

2.3.2.5 Optički kroskonektori (OXC)

Nalaze se na spojevima sa velikom gustinom saobraćaja i sprovode optičku komutaciju tipa “svako sa svakim” (imaju potpuno dostupno komutaciono polje), bilo da su u pitanju vlakna, opsezi talasnih dužina ili pojedine talasne dužine. Oni imaju veliku matricu prespajanja i dosta funkcija, od jednostavne restauracije mreža do dinamičkog upravljanja svetlosnim putevima. Njihova uloga je analogna ruterima ili ATM komutatorima. Potpuno optički OXC-ovi nemaju multipleksiranje i opsluživanje na drugim nivoima izuzev na optičkom. Oni dozvoljavaju operatorima da ponude nove servise, koji se često zovu ¨optički servisi¨.

Razlikujemo lambda komutatore, koji omogućavaju postavljanje snopa talasnih dužina duž mreže i optičke paketske komutatore, koji prosleđuju individualne optičke pakete na isti način kao što ruteri prosljeduju IP pakete. Uvođenje WDM nije pogodno samo zbog povećanja kapaciteta, već i zbog dodatnih opcija u pogledu direktnog spajanja određenih čvorova u mreži na potpuno optičkom sloju, bez dodatnih konverzija u međučvorovima.

2.3.3 VRSTE WDM

Postoje dva tipa optičkog WDM multipleksiranja, i to: CWDM (*Coarse WDM*) i DWDM (*Dense WDM*). Suštinske razlike između ova dva tipa su u gustini i broju kanala koji se multipleksiraju za prenos po jednom vlaknu, što samo po sebi, utiče na karakteristike komponenti i tehnologiju izrade. Cena po jednom kanalu je povoljnija u korist CWDM, ali ako se uzme u obzir ukupan propusni opseg kao i cena polaganja novih optičkih vlakana, na magistralnim pravcima, korišćenje DWDM sistema je neminovno.

CWDM nije konkurencija DWDM-u, ili obrnuto. Svaka od ovih tehnologija ima svoje specifične prednosti i nedostatke, zbog kojih svaka nalazi svoje mesto u različitim primenama, i vrlo često jedna drugu upotpunjavaju.

2.3.3.1 Coarse WDM

CWDM sistemi tipično koriste razmak između kanala 3.000 GHz (20 nm), odnosno 17 kanala od kojih se 16 koristi za prenos podataka, a preostali je servisni optički supervizor kanal OCS (*Optical Supervisor Channel*). Ovi kanali su raspoređeni u opsegu od 1270 do 1610 nm, a ciljna udaljenost je do 50 kilometara. Svoju primenu pronalaze u gradskim metro mrežama zbog čega je danas korišćeni CWDM standardizovan usaglašavanjem prvobitnog ITU-T G.694.2 standarda za CWDM i standardom IEEE 10GbaseLX-4.

CWDM koristi kompletan frekvencijski pojas između drugog i trećeg optičkog prozora (~1300 nm i ~1550 nm). Drugi optički prozor je područje minimalne disperzije, a treći optički prozor je područje minimalnog prigušenja, a ono što je omogućilo spajanje tih prozora jeste ZWPF (*Zero Water Peak Fiber*) koje smanjuje povećanu atenuaciju u području oko 1400 nm. ZWPF predstavlja optičko vlakno sa nultim nivoom vodenog grebena, čijim pronalaskom se rešio dugo prisutan problem prenosa u tom opsegu, a koji se odnosio na prisustvo molekula vode u optičkom vlaknu.

2.3.3.2 Dense WDM

DWDM ili tzv. gusti optički multiplekser rešava problem velikog neslaganja između ograničenog protoka koji elektronska oprema može da ponudi i značajno većeg kapaciteta koji teoretski, a sve više i praktično, nude optička vlakna. DWDM mreža dozvoljava krajnjim korisnicima da rade na brzinama elektronske opreme, zatim prikuplja veći broj takvih električnih signala i na ulazu u DWDM sistem im dodeljuje različite talasne dužine u procesu elektro-optičke konverzije. Dobijeni optički signali kombinuju se i istovremeno prenose jednim optičkim vlaknom. Pri tome je od suštinske važnosti da optičke signale na različitim talasnim dužinama, zbog njihove velike gustine, emituju laseri čije karakteristike su velika koherentnost snopa (uzak spektar) i stabilnost talasne dužine zračenja. Dakle, DWDM deli raspoloživi spektar vlakna na nepreklapajuće intervale oko talasnih dužina na kojima se vrši prenos pojedinih signala.

ITU-T standard G.694.1 definiše skup talasnih dužina za upotrebu u DWDM sistemima, međusobnog razmaka 100 GHz (0,78 nm) u opsegu od 1525 do 1565 nm, međutim proizvođačima je dozvoljeno da talasne dužine smeštaju i na manjim razmacima (50 i 25 GHz) kako bi se povećao broj kanala. Naravno, što je manje rastojanje susednih talasnih dužina u spektru, uticaj nelinearnih efekata je izraženiji, a potrebni su i kvalitetniji laseri. Već na razmaku od 50 GHz maksimalan protok po jednoj talasnoj dužini današnje opreme iznosi oko 10 Gbit/s.

Kod DWDM sistema teži se izbegavanju regeneratora kako bi se izbegla opto-električna konverzija. Regeneratori koji se koriste vrše isključivo pojačanje amplitude optičkog signala i to podjednako za sve talasne dužine. Međutim, radi izbegavanja optičkog šuma i sprečavanja izobličenja signala, upotrebom kvalitetnih lasera, rastojanja koja se postižu između regeneratora u DWDM sistemu su od 600 do 1000 km.

3. KRIPTOGRAFSKI SISTEMI

3.1 KRIPTOGRAFIJA U SAVREMENIM TELEKOMUNIKACIJAMA

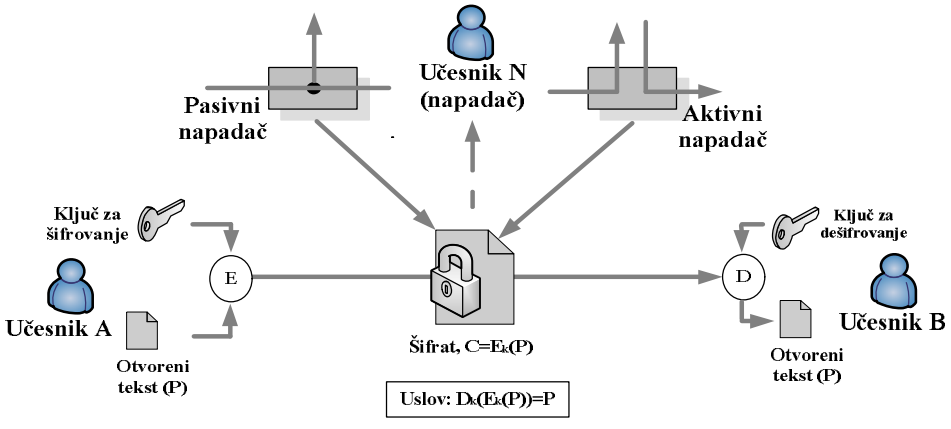
Kriptografija se bavi izučavanjem metoda očuvanja tajnosti informacija. Bilo da se radi o prenosu (ili skladištenju) ličnih, poslovnih, vojnih ili diplomatskih podataka, oni postaju ranjivi na različite pretnje i napade neželjene strane. Ti problemi se mogu izbeći tehnikama šifrovanja informacija koje njihov sadržaj čine nedostupnim za neželjenu stranu. Suprotna od kriptografije je kriptoanaliza i ona predstavlja umetnost provaljivanja šifara protivnika, dok je kriptologija nauka koja obuhvata i kriptografiju i kriptoanalizu, a bavi se matematičkim principima i matematičkom implementacijom kriptografskih i kriptoanalitičkih metoda.

3.1.1 OSNOVNI TERMINI

3.1.1.1 Šifrovanje i dešifrovanje

Na slici 11 simbolično je prikazan model kriptografskog sistema. Razlikujemo učesnike u komunikaciji koji žele bezbedno da komuniciraju i koji se mogu tretirati kao pošiljalac i primalac (označeni kao učesnik A i učesnik B), i napadača čija je namera da neovlašćeno dođe u posed tajne informacije.

Otvoreni tekst, koji pošiljalac želi da pošalje primaocu, označavamo sa M (*message*) ili sa P (*plaintext*). Za telekomunikacioni uređaj, M predstavlja bilo koji digitalni signal koji se šalje u komunikacioni kanal i koji je potrebno zaštititi.



Slika 11. Model kriptografskog sistema

Šifrat, označen sa C, takođe je digitalni signal, koji može biti iste ili veće dužine od P, što najčešće zavisi od primenjenog kriptografskog algoritma, ali je ovaj signal za napadača nerazumljiv.

Funkcija šifrovanja E, obrađuje P i daje rezultat C, $E_k(P)=C$. U obrnutom procesu, funkcija dešifrovanja D se može prikazati kao $D_k(C)=P$, a pošto je cilj dešifrovanja da se dobije originalni otvoreni tekst, mora da važi jednakost: $D_k(E_k(P))=P$. Funkcije šifrovanja i dešifrovanja i njihove međusobne zavisnosti postižu se upotrebom odgovarajućeg algoritma i ključeva.

3.1.1.2 Kritptografski algoritmi i ključevi

Kriptografski algoritam *(Cryptographic algorithm)* predstavlja spoj dve srodne matematičke funkcije koje služe za šifrovanje i dešifrovanje poruka. Postoji veliki broj algoritama, od apsolutno sigurnog (koji kao ključ koristi čisto slučajan niz iste dužine kao i poruka) pa do raznih varijanti upotrebe matematičkih operacija u kombinaciji sa ključem ograničene dužine. Kako bi algoritam bio pouzdan i praktično primenljiv, što ne važi za apsolutno sigurni algoritam, on mora ispunjavati stroge uslove koji se pred njega stavljaju u pogledu dužine ključa, brzine izvršenja i otpornosti na poznate kriptoanalitičke metode.

Na tajnosti ključa (K - *Key*) funkcioniše većina savremenih kriptografskih sistema. Ključ može imati bilo koju vrednost, a njegova osnovna namena je da se pomoću njega izvrši šifrovanje i dešifrovanje, zbog čega funkcije E i D imaju indeks K. Načini generisanja i upravljanja ključevima čine posebnu granu kriptografije koja će samo delimično biti razmatrana u nastavku.

Kriptografski sistem (*Cryptosystem*) ili šifarski sistem, predstavlja algoritam sa svim mogućim otvorenim tekstovima, šifratima i ključevima.

U pojedinim fazama razvoja kriptografije, sigurnost kriptografskih sistema se zasnivala na tajnosti algoritama, a ovaj princip je i danas ponegde prisutan. Još iz istorije je poznat Kerkofov princip po kome algoritmi moraju biti javni, a da se sigurnost sistema zasniva na tajnosti ključeva. Kerkofova hipoteza: Ako snaga vašeg kriptosistema počiva na činjenici da napadač ne zna kako vaš algoritam funkcioniše – propali ste. Ukoliko verujete da će tajnost strukture vašeg algoritma povećati sigurnost vašeg kriptosistema više nego slobodna analiza akademske zajednice, varate se. Ukoliko mislite da niko neće rastaviti vaš izvorni kod i obrnutim procesom (reverznim inženjeringom) detaljno proučiti vaš algoritam, naivni ste [1]. Pojedini teoretičari tajne algoritme nazivaju ograničenim algoritmima. Smatra se da su njihove loše strane: nemogućnost implementacije u velikim grupama korisnika, ograničen razvoj i implementacija algoritma na okvire grupe koja ga koristi, otežana kontrole kvaliteta i standardizacija, potreba za čestim promenama samog algoritma itd. Međutim, pojedini zatvoreni profesionalni sistemi u kojima se navedeni nedostaci strogim merama mogu prevazići i dalje algoritme čuvaju u tajnosti.

3.1.2 ISTORIJAT I NAMENA KRIPTOGRAFIJE

U davnoj istoriji prve kriptografske tehnike pojavile su se onog trenutka kada je pismo postalo sredstvo komunikacije. Od samog početka, šifrovanje podataka koristilo se prvenstveno u vojne svrhe. Među prvim vojskovođama koji su koristili šifrovane poruke pominje se Julije Cezar. Njegovo poznato šifrovanje zasnivalo se na pomeranju pojedinih ili svih slova u tekstu za određen broj mesta u abecedi. S obzirom da je korišćena za čuvanje vojnih i nacionalnih tajni, kriptografija je tokom istorije imala bitan uticaj na ishode mnogih ratova uključujući i oba svetska rata. Upravo iz tog razloga, iako nikada nije postojala zvanična zabrana, literatura iz ove oblasti skoro da nije objavljivana sve do 1960-ih godina. To ne znači da se daleko od očiju javnosti nisu otkrivale nove tehnike za šifrovanje, a s druge strane za kriptoanalizu. Borba između tvoraca kriptografskog sistema i napadača (kriptoanalitičara) zapravo je uvek prisutna i nikada se neće završiti. Cilj savremenih kriptografskih algoritama je da se bude korak do dva ispred napadača.

Pojavom i razvojem elektronskih komunikacija, kriptografija dobija novu dimenziju i potreba za njom postaje sve veća. Danas je upotreba savremenih informaciono komunikacionih tehnologija (IKT) u većini društvenih sfera nezamisliva bez kriptografske zaštite podataka, a postoje brojni proizvodi koji omogućavaju jednostavnu upotrebu kriptografije, čak i za lične potrebe. Ogroman broj elektronskih komunikacija u svakodnevnom životu, bilo da se radi o razmeni elektronske pošte između poslovnih partnera, korišćenju usluga elektronskog bankarstva ili pak o zaštiti tajnih informacija značajnih za bezbednost zemlje, bitno je te podatke zaštititi od neovlašćenog pristupa. Da bi se to postiglo, podaci se postupkom šifrovanja, modifikuju u drugi, za napadača nerazumljiv oblik, tako da ukoliko dođe u posed podataka u toku prenosa, neće uspeti da ih protumači. Postupak modifikacije, odnosno šifrovanja podataka definisan je posebnim algoritmima, o kojima će kasnije biti više reči. U savremenim komunikacijama, najčešće se koriste javno dostupni (komercijalni) algoritmi, a sigurnost sistema se zasniva na njihovom kvalitetu i tajnosti ključeva.

Međutim, javnost kriptografskih algoritama i njihova dostupnost običnim ljudima ne znači da vodeće nacionalne agencije zadužene za zaštitu informacija danas u svetu, i dalje ne skrivaju najnovija otkrića u ovoj oblasti, posebno ona koja se tiču kriptoanalize. Pretpostavlja se da su današnja kriptološka znanja američke agencije NSA (*National Security Agency*) u pogledu algoritama i protokola mnogo godina ispred trenutnog stanja poznatog javnosti i nesumnjivo su dovoljna za provaljivanje mnogih sistema koji se danas koriste u praksi [1]. Otuda potreba da se u pojedinim profesionalnim sistemima, posebno u državnim institucijama, i pored primenjenih svih mera za zaštitu tajnosti ključeva, algoritmi ipak čuvaju u tajnosti.

Namena kriptografije, u opštem slučaju, je da se ostvari tajnost i nepromenljivost podataka u toku prenosa, da se može ustanoviti identitet druge strane i da obe strane znaju da se sadržaj komunikacije ne može poreći. Iz njene namene proizilaze četiri osnovne funkcije ili cilja kriptografije:

- Poverljivost (*confidentiality*) ili tajnost, predstavlja obezbeđivanje da sadržaj informacije bude dostupan samo ovlašćenim stranama, odnosno samo onima koji poseduju ključ. Često se sama kriptografija poistovećuje sa ovom funkcijom, što je međutim pogrešno. Ponekad se za poverljivost koriste i termini tajnost ili privatnost.
- Integritet podataka (*data integrity*), znači osiguravanje nepromenljivosti od strane neovlašćenih lica u toku prenosa. Da bi se osiguralo da učesnici u komunikaciji znaju da su podaci koje razmenjuju dostupni samo njima i da su nepromenjeni, neophodno je obezbediti otkrivanje bilo kakve promene podataka koje može biti dodavanje, uklanjanje ili promena podataka. Takođe je potrebno obezbediti razliku između promena usled napada neovlašćenih lica i nenamernih grešaka pri prenosu.
- Autentifikacija (*authentication*) je vezana za identifikaciju učesnika u komunikaciji i same informacije. Elementi autentičnosti informacije su njeno poreklo, vreme nastanka i vreme slanja. Autentifikacija se može podeliti na autentifikaciju entiteta i autentifikaciju porekla podataka. Ova funkcija obezbeđuje da se učesnici u komunikaciji, pre razmene informacija „predstave“ jedan drugom.
- Neporecivost (*non-repudiation*) onemogućava negiranje učešća u komunikaciji kao i sadržaja komunikacije od strane učesnika. Sa aspekta razmene informacija, ovo znači da ni jedna strana ne može poreći svoje učešće u razmeni kao i sadržaj razmenjenih informacija.

Postoje različite metode kojima se ostvaruju neke ili sve četiri funkcije kriptografije. Njene funkcije nisu vezane za tipove kriptografije, simetrični ili asmetrični. Oba tipa mogu pružiti sve navedene funkcije.

3.1.3 ANALIZA PRETNJI I NAPADA

Napadi na kriptografski sistem predstavljaju tehnike kriptoanalize. Kriptoanaliza je upravo suprotna kriptografiji i bavi se razbijanjem šifri, tj. otkrivanjem postupaka za dolazak do otvorenog teksta bez poznavanja tajnih podataka. Najčešće se svodi na provaljivanje tajnog ključa.

Prilikom procene pretnji i napada na sigurnost sopstvenog telekomunikacionog sistema, potrebno je proceniti napadača na osnovu sledećih parametara:

- Stepen poverljivosti i vreme aktuelnosti sopstvenih zaštićenih informacija,
- Javnost sopstvenog algoritma,
- Preispitivanje sopstvenih rešenja,
- Praćenje statističkih informacija iz javno dostupnih izvora,
- Identifikacija napadača,
- Motivi napadača,
- Procesorske moć napadača,
- Pretpostavke o dekripterskim mogućnostima napadača.

Pri proceni napadača, takođe je neophodno znati, da svaki ozbiljan napadač svoje sposobnosti čuva u strogoj tajnosti, a da se povećanjem procesorske moći računara i primenom najnovijih naučnih dostignuća iz oblasti kriptoanalize, mogućnosti dekriptovanja konstantno povećavaju. Postoje četiri opšta tipa kriptoanalitičkih napada u zavisnosti od informacija koje napadač poseduje o kriptografskom sistemu:

- Napad "samo šifrat" (C*iphertext-only attack*). Kriptoanalitičar ima šifrate nekoliko poruka šifrovanih istim algoritmom za šifrovanje. Zadatak mu je da rekonstruiše otvoreni tekst što većeg broja poruka, ili da otkrije ključ (ili ključeve) korišćene za šifrovanje poruka kako bi dešifrovao druge poruke šifrovane istim ključem (ili ključevima).
  Poznato: $C_1 = E_k(P_1)$, $C_2 = E_k(P_2)$, ... $C_i = E_k(P_i)$
  Izračunati: Ili P_1, P_2, ... P_i; k; ili algoritam
  da bi se dobilo P_{i+1} iz $C_{i+1} = E_k(P_{i+1})$
- Napad "poznat otvoreni tekst" (*Known-plaintext attack*). Kriptoanalitičar ima pristup šifratima za nekoliko poruka, kao i otvorenim tekstovima tih poruka. Njegov posao je da izračuna ključ (ili ključeve) korišćen za šifrovanje poruka, ili algoritam, kako bi dešifrovao svaku novu poruku šifrovanu istim ključem (ili ključevima).
  Poznato: P_1, $C_1 = E_k(P_1)$, P_2, $C_2 = E_k(P_2)$, ... P_i, $C_i = E_k(P_i)$
  Izračunati: Ili k, ili algoritam da bi se dobilo P_{i+1} *iz* $C_{i+1} = Ek(P_{i+1})$
- Napad "odabrani otvoreni tekst" (*Chosen-plaintext attack*). Kriptoanalitičar ne samo da ima pristup šifratu i pripadajućem otvorenom tekstu nekoliko poruka, već i bira otvoreni tekst koji će biti šifrovan. Ovakav napad je mnogo moćniji od napada "poznat otvoreni tekst", jer kriptoanalitičar može da odabere specifične blokove otvorenog teksta za šifrovanje i tako dođe do više informacija o ključu.
  Poznato: P_1, $C_1 = E_k(P_1)$, P_2, $C_2 = E_k(P_2)$, ... P_i, $C_i = E_k(P_i)$,
  gde kriptoanalitičar odabira P_1, P_2, ... P_i
  Izračunati: Ili k, ili algoritam da bi se dobilo P_{i+1} iz $C_{i+1} = E_k(P_{i+1})$
- Napad "prilagodljiv odabrani otvoreni tekst" (*Adaptive-chosen-plaintext attack*) predstavlja posebnu vrstu napada "odabran otvoreni tekst" u kome napadač može čak i da modifikuje ono što je odabrao za šifrovanje, a na osnovu rezultata prethodnih šifrovanja. Kod napada "odabran otvoreni tekst", napadač odabira za šifrovanje blok otvorenog teksta dok kod ovog napada on ima mogućnost da odabere manji blok otvorenog teksta, a zatim još jedan na osnovu rezultata šifrovanja prvog, i tako dalje.

Sa aspekta primenjene kriptoanalitičke tehnike, u literaturi se najčešće pominju tri metode: linearna kriptoanaliza, diferencijalna kriptoanaliza i napad grubom silom.

Jedan od osnovnih postulata kriptografije i kriptoanalize glasi da ne postoji apsolutno siguran praktično primenljiv algoritam, već je samo pitanje vremena i sredstava koja su napadaču potrebna za probijanje.

Vrste napada na sigurnost telekomunikacionog sistema, najbolje se mogu ilustrovati modelom, u kome su izvorišni i odredišni uređaji međusobno povezani komunikacionim kanalom. Podrazumevano je da je komunikacioni kanal nebezbedna sredina.

Sa stanovišta pretnji i napada na sigurnost kriptografskog sistema namenjenog za zaštitu podataka u optičkim telekomunikacionim mrežama, napade u najširem smislu možemo podeliti na pasivne i aktivne. Pasivnim napadima se samo prisluškuje poslata poruka i takve napade je veoma teško detektovati. Aktivni napadi uključuju i menjanje sadržaja poruke, maskiranje i ometanje (poznatije kao DoS – *Denial of Service* napad). Da li će napadač primeniti aktivni ili pasivni napad, zavisi od posedovanja opreme za prisluškivanje i obmanjivanje, vrste kriptoanalitičkog napada za koji poseduje kriptoanalitička znanja i niza drugih faktora.

Najčešće korišćeni napadi, kada su u pitanju optičke telekomunikacione mreže su:

- Prisluškivanje optičkog vlakna, može se izvršiti direktnim priključenjem ili punktiranjem optičkog vlakna. Kako bi napadač priključio prislušnu opremu, koja je inače na tržištu sve dostupnija, potrebno je da zaštitni omotač optičkog vlakna ukloni hemijskim rastvorima, a zatim umetne sondu u samo vlakno preko koje je moguće pristupiti svim informacijama koje se prenose. Ovakve napade je skoro nemoguće detektovati na krajevima optičkog vlakna. Prisluškivanjem optičkog vlakna napadač može doći do neograničenog broja šifrata, a u slučaju nedoslednog preduzimanja kriptografskih mera, i do otvorenih tekstova.
- Napad na pojedine mrežne elemente optičke mreže (SDH ADM (*Add/Drop Multiplexing)* multiplekser, optički (OADM) multiplekser, optički kros konektor (OXC) ili optički pojačavač), koji se obično štite fizičkim metodama zaštite. Ako u primeni fizičkih metoda zaštite postoje propusti, napadač može pristupiti portovima i korisničkim podacima tj. otvorenom tekstu i tako, u kombinaciji sa prisluškivanjem, stvoriti idealne uslove za napad „odabrani otvoreni tekst“ ili „prilagodljiv odabrani otvoreni tekst“. U sklopu ovih napada može se nalaziti i napad prevarom ili ucenom, koje napadač preduzima koristeći ranjivost ljudskog faktora. Time stvara uslove za prikupljanje što više tajnih informacija o kriptografskom sistemu i efikasniju kriptoanalizu.

Iz navedenog se može zaključiti da postoje određene ranjivosti optičkih telekomunikacionih mreža tj. njihovih komponenti, a da su mogući brojni napadi i oblici ugrožavanja njihove sigurnosti. Detekcija napada je ograničena. U nastavku će biti izneti načini sprečavanja i kriptografske tehnike za zaštitu podataka od pojedinih napada.

3.2 KRIPTOGRAFSKI ALGORITMI

Postoje dva opšta tipa kriptografskih sistema zasnovanih na kriptološkim ključevima na osnovu kojih njihovi algoritmi izvršavaju funkcije šifrovanja i dešifrovanja: simetrični i asimetrični ili sistemi sa javnim ključem. Pre osnovnih postulata o kriptografskim sistemima, biće objašnjeni principijalni načini organizacije učesnika u telekomunikacionoj mreži sa aspekta zaštite.

3.2.1 TIPOVI ZAŠTIĆENIH KOMUNIKACIJA

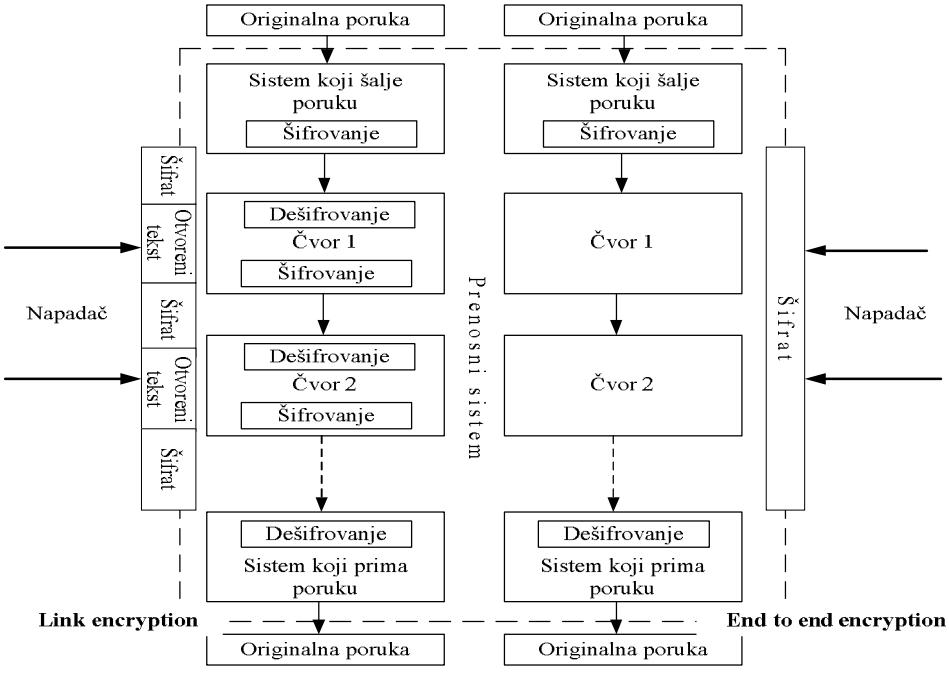
Zavisno od mesta postavljanja kriptomodula u odnosu na komunikaciione kanale i organizacije ključeva u mreži, načini zaštite u optičkim telekomunikacionim mrežama mogili bi se svrstati u dve grupe:

- Zaštita linkova (*link encryption*) i
- Zaštita sa kraja na kraj (*end to end encryption*).

3.2.1.1 Link encryption

Link encryption (slika 12) je pristup u kome se šifruje kompletan saobraćaj na linkovima između pojedinih tačaka mreže. Šifrovanje se vrši u nezavisnim uređajima koji se povezuju između mrežnog telekomunikacionog uređaja i linije. Na svakom linku koristi se različit ključ. Koristi se u sistemima koji su u neprekidnom radu. Obezbeđena je automatska resinhronizacija, kako zbog periodične promene radnih kriptoloških parametara tako i zbog eventualnih prekida u šifrovanju i u komunikacionom kanalu. Šifrovanje se realizuje na prvom i drugom sloju OSI (*Open Systems Interconnection*) referentnog modela. Zbog šifrovanja kompletnog saobraćaja (uključujući i hedere), obezbeđeno je da napadač ne može pratiti rutiranje saobraćaja, što bitno smanjuje njegove argumente za kriptoanalizu. Ovaj tip se još zove i kontrola toka sobraćaja.

Dobre osobine *link encryption* su transparentnost sistema za korisnike i jednostavnija distribucija kriptoloških ključeva, a negativno je to što se do informacija u međučvoromima mreže može doći u potpuno otvorenom obliku i što je neophodno obezbediti zaštitu na svim linkovima mreže jer bi nezaštićeni delovi mreže ugrožavali bezbednost kompletnog sistema. Samim tim cena sistema zaštite se povećava.



Slika 12. Tipovi zaštite komunikacija

3.2.1.2 End to end encryption

Kod ovog načina šifrovanje se vrši na kompletnom prenosnom putu između dve tačke mreže (slika 12) koje razmenjuju tajne informacije. Postupak je isti bez obzira na broj međučvorova u mreži. Šifrovanje se izvršava na višim slojevima OSI modela, a servisne infromacije i hederi se ne šifruju.

Prednosti *end to end encryption* su što se informacija na spojnom putu ne dešifruje pre odredišta, tj. nisu dostupne u međučvorovima u otvorenom obliku i što je obezbeđeno da svaki od učesnika ima različite ključeve za drugog učesnika. Glavni nedostatak ovog načina šifrovanja je što se delovi tajne informacije koji se odnose na rutiranje ne smeju šifrovati čime je napadaču obezbeđeno da vrši analizu saobraćaja, što mu znatno pomaže u kriptoanalizi. Kombinacija oba tipa šifrovanja (*link encryption i end to end*) rešila bi sve navedene nedostatke. Administratori mreže bili bi zaduženi za *link encryption,* dok bi *end to end* bio poveren krajnjim korisnicima.

3.2.2 SIMETRIČNI KRIPTOGRAFSKI ALGORITMI

3.2.2.1 Principi simetrične kriptografije

Kod simetričnih kriptografskih sistema dve strane bezbedno komuniciraju tako što poruke šifruju i dešifruju identičnim ključem. Protokol koji mora biti izvršen je sledeći:

- Korak 1: Učesnici A i B se dogovaraju o algoritmu,
- Korak 2: Učesnici A i B se dogovaraju o ključu,
- Korak 3: Učesnik A, pomoću algoritma i ključa, šifruje poruku (otvoreni tekst) i dobija šifrat,
- Korak 4: Učesnik A šalje šifrat učesniku B,
- Korak 5: Učesnik B dešifruje šifrat i dobija originalnu poruku (otvoreni tekst).

Treća, neovlašćena strana C ili napadač, sve vreme prati komunikaciju učesnika i preduzima adekvatne napade. Ukoliko, na primer, napadač prisluškivanjem dođe do informacija iz koraka 2, a algoritam je javan, preostaje mu samo da posle uhvaćenog šifrata u koraku 4, izvrši dešifrovanje. Napadač C bi mogao da preduzme i druge - aktivne napade, recimo da pre koraka 4 prekine komunikacioni kanal i onemogući da učesnik B uopšte primi šifrat. Ili da presretne šifrat, poslat od učesnika A, zameni ga sopstvenim, koji pošalje učesniku B. Ukoliko bi imao ključ do kog je došao prisluškivanjem u koraku 2, napadač bi mogao da obmane učesnika B svojom porukom, jer on ne bi imao načina da utvrdi da poruku nije poslao učesnik A. Iz ovih razloga veoma je bitno da se korak 2 obavi u tajnosti, tj. da napadač ne sme doći u posed ključa.

Pored problema sa očuvenjem tajnosti ključa, drugi veliki problem simetričnih kriptografskih sistema je brz rast broja potrebnih ključeva sa rastom broja učesnika. Ako se pretpostavi da svaki par učesnika u mreži upotrebljava poseban ključ, za mrežu od *N* učesnika potrebno je *N(N-1)/2* ključeva (npr. za 100 učesnika potrebno je 4950 ključeva). Upravljanje ključevima i način distribucije ključeva u simetričnim kriptografskim sistemima, zbog toga zauzimaju centralno mesto.

Simetrične kriptografske sisteme možemo podeliti u dve grupe:

- Sekvencijalni (*stream*) su sistemi sa algoritmima koji deluju na jedan bit ili bajt, tj. kod kojih se kriptografska transformacija obavlja na svakoj jediničnoj informaciji otvorenog teksta. Pogodni su za upotrebu u lošim uslovima prenosa jer nemaju propagaciju greške, koriste se za rad u realnom vremenu (npr. zaštita govora) i najčešće se realizuju hardverski. Generalno su manje u upotrebi od blokovskih sistema.
- Blokovski sistemi transformišu otvoreni tekst u šifrovani po blokovima jednake dužine. Šifrat se dobija iz bloka otvorenog teksta višestrukom primenom funkcije koja se naziva runda, a ulazni parametri su ključ, koji je takođe fiksne dužine, i izlaz iz prethodne runde.

Svi simetrični algoritmi, u osnovi, obavljaju dve operacije: supstituciju (zamenjivanje) i transpoziciju (premeštanje) nad elementima otvorenog teksta. Šifre supstitucije svaki element otvorenog teksta (slovo, bit, bajt i sl.) preslikavaju u različit element šifrata zavisno od ključa, dok transpozicione šifre vrše preuređenje elemenata po datom ključu u okviru otvorenog teksta i to tako što ih najpre podele na podjednake blokove. I jedne i druge su, ako se samostalno koriste, slabe jer zadržavaju statističke karakteristike jezika. Stariji algoritmi koristili su jednu od ove dve osnovne operacije, dok savremeniji kombinuju obe i to ponavljajući ih više puta. Teorijsko tumačenje ovih operacija dao je Shanon. On je ukazao da su one vezane za tehnike za prikrivanje redundantnosti u otvorenom tekstu koja se koristi u kriptoanalizi. Te tehnike su difuzija i konfuzija. Difuzija razuđuje redundantnost otvorenog teksta raširijući je po šifratu. Ona se postiže postupcima kojima se statistička struktura otvorenog teksta skriva tako što se uticaj jednog bita otvorenog teksta prenosi na što više bitova šifrata. Samim tim, male promene u bloku otvorenog teksta (npr. 1 bit) moraju da izazovu nepredvidive promene u bloku šifrata. Konfuzija prikriva vezu između otvorenog teksta i šifrata, odnosno čini je što je moguće kompleksnijom (jer je tu vezu nemoguće ukloniti). Svojstvo konfuzije podrazumeva da prilikom napada potpunom pretragom ključeva, svi ključevi treba da budu približno jednako verovatni. Ovim tehnikama se, dakle otežava kriptoanaliza zasnovana na redundantnosti i statističkim osobinama jezika. U savremenim kriptografskim sistemima principijalna kombinacija difuzije i konfuzije je obavezna.

Dobar kriptografski algoritam treba da ispuni najmanje jedan od sledeća dva uslova:

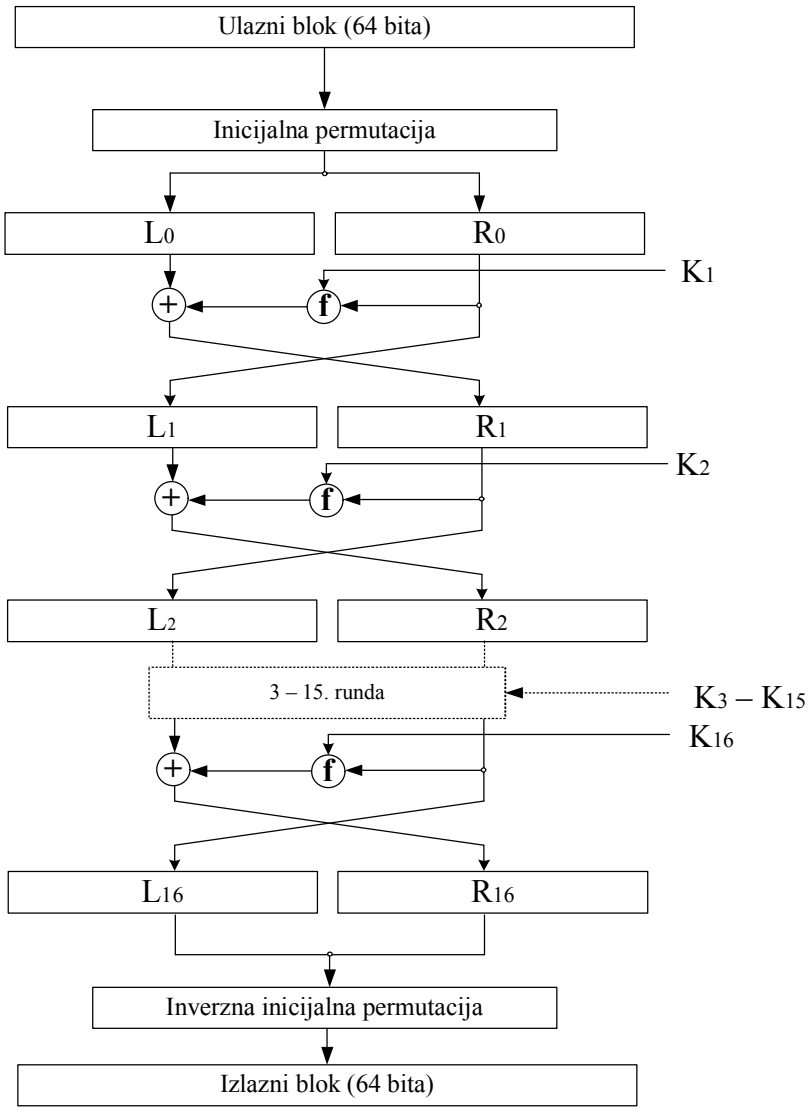
- Cena razbijanja šifrata teksta prevazilazi cenu poruke koju isti nosi ili
- Vreme koje je potrebno za razbijanje šifrata je duže od vremena važenja tajne informacije u otvorenom tekstu.

Pri projektovanju kriptografskog sistema treba voditi računa i o tome da algoritam bude praktično primenjljiv tj. da ne bude samo otporan na kriptoanalitičke napade već i relativno jednostavan za korišćenje.

3.2.2.2 DES

DES (*Data Encryption Standard*) je od najpoznatijih i najraširenih simetričnih algoritama. Iako danas nije u upotrebi u svom izvornom obliku, postoje mnogi algoritmi bazirani na DES-u. Razvijen je sedamdesetih godina u IBM-u, a 1977. godine prihvaćen od američke vlade kao standard za zaštitu podataka, od kada je u masovnoj upotrebi.

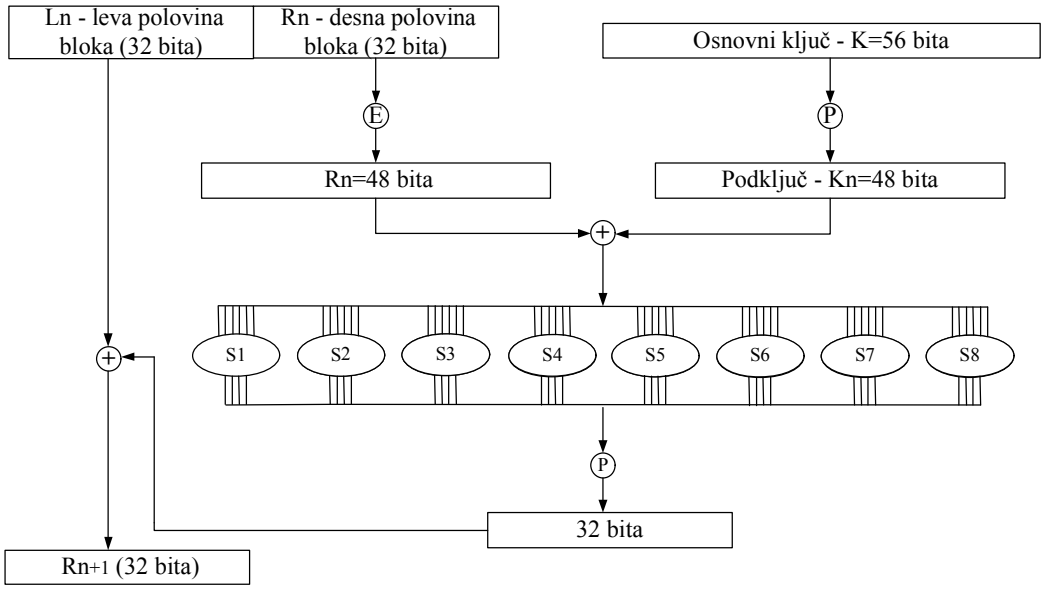
DES šifruje otvoreni tekst u blokovima dužine 64 bita sa ključem k dužine 56 bita, čime se dobija šifrat dužine 64 bita. Tri su osnovna koraka u algoritmu (slika 13): inicijalna permutacija (IP), 16 rundi obrade podataka (proširenje, XOR sa podključem, supstitucija), završna inverzna permutacija (IP^{-1}).



Slika 13. Algoritam DES

Posle IP, koja menja raspored bita u ulaznom bloku po unapred određenoj tablici, blok se deli na levu i desnu polovinu (po 32 bita). Zatim se na ta dva podbloka primenjuje funkcija *f* u 16 rundi, u kojima se podaci kombinuju sa ključem.

Operacije jedne runde su sledeće (slika 14): Bitovi ključa se pomeraju u odnosu na prethodnu rundu, a zatim se bira 48 od 56 bitova ključa koji će biti korišćeni. Na taj način se dobija 16 podključeva (u svakoj rundi po jedan). Desna polovina podataka proširuje se sa 32 na 48 bitova preko fiksne permutacije proširenja, kombinuje sa 48 bitova pomerenog i permutovanog ključa pomoću operacije XOR, šalje kroz 8 S-kutija, što daje 32 nova bita, i ponovo se permutuje.



Slika 14. Operacije u jednoj rundi DES

Permutacija proširenja (*expansion permutation*), ili E-kutija, koja proširuje desnu polovinu podataka (u svakoj rundi) time što menja redosled bitova i ponavlja određene bitove, ima dve svrhe: 1) da desnu polovinu dovede na veličinu ključa i 2) da se time dobije duži rezultat koji može da se komprimuje za vreme operacije supstitucije. Omogućavajući da jedan bit utiče na dve supstitucije, zavisnost izlaznih bitova od ulaznih brže se širi, čime se postiže tzv. efekat lavine.

Supstitucija pomoću S-kutija *(supstitution boxes)* obavlja se nakon što se na komprimovani ključ i prošireni blok primeni operacija XOR. Svaka S-kutija ima 6-bitni ulaz i 4-bitni izlaz, a postoji 8 S-kutija u koje ulazi osam 6-bitnih podblokova ulaznog 48-bitnog bloka. Svaka S-kutija ima 4 reda i 16 kolona. Ulazni bitovi definišu jedan element u S-kutiji na način da se kombinuju 1. i 6. bit i daju 2-bitni broj (od 0 do 3) koji odgovara jednom redu tabele, a kombinovani 2-5 ulazni bit daju 4-bitni broj (od 0 do 15) koji odgovara jednoj koloni tabele. Broj na datoj poziciji S-kutije (dobijenoj ukrštanjem) predstavlja izlazni 4-bitni podblok. Osam S-kutija daje osam 4-bitnih blokova čijom se kombinacijom dobija izlazni 32-bitni blok. Supstitucija pomoću S-kutija najznačajniji je korak DES-a jer je jedina nelinearna operacija u algoritmu zbog čega se njegova sigurnost, najviše zasniva na ovoj operaciji.

Permutacija pomoću P-kutije predstavlja pravu permutaciju, bez komprimovanja ili proširenja. Permutacijom ulaznog 32-bitnog bloka dobija se izlazni blok iste dužine.

Ove četiri operacije čine funkciju *f*. Izlaz funkcije *f* se kombinuje sa levom polovinom podataka pomoću još jedne operacije XOR. Rezultat ove operacije postaje desna polovina za sledeću rundu, a stara desna polovina postaje nova leva.

Nakon 16 rundi izvršava se IP^{-1} koja je inverzna permutaciji IP, a njom se obezbeđuje da se isti algoritam koristi i za šifrovanje i za dešifrovanje.

Dešifrovanje DES vrši se potpno istim algoritmom, s tim što se podključevi koriste obrnutim redosledom od šesnaestog do prvog.

Ciljevi koji su postignuti DES-om su sledeći:

- Šifrat zavisi od otvorenog teksta i ključa na složen način (princip konfuzije),
- Svaki bit šifrata je funkcija svkog bita otvorenog teksta i ključa (princip difuzije) i
- Efekat lavine, tj. male promene ulaza izazivaju velike promene u izlazu. Promena jednog bita ključa ili jednog bita otvorenog teksta u 64-bitnom bloku menjaju 50% izlaza tj. šifrata.

Međutim, izazovi koje je godinama pred kriptoanalitičare postavljao DES, postali su dostižni krajem devedesetih godina kada su objedinjene grupe EFF (*Electronic Frontier Foundation*) i *Distributed.net*, uz pomoć 100.000 PC računara na Internetu, probili DES metodom "napad грубом силом" za 22 sata i 15 minuta. Pritom je brzina pretraživanja bila 245 biliona ključeva u sekundi.

3.2.2.3 Triple DES

Višestruki DES podrazumeva da se algoritam ponavlja više puta ali sa različitim 56-bitnim ključevima. Najpoznatija realizacija višestrukog DES-a je *Triple* DES u kojoj se jedan blok otvorenog teksta obrađuje tri puta sa dva ključa: prvo se šifruje sa prvim ključem, zatim dešifruje sa drugim ključem i najzad ponovo šifruje sa prvim ključem. Primalac dešifruje sa prvim, šifruje sa drugim i konačno dešifruje sa prvim. Ovim se rešava problem dužine ključa kod standardnog DES-a i time udvostručava broj kombinacija koje bi napadač "grubom silom" morao da pretraži da bi došao do ključa. Ali *Triple* DES sa sobom nosi novi problem, a to je brzina; dva do tri puta je sporiji od DES-a, zbog čega je i bio privremeno rešenje nakon razbijanja standardnog DES-a, a pre izbora novog standarda.

3.2.2.4 AES

NIST (*National Institute of Standards and Technology*) je 1997. raspisao konkurs za kriptografski sistem koji će zameniti DES sa sledećim uslovima:

- Simetrični blokovski algoritam sa javnim kodom,
- Podržavanje veličine bloka od minimalno 128 bita i
- Podržavanje veličine ključa od 128, 192 i 256 bita.

Pobednik konkursa algoritam RIJNDAEL, belgijskih kriptografa Joana Daemena i Vincenta Rijmena, karakterističan po tome što pri konstrukciji supstitucijskih kutija koristi operacije u konačnom polju Galoa GF (2^8), modifikovan je 2000. godine i nazvan AES (*Advanced Encryption Standard),* a od novmbra 2001 i zvanično zamenjuje DES. NIST tada procenjuje da bi računaru koji bi mogao da probije 56-bitni DES "grubom silom" u jednoj sekundi, bilo potrebno približno 149 triliona godina za razbijanje 128-bitnog AES ključa.

Osnovne karakteristike algoritma su:

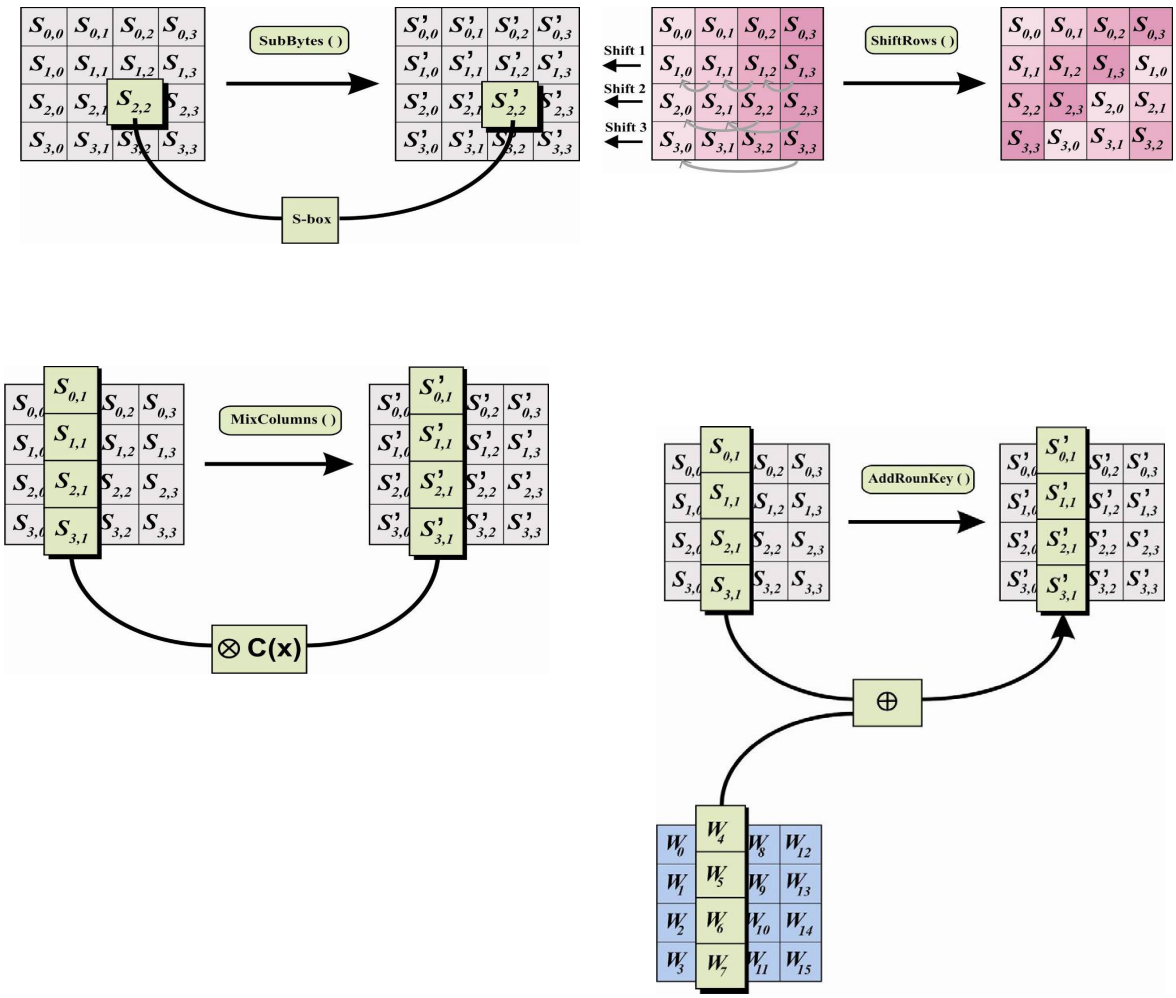
- Promenljiva veličina bloka otvorenog teksta (128, 192 ili 256 bitova),
- Promenljiva dužina ključeva (128, 192 ili 256 bitova) i
- Broj rundi promenljiv i zavisi od veličine bloka i dužine ključa.

U nastavku će biti data logička interpretacija rada algoritma sa 128-bitnim ulaznim blokom i 128-bitnim ključem. Šifrovanje podataka obavlja se iz više rundi, čiji broj zavisi od veličine ulaznog bloka i dužine ključa, a može biti 10, 12 ili 14 (u našem slučaju 10). Ulazni 128-bitni blok otvorenog teksta se deli u 4 grupe od po 4 bajta na osnovu kojih se formira dvodimenzionalna matrica ulaznih bajtova. Na osnovu matrice ulaznih bajtova formira se matrica stanja. Sve operacije koje se dalje obavljaju izvode se nad matricom stanja. Broj redova matrice stanja *r* je fiksan (četiri reda), što znači da svaka kolona ima ukupno 32 bita, a broj kolona matrice zavisi od veličine bloka po sledećem: $0<c<N_b$, gde je *c* broj kolona, a N_b dužina bloka u bitovima podeljena sa 32.

U svkoj od prvih 9 rundi (u desetoj rundi se preskače treća operacija), nad elementima matrice stanja izvršavaju se sledeće četiri operacije, koje su ilustrovane na slici 15:

- Zamena bajtova (*ByteSub*), je operacija supstitucije koja se obavlja nad svakim bajtom iz matrice stanja tako što se svaki element menja sa elementom iz pomoćne *lookup* tabele odnosno *S-box-a*.
- Pomeranje bajtova (*ShiftRow*), operacija se odnosi na pomeranje elemenata (bajtova) u okviru redova za određeni broj pozicija. Prvi red ostaje nepromenjen, dok se u svakom sledećem bajtovi pomeraju kružno ulevo, i to: drugi red za po jedno mesto, treća za po dva mesta ulevo, a četvrti za po tri mesta.
- Mešanje podataka u kolonama (*MixColumn*), je operacija koja koristi određenu linearnu transformaciju nad svakom kolonom iz matrice stanja. Obavlja se operacija množenja sa konstantom *C(x)*. Svaka kolona se tretira kao polinom u Polju Galoa GF(2^8) i množi sa nesvodljivim fiksnim polinomom $C(x)=3x^3+x^2+x+2$.
- Dodavanje podključa (*AddRoundKey*), operacija se odnosi na XOR operaciju nad matricom stanja i matricom ključeva.

U većini slučajeva sa navedenim dužinama ključeva AES zadovoljava bezbednosne zahteve, a činjenica da se temelji na Rijndeal algoritmu koji omogućava korišćenje i dužih ključeva od 256 bitova, otvara perspektive AES-a. Otpornost AES-a na linearnu i diferencijalnu kriptoanalizu ukazuje na to da se pri njegovoj izradi posebna pažnja posvetila činjenici da sve moguće strategije napada imaju očekivano vreme trajanja i memorijske zahteve.



Slika 15. Runda AES-a

3.2.2.5 Ostali simetrični algoritmi

Postoji više DES baziranih algoritma, a najčešće korišćeni su: DES sa nezavisnim podključevima, DESX, Crypt (3), Generalizovani DES, DES sa izmenljivim S-kutijama, RDES, s*nDES i DES sa S-kutijama zavisnim od ključa. Sve navedene varijante rezultat su pokušaja da se neutrališu slabosti standardnog algoritma DES, prvenstveno da se izvrši produženje ključa, da se S-kutije organizuju i isprojektuju na drugačiji način ili da se umetnu dodatne operacije koje otežavaju napade poznatim kriptoanalitičkim metodama.

Zanimljivo je da je uslove za AES konkurs, ispunilo 15 algoritama, a u uži krug pored Rijndaela ušlo još 4 algoritama: Twofish, RC6, Mars i Serpent.

Takođe često korišćeni simetrični algoritmi su i: IDEA, Blowfish, Mydriga, NewDES, FEAL, REDOC, LOKI i drugi.

3.2.2.6 Režimi rada simetričnih algoritama

Režim rada algoritma predstavlja način upotrebe bazičnog kriptografskog algoritma i najčešće je kombinacija neke vrste povratne sprege i određenih jednostavnih operacija. Operacije koje se primenjuju nad algoritmom su jednostavne jer je bezbednost određena bazičnim algoritmom a ne režimom rada. Postoji više režima rada u kojima mogu raditi simetrični algoritmi, a najčešći su:

- ECB (*Electronic Code Book mode*), otvoreni tekst se deli na blokove određene dužine, a poslednji blok se dopunjava slučajno generisanim nizom. Šifrovanje se obavlja blok po blok pomoću istog ključa. Kod ovog režima identični blokovi otvorenog teksta uvek daju identične šifrate.
- CBC (*Cipher Block Chaining*) ili režim ulančavanja blokova. Najpre se računa rezultat XOR operacije izvršene nad trenutnim blokom otvorenog teksta i šifratom prethodnog bloka, a zatim se rezultat šifruje ključem, čime se ostvaruje povratna sprega, tako da istim blokovima otvorenog teksta odgovaraju različiti blokovi šifrata, a blok šifrata je zavisan od tekućeg i svih prethodnih blokova otvorenog teksta.
- CFB (*Cipher Feedback Mode*) ili režim povratnog šifrovanja. U nekim varijantama javlja se potreba da se delovi otvorenog teksta šifruju i prenose u jedinicama veličine *r* bita (r < veličina bloka), što u CBC režimu nije moguće. Ovim modom se prevazilazi osnovni problem CBC režima - da šifrovanje i prenos podataka ne mogu početi sve dok se ne primi kompletan blok podataka. Koristi se i u sekvencijalnim algoritmima.
- OFB (*Output Feedback Mode*) ili izlazni povratni režim. Ovaj način rada predstavlja spoj dobrih osobina ECB i CFB režima, sprečava propagaciju greške i ima poboljšane bezbednosne karakteristike. OFB mod rada takođe omogućava prenos podataka u jedinicama manjim od veličine bloka.

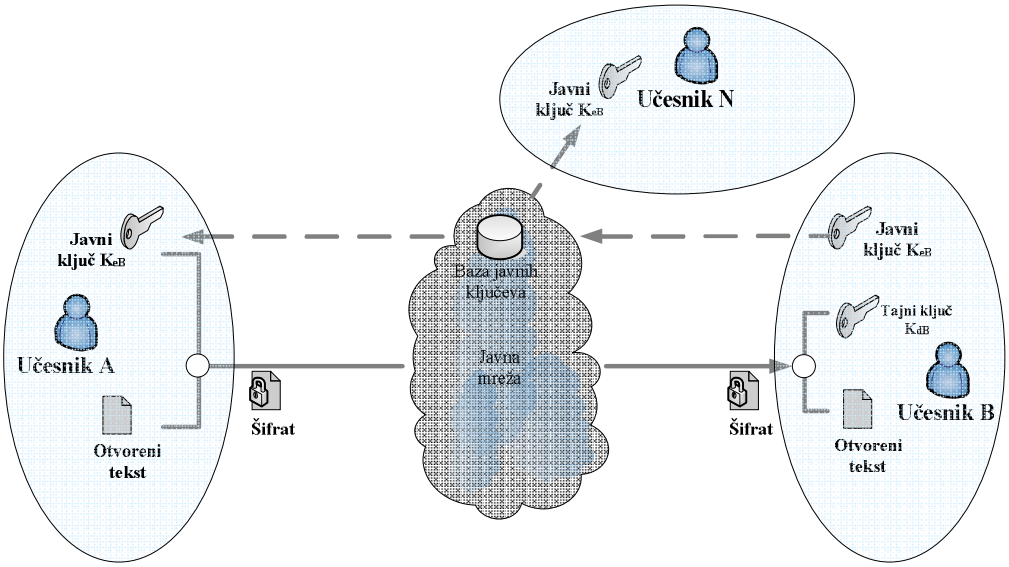
Koji će se režim rada koristiti zavisi od specifičnih zahteva korisnika. Ako su jednostavnost i brzina najbitniji, ECB mod je pravi izbor, ali ako se zahteva veća bezbednost bira se neki od preostalih režima.

3.2.3 ASIMETRIČNI KRIPTOGRAFSKI ALGORITMI

3.2.3.1 Javni i tajni ključ

Osnovni koncept asimetričnih kriptografskih sistema bazira se na različitim ključevima za šifrovanje i dešifrovanje od kojih je jedan javni, a drugi tajni (privatni) za razliku od simetričnih sistema koji koriste jedan, po pravilu, tajni ključ i za šifrovanje i za dešifrovanje. Asimetrični sistemi se zbog toga često nazivaju i sistemi sa javnim ključem (PKI – *Public Key Infrastructure*).

Informacije koje su šifrovane javnim ključem mogu se dešifrovati samo tajnim ključem, a oba ključa moraju biti povezana jedinstvenom jednosmernom funkcijom koja garantuje da se tajni ključ ne sme izračunati iz javnog ključa ili se barem ne sme izračunati u razumnom vremenu. Asimetrični algoritmi se zasnivaju na određenim osobinama brojeva gde se prilikom šifrovanja otvoreni tekst tretira kao niz prirodnih brojeva koji se odabranom funkcijom šifrovanja i ključem *Ke* preračunavaju u šifrovani tekst, ali tako da se iz njega ne može odrediti otvoreni tekst bez obzira što je ključ za šifrovanje poznat tj. javan. Međutim, ukoliko je poznat ključ za dešifrovanje *Kd* moguće je lako računanje otvorenog teksta. Asimetrično šifrovanje predstavlja jako složen vid zaštite. Za njegovu realizaciju svaki od učesnika mora posedovati dva ključa (javni i tajni) koji su, iako različiti, međusobno povezani određenim transformacijama. Na slici 16 prikazan primer asimetričnog šifrovanja.



Slika 16. Princip asimetričnog šifrovanja

Za utemeljivače asimetrične kriptografije smatraju se W. Diffie i E. Hellman čiji je protokol (DiffieHellmannov) namenjen za razmenu ključeva, o kome će više biti rečeno u trećem delu. Pored navedenog najčešće korišćeni asimetrični algoritmi su RSA (*Rivest, Shamir, Adleman*) i ElGamal algoritam.

3.2.3.2 RSA

Predstavlja najpopularniji asimetrični algoritam koji nosi naziv po svojim izumiteljima: *Rivest, Shamir* i *Adleman*. Uređeni par brojeva (*N,d*) predstavlja tajni ključ, a (*N,e*) javni ključ gde je *N* zajednički za oba ključa. Učesnik A šifruje poruku pomoću formule $C=P^e \bmod N$, gde je *P* otvoreni tekst a *C* šifrovan tekst, dok učesnik B dešifruje sa $P=C^d \bmod N$.

Primer: Tajni ključ predstavlja uređeni par (119,77), a javni ključ je uređeni par (119,5). Učesnik A želi da pošalje karakter *F (6* – prema ASCII kodu) učesniku *B*, što bi činilo otvoreni tekst (P). Korišćenjem formule algoritma dobija $C=6^5 \bmod 119=41$. Učesnik B formulom za dešifrovanje dobija $P=41^{77} \bmod 119=6(F)$.

Neovlašćeni učesnik C zna javni ključ i formulu za dešifrovanje, ali ne zna tajni ključ što mu onemogućava dešifrovanje. U prethodnom primeru napadač bi veoma lako došao do tajnog ključa *d*, međutim koncept RSA za *d* i *e* predviđa korišćenje veoma velikih brojeva (preko trista decimalnih cifara). To u praksi znači veoma veliki broj kombinacija koje se moraju isprobati radi otkrivanja tajnog ključa i veoma dugo vreme razbijanja čak i uz pomoć najbržih danas dostupnih računara.

Prilikom izbora brojeva *N, d* i *e,*RSA koristi teoriju prostih brojeva i sledeću proceduru:

- Izabrati dva prosta broja *p* i *q* i izračunati $N=p \times q$,
- Izabrati $e<N$ tako da *e* i proizvod $(p-1)(q-1)$ budu uzajamno prosti tj. da nemaju zajedničkog delitelja osim 1),
- Odrediti broj *d* tako da zadovoljava jednačinu $(e \times d) \bmod [(p-1)(q-1)]=1$

Kao ilustracija formiranja para ključeva data je sledeća procedura: izabrati proste brojeve $p=2357$, $q=2551$; izračunati $N=p \times q=6012707$; izračunati $(p-1)(q-1)=6007800$; bira se slučajni broj $e=3113390$; računa se $d= 3674911$.

Određivanje otvorenog teksta na osnovu šifrovata i javnog ključa ekvivalentno je faktorizaciji proizvoda dva velika prosta broja. RSA algoritam zasniva bezbednost na sledećim tvrdnjama:

- Lako se određuje da li je veliki broj prost ili složen i lako se računa proizvod dva velika prosta broja,
- Lako se određuje ključ za dešifrovanje *d* tako da važi: $(e \times d) \bmod [(p-1)(q-1)]=1$,
- Lako se računa otvoreni tekst ukoliko je poznat ključ za dešifrovanje: $P=C^d \bmod N$,
- Teško se određuje ključ za dešifrovanje *d* bez poznavanja proizvoda $(p-1)(q-1)$, a on se može odrediti samo ako se faktoriše broj *N*. Faktorizacija velikog broja *N* je teška i zahteva veliku procesorsku snagu i mnogo vremena a trenutno ne postoji ni jedan, javno dostupan algoritam, koji bi to vreme redukovao na razumno.

Iz navedenih tvrdnji se zaključuje da je algoritam siguran, pri čemu ne smemo zaboraviti da velike proste brojeve *p* i *q,* nakon formiranja ključeva, ne objavljujemo.

3.2.4 HIBRIDNI SISTEMI

Osnovna prednost simetričnih algoritama je njihova efikasnost što se ogleda u kratkom vremenu šifrovanja. Međutim oni imaju dva velika nedostatka, a to su:

- Oba učesnika u komunikaciji moraju imati jedinstven simetrični tajni ključ pa se javlja problem distribucije i dogovaranja u vezi sa tim ključem, a pošto je tajnost simetričnog ključa izuzetno važna to proces razmene ključeva čini složenim,
- Veliki broj potrebnih ključeva koji raste sa povećanjem broja učesnika u telekomunikacionoj mreži; npr za *N* učesnika neophodno je $Nx(N-1)/2$ ključeva.

Asimetrični algoritmi rešavaju problem distribucije ključeva, s obzirom da svaki učesnik ima svoj par javni - tajni ključ i da ne postoji potreba za razmenom tajnih ključeva. Javni ključevi svih učesnika su dostupni svim mogućim učesnicima u komunikaciji ili se razmenjuju nezaštićenim kanalom, a svoj tajni ključ svaki učesnik čuva kod sebe. Broj potrebnih ključeva se drastično smanjuje u odnosu na simetrične algoritme. Za *N* učesnika potrebno je *N* parova ključeva. U vezi sa implementacijom asimetričnih algoritama postoje dva problema, a to su:

- Njihova kompleksnost zbog operisanja sa dugačkim ključevima što oduzima mnogo vremena, pa su oko 1000 puta sporiji od simetričnih i
- Obaveza verifikacije javnih ključeva kako bi učesnici u komunikaciji bili sigurni u identitet "sagovornika", što uvodi u sistem treću stranu koja bi vršila tu funkciju verifikacije.

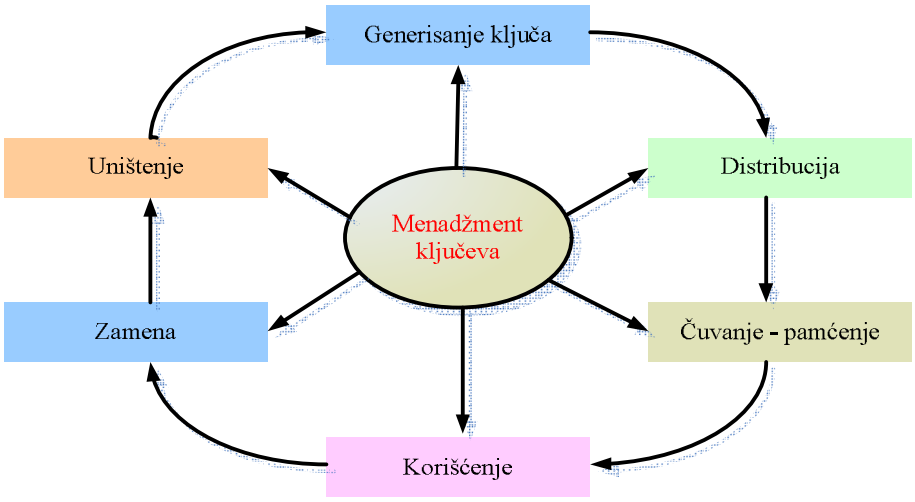
U obe vrste sistema nesporno se može postići poverljivost podataka. Činjenica je da simetrični sistemi na bazi slučajnog i pseudoslučajnog niza pružaju viši nivo bezbednosti od asimetričnih sistema pri istim dužinama ključeva. Što se tiče utvrđivanja autentičnosti učesnika u komunikaciji to se izuzetno kvalitetno realizuje u asimetričnim sistemima korišćenjem tehnike digitalnog potpisa uz upotrebu digitalnih sertifikata. U simetričnim sistemima takođe se mogu realizovati sistemi za autentifikaciju, a najpoznatiji je Kerberos. Integritet podataka u oba sistema se relativno lako realizuje a kao kriterijum se uzima uspešno dešifrovanje (struktura i sadržaj poruke). Kod realizacije servisa neporicanja kod simetričnih sistema se javlja problem postojanja aktivne treće strane od poverenja koja u spornim situacijama vrši arbitražu. Prednost asimetričnih sistema u ovom slučaju je u tome što je subjekat sam u stanju da pruži dokaze učešća drugog entiteta.

I pored toga što pojava asimetričnih algoritama predstavlja revolucionalno otkriće, u realnom svetu kriptografija sa javnim ključem ne predstavlja zamenu za simetričnu. Ona se najčešće ne koristi za šifriranje poruka, već za šifriranje ključeva. Naime, učesnici A i B komuniciraju pomoću simetričnog sistema sa tajnim ključem koji su razmenili pomoću asimetričnog sistema. Takve kriptografske sisteme nazivamo hibridni. Oni kombinuju najbolje pojedinačne karakteristike oba sistema. Upravo oni se nameću kao moguće rešenje koje je neophodno tražiti prilikom projektovanja sistema zaštite u optičkim telekomunikacionim mrežama.

3.3 UPRAVLJANJE KRIPTOGRAFSKIM KLJUČEVIMA

3.3.1 FAZE KRIPTOLOŠKIH KLJUČEVA

S obzirom da su ključevi najosetljiviji element u kriptografskom sistemu i da se većina napada na sistem bavi njihovim otkrivanjem, upravljanje ključevima je od suštinske važnosti za sigurnost celokupnog sistema. Na slici 17 prikazane su faze kroz koje kriptološki ključevi prolaze. Zadatak uprvaljanja ključevima je, da u svakom trenutku, od generisanja pa do uništenja obezbedi njihovu tajnost i integritet. Poznato je da ključeve možemo podeliti na simetrične, javne i privatne, a da simetrični i privatni predstavljaju tajne ključeve.



Slika 17. Faze kriptološkog ključa

Upravljanje kriptološkim ključevima je proces kroz koji se postiže:

- Generisanje sigurnog ključa,
- Bezbedna distribuciju ključa do svih učesnika u komunikaciji,
- Čuvanje ključeva,
- Korišćenje ključa (aktivacija i deaktivacija),
- Zamena ključa i
- Uništenje ključa nakon isteka i u slučaju opasnosti ili eventualno arhiviranje.

3.3.1.1 Generisanje ključeva

Veliku pažnju prilikom generisanja ključeva treba posvetiti izboru samog generatora tj. njegovim osobinama i potencijalnim slabostima koje napadač može upotrebiti pri pokušaju provaljivanja ključa. Uz pomoć statističkih testova za određivanje osobine generisanog ključa može se zaključiti da većina generatora ne poseduje apsolutnu sigurnost, tj. niz brojeva koje generiše nije slučajan već pseudoslučajan. Pošto ne postoje univerzalni testovi čiji prolaz garantuje da je neki generator potpuno pouzdan, generatori pseudoslučajnih brojeva se konstruišu na osnovu matematičke analize njihovih strukturalnih osobina. Glavni uslov za postizanje sigurnosti generatora jeste dovoljno veliki period. Ulaz u generator mora biti tako odabran da ga je praktično nemoguće otkriti nekom metodom pogađanja. Ovim se omogućava generisanje vrlo velikog broja pseudoslučajnih nizova brojeva koje je nemoguće analizirati u realnom vremenu. Ovako dobijeni nizovi se mogu upotrebiti kao kriptološki ključevi. Ovakvi generatori slučajnih brojeva kod kojih je uz poznavanje algoritma i nepoznavanje početnih uslova nemoguće predvideti niz generisanih brojeva zovu se generatori kriptografskih sigurnih pseudoslučajnih brojeva CSPRNG (*Cryptographically secure pseudorandom number generator*).

Pojedini ključevi, i pored toga što su generisani u pouzdanim i proverenim generatorima mogu imati nezadovoljavajuće karakteristike ako se upotrebe u određenim algoritmima za šifrovanje. Na primer, DES algoritam ima definisane slabe ključeve koji po pitanju otpornosti na kriptoanalizu ne daju zadovoljavajuće rezultate. Isto tako, kada se koristi RSA algoritam brojevi p i q se moraju birati iz skupa prostih brojeva i u skladu sa tim generisati ključ u binarnom obliku. Ograničenja kao što su ova neophodno je integrisati u rad samog generatora.

Jedna od veoma bitnih karakteristika koja se mora imati u vidu je dužina ključa. Najbolja varijanta je kada korisnik ili administrator može da vrši njen izbor. Sigurnost kriptografskog sistema, pored snage algoritma, treba da se zasniva na tajnosti i dužini ključa. Među teoretičarima vlada mišljenje da je snaga algoritma savršena ukoliko ne postoji ni jedna druga mogućnost za provaljivanje sistema od pretraživanja svih mogućih ključeva odnosno napada "grubom silom." Složenost napada "grubom silom" lako se izračunava. Na primer, za 64-bitni ključ neophodno je ispitati 2^{64} mogućih ključeva. Sa povećanjem dužine ključa složenost napada se eksponencijalno povećava, a sa njim i vreme potrebno za uspešnu kriptoanalizu "grubom silom." Zbog toga je važno što približnije pretpostaviti procesorsku snagu potencijalnog napadača kako bi se odredila optimalna dužina ključa, jer ona utiče i na efikasnost rada samog algoritma zbog čega se ne mogu koristiti previše dugi ključevi jer bi oni znatno usporili algoritam.

Istraživanja u kriptoanalizi dovode do otkrivanja potencijalnih slabosti algoritama pa se svakih nekoliko godina povećava minimalna preporučena dužina ključa za pojedine algoritme. Neki od algoritama koriste ključeve fiksne dužine, kao što je DES algoritam sa ključem od 56 bita. Ključ dužine 1024 bita u okviru RSA algoritma je sigurniji nego ključ od 512 bita kod istog algoritma.

3.3.1.2 Distribucija ključeva

Nakon generisanja ključeva isti se moraju koristiti na različitim lokacijama pa je sledeći korak njihova distribucija do učesnika. Zadaci distribucije su:

- Da se ključevi dostave tajnim kanalom na odredište,
- Da ključevi budu prenešeni u univerzalnom i za učesnike razumljivom formatu.

U cilju izvršenja sigurne razmene ključeva između dva učesnika u simetričnom sistemu mogu se koristiti razni protokoli koji se zasnivaju na postojanju trećeg entiteta od poverenja. Ovaj entitet se naziva centar za distribuciju ključeva ili KDC (*Key Distribution Center*). Uloga KDC-a je da putem sigurnog kanala svakom učesniku obezbedi simetrični ključ za komunikaciju sa bilo kojim učesnikom u mreži. Uslov za to je da svi učesnici poseduju tajni simetrični ključ za komunikaciju sa KDC za čiju distribuciju se razvijaju posebni protokoli, a u određenim situacijama se preuzimaju fizički. Implementacijom KDC-a, pored bezbednosnih, rešava se i veoma izražen problem skalabilnosti mreže.

3.3.1.3 Zamena i uništenje ključeva

Ne postoji univerzalno pravilo o frekvenciji zamene ključeva, ali se za svaki kriptografski sistem određuje optimalno vreme trajanja jednog ključa. Ideja roka važenja ključeva potiče od činjenica da mera uspešnosti napadača direktno zavisi od skupa prikupljenih informacija o kriptografskom sistemu od kojih je najbitnija informacija ključ. Sistemi koji vrše zamenu ključeva implementiraju se u sam algoritam i upravljački softver, ili se preko odgovarajućeg interfejsa "prepuštaju" operateru.

Razlozi za zamenu ključeva mogu biti:

- Redovno obnavljanje u određenim intervalima u cilju sprečavanja provaljivanja od strane napadača i
- Sumnja da je korišćeni ključ već provaljen (kada zamenu treba izvršiti urgentno).

Nakon isteka roka važenja ključevi se obavezno uništavaju što se realizuje automatski. Prilikom distribucije, čuvanja ili korišćenja ključevi se mogu oštetiti ili doći u posed neovlašćenih osoba. U ovakvim situacijama isti se stavljaju van snage o čemu moraju biti obavešteni svi učesnici za šta se razrađuju posebni mehanizmi.

3.3.2 PROTOKOLI ZA RAZMENU KLJUČEVA

3.3.2.1 KDC

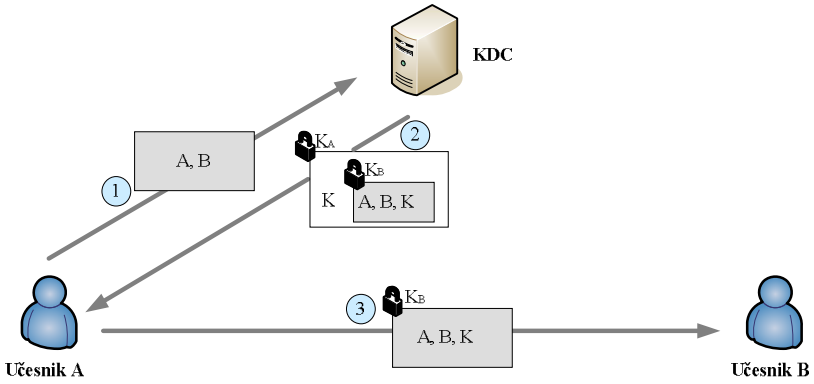
Koncept KDC-a podrazumeva da se za svaki komunikacioni kanal za šifrovanje određene poruke ili za šifrovanje u određenom vremenskom intervalu koristi privremeni ključ sesije. Nakon isteka intervala, uspostavlja se sledeći ključ sesije, a prethodni se uništava. Razlozi za korišćenje ključa sesije su sledeći:

- Često korišćeni simetrični ključevi lakše se razbijaju,
- Zaštita od napada ponavljanjem prethodnih poruka,
- Razbijanje ključa jedne sesije neće biti moguće dekriptovanje podataka poslatih tokom ranijih ili kasnijih sesija,
- Ukoliko autentifikacija nije na zahtevanom nivou, onda je bolje koristiti privremene ključeve sesija.

Do ključa sesije, koji ćemo u primerima obeležavati sa K_{AB}, u opštem slučaju, dolazi se kroz nakoliko koraka (uslov je postojanje tajnih ključeva K_A i K_B koje učesnici dele sa KDC-om), što je ilustrovano na slici 18:

- Korak 1: Učesnik A šalje otvorenu poruku KDC-u sa zahtevom za komunikaciju sa učesnikom B, a u cilju kreiranja zajedničkog ključa sesije K_{AB}. Poruka sadrži podatke o identitetu učesnika A i B.

- Korak 2: KDC formira tzv. tiket namenjen učesniku B, koji sadrži identitete oba učesnika i sesijski ključ K_{AB}, šifruje ga ključem K_B, zatim tiket upakuje zajedno sa sesijskim ključem K_{AB}, šifruje ključem K_A i šalje učesniku A. Učesnik A nakon dešifrovanja otpakuje K_{AB}, ali pošto nema ključ K_B ne može da otpakuje tiket namenjen učesniku B.
- Korak 3: Učesnik A prosleđuje tiket učesniku B koji otpakuje K_{AB}.



Slika 18. Razmena ključeva korišćenjem KDC

Pored navedenog standardnog načina razmene ključeva sa KDC-om postoji nekoliko drugih varijanti odnosno protokola za razmenu ključeva. U nastavku će biti predstavljeni neki od najčešće korišćenih protokola. Način organizacije i funkcionisanja KDC-a za konkretnu telekomunikacionu mrežu zavisi od topologije mreže, broja učesnika i frekvencije saobraćaja, a za veće mreže može se realizovati više hijerarhijski organizovanih distributivnih centara od koji svaki opslužuje po deo mreže.

3.3.2.2 DiffieHellman-ova eksponencijalna razmena ključeva

DiffieHellman protokol za rezmenu ključeva zasniva se na diskretnom logaritamskom problemu tj. na činjenici da je teško izračunati g^{xy} ukoliko je poznato g^x i g^y. Namenjen je isključivo za razmenu simetričnih ključeva a nepraktičan je za šifrovanje poruka. Ne zahteva nužno angažovanje treće strane.

Obuhvata sledeće korake:

- Učesnici A i B biraju veliki prost broj n i broj g takav da je $G=(0,1,...n-1)$ ciklična multiplikativna grupa, a g njen generator,
- Učesnik A bira veliki slučajan broj x i šalje učesniku B poruku: $X=g^x \bmod n$,
- Učesnik B bira veliki slučajan broj y i šalje učesniku A poruku: $Y=g^y \bmod n$,
- Učesnik A određuje $k=Y^x \bmod n$,
- Učesnik B određuje $k'=X^y \bmod n$,
- Vrednosti k i k' jednake su $g^{xy} \bmod n$ i čine tajni simetrični ključ koji učesnici A i B nezavisno generišu. Napadač, da bi došao do k mora da izračuna diskretni logaritam odnosno mora da faktoriše broj reda veličine n, što je u realnom vremenu nemoguće.

DiffieHellman protokol je neotporan na napad tipa *man-in-the-middl,* gde napadač može da se predstavi kao druga strana za oba učesnika i obmanjivanjem dođe do simetričnih ključeva, a da učesnici ne primete problem. Prevencija protiv ovog napada su razni protokoli za autentifikaciju, npr. *Station-to-Station* protokol uključujući i digitalno potpisivanje od strane učesnika.

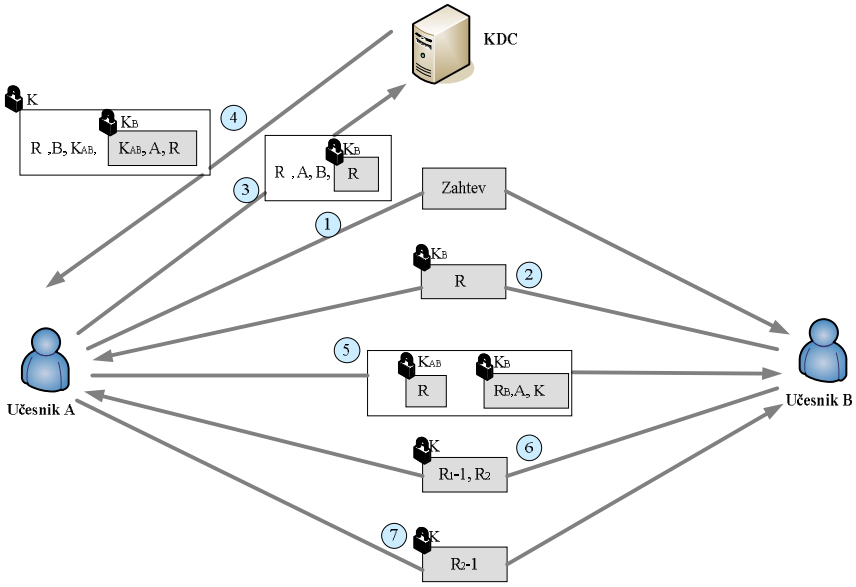
3.3.2.3 Needham-Schroeder protokol

Važi za fundamentalni protokol za formiranje sesijskih ključeva putem KDC-a na osnovu koga su nastali mnogi drugi protokoli i predstavlja odlično rešenje po pitanju sigurnosti. Kako bi se postigla što sigurnija razmena ključeva, koristi se više naizmeničnih koraka tipa "izazov-odgovor" između dva učesnika.

Prema poslednjoj verziji ovog protokola koriste se četiri slučajna broja: R_A, R_B, R_1 i R_2 za svaki sesijski ključ. Koraci protokola *Needham-Schroeder* prikazani su na slici 19.

Protokol se sastoji od sledećih sedam koraka:

- Korak 1: Učesnik A šalje svoj identitet učesniku B otvoreno u vidu zahteva za komunikaciju,
- Korak 2: Učesnik B pomoću svog tajnog ključa koji deli sa KDC (K_B) šifruje prethodno generisani broj R_B , ali ga šalje učesniku A.
- Korak 3: Primljenu poruka učesnik A dopunjava sa generisanim slučajnim brojem R_A, identitetom učesnika A i identitetom učesnika B i prosleđuje je KDC-u. Treba napomenuti da ova poruka nije šifrovana, i da predstavlja zahtev učesnika A namenjen KDC-u u cilju obezbeđivanja tajnog ključa sesije K_{AB} za obavljanje sigurne razmene podataka između učesnika A i B.
- Korak 4: KDC vraća učesniku A poruku šifrovanu tajnim ključem K_A sa sledećim sadržajem: broj R_A, identitet uečsnika B, ključ sesije K_{AB} i tiket koji je namenjen učesniku B. Ovaj tiket je šifrovan tajnim ključem K_B, a sadrži ključ sesije K_{AB}, identitet učesnika A i broj R_B. Ovim učesnik A dobija odziv od KDC-a koji sadrži sve neophodne podatke za bezbednu komunikaciju sa učesnikom B.
- Korak 5: Učesnik A prosleđuje učesniku B tiket dobijen od KDC-a i novi broj R_1 koji šifruje sesijskim ključem K_{AB} u cilju prozivanja i verifikacije učesnika B.
- Korak 6: Učesnik B odgovara slanjem šifrovanog broja R_1-1 i pozivom učesnika A brojem R_2. Ako učesnik A nakon dešifrovanja primljene poruke dobije očekivani broj R_1-1, to znači da je identitet učesnika B verifikovan, jer je onaj ko je poslao ovu poruku bio u stanju da otvori tiket primenom K_B i dođe do K_{AB}, a to može samo učesnik B.



Slika 19. Protokol Needham-Schroeder

- Korak 7: U okviru poslednjeg koraka učesnik A ponovo odgovara na poziv slanjem šifrovanog broja R_2-1. Ovom porukom učesnik A obaveštava učesnika B da je primio verifikaciju i istovremeno verifikuje sebe učesniku B. Dalja komunikacija se obavlja primenom tajnog sesijskog ključa K_{AB}.

4. IMPLEMENTACIJA KRIPTOGRAFSKOG SISTEMA U OPTIČKU TELEKOMUNIKACIONU MREŽU

4.1 ANALIZA KOMUNIKACIONIH KARAKTERISTIKA

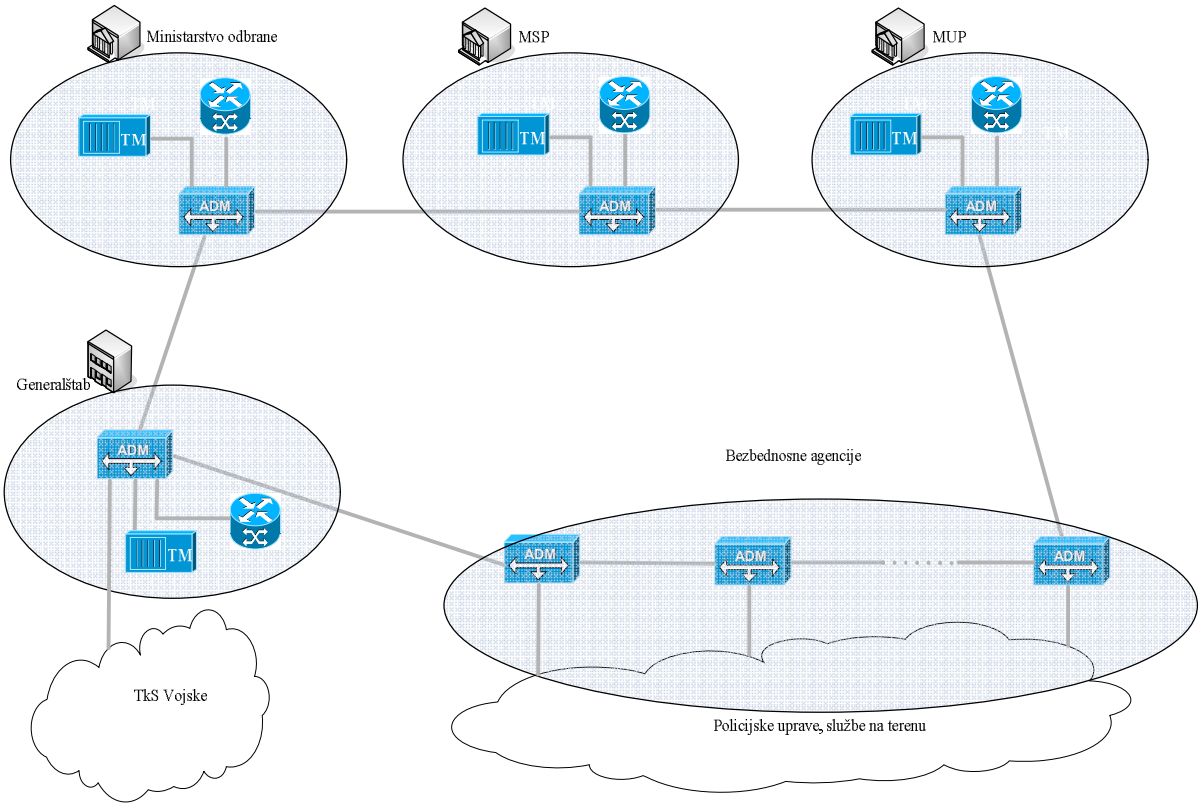
4.1.1 MODEL MREŽE

Na primeru optičke telekomunikacione mreže koju ćemo posmatrati kao model za implementaciju kriptografskog sistema izvršićemo kratku analizu komunikacionih karakteristika, izneti zahteve za proizvodima koji će biti primenjeni i ukazati na bitne procese pri projektovanju sistema zaštite. Posmatraćemo primer optičke telekomunikacione mreže državnih organa, koja po svojoj prirodi zahteva visok nivo zaštite informacija, u kojoj funkcioniše tehnološki zastareo sistem zaštite na fiizičkom sloju za koji postoji osnovana sumnja da ga je lako provaliti i koji, s obzirom na zahtevani nivo bezbednosti informacija, ultimativno zahteva modernizaciju. Kroz servise koji koriste ovu mrežu do sada je implementiran deo sistema zaštite na višim slojevima. Kako bi se postigla potpuna slojevitost sistema zaštite i veća sigurnost podataka, razmatramo primenu hardverskih *link encryption* rešenja za zaštitu na prvom i/ili drugom sloju.

Pomenuti model mreže, prikazan na slici 20, ima čvorove u telekomunikacionim centrima sledećih državnih organa: ministarstvo odbrane, ministarstvo spoljnih poslova, ministarstvo unutrašnjih poslova, generalštab vojske i bezbenosne agencije. U navedenom primeru telekomunikacione mreže se podrazumeva da je na izvorima informacija izvršena klasifikacija podataka po stepenu tajnosti, te da se infrastruktura koju analiziramo koristi uglavnom za prenos poverljivih podataka.

Namena mreže je za povezivanje lokalnih servera, terminalnih uređaja, digitalnih automatskih telfonskih centrala, sistema daljinskog nadgledanja, upravljanja i navođenja. Služi kao osnova informacionim sistemima čiji je cilj upravljanje, komandovanje i rukovođenje sistemom odbrane kao i sektorom javne i državne bezbednosti.

Ovakav model mreže iznet je u cilju preciznijeg definisanja predloženog rešenja sistema zaštite, bez bilo kakvih tendencija i poklapanja sa stvarnim telekomunikacionim mrežama.



Slika 20 Otička telekomunikaciona mreža državnih organa

4.1.2 BITSKE BRZINE

Bitske brzine koje egzistiraju u mreži prikazane su u tabeli 4. Iako su transportni i pristupni deo mreže delovi jedinstvenog sistema, zbog njihovih specifičnosti i razlika moguće ih je razmatrati nezavisno. Činjenica je da su telekomunikacioni servisi u ekspanziji i da se svakih nekoliko godina zahtevana bitska brzina na spojnom putu udvostručava. Zbog toga se sa aspekta implementacije sistema zaštite nameće pitanje plana razvoja i dogradnje mreže u narednom periodu.

Transportni deo		**Pristupni deo**	
Trenutno	**Plan dogradnje u narednih 8 godina**	**Trenutno**	**Plan dogradnje u narednih 8 godina**
STM-1, 155.520 kbit/s	STM-16, 2.488.320 kbit/s + DWDM	E1 PDH 2.048 kbit/s	1Gb Ethernet + CWDM
STM-4, 622.080 kbit/s	STM-64, 9.953.280 kbit/s + DWDM, 1Gb Ethernet + DWDM	E3 PDH 34.368 kbit/s	STM-1, 155.520 kbit/s

Tabela 4. Bitske brzina u mreži

4.1.3 OSTALE KARAKTERISTIKE

Osnovni zadatak rešenja koje će biti primenjeno je da se karakteristike telekomunikacione mreže ne degradiraju, jer je ta mreža i ranije korišćena bez umetnutog sistema ili sa starijim sistemom zaštite. Sa aspekta implementacije kripto uređaja u vidu hardverskog rešenja, pored bitske brzine, moraju se analizirati i sledeće karakteristike:

- Telekomunikacioni servisi koji se koriste u mreži i
- Interfejsi koje je neophodno zaštititi.

Najčešći servisi koji se koriste i koji zahtevaju zaštitu su: prenos podataka između lokalnih servera, razne vrste aplikacija za upravljanje bezbednosnim procesima, pristup intranet mreži, video konferencijski sistem i prenos govora u standardnom i VoIP formatu. Vrstu telekomunikacionog servisa treba posmatrati zbog mogućeg kašnjenja koje kripto uređaj može uneti zbog izvršenja kriptološke sinhronizacije, razmene ključeva i samog izvršenja šifrovanja. Najosetljiviji servisi u ovom pogledu su prenos govora i video signala, koji zahtevaju prenos informacija u realnom vremenu.

Interfejsi koji se u mreži koriste ispunjavaju ITU-T i IEEE preporuke za PDH, SDH i Carrier Ethernet digitalne hijerarhije. U pristupnom delu mreže kreću se od E1 G.703 do STM-1 SDH, a u transportnom delu egzistiraju interfejsi STM-1 i STM-4 SDH, kao i FE 100Base-FX, FE 100Base-TX i GbE 1000Base-LX Carrier Ethernet. Interfejsi kripto uređaja namenjenih za zaštitu navedenih tipova signala moraju biti standrdizovani i ispunjavati iste preporuke. Provera u nominalnim vrednostima izvršila bi se kroz njihovo verifiaciono ispitivanje.

4.2 ZAHTEVI ZA KRIPTO UREĐAJIMA

S obzirom na napred iznetu analizu komunikacionih karakteristika mreže, držeći se instrukcija iz politike zaštite, a imajući u vidu raspoložive tehnologije, neophodno je definisati zahteve za konkretnim rešenjem kriptografske zaštite. U središtu pažnje prilikom definisanja zahteva su:

- Poštovanje zakonske regulative koja uređuje oblast zaštite informacija,
- Bezbednost rešenja, tj. nužnost ispunjavanja svih funkcija kriptografije (tajnosti, integriteta, autentifikacije i neporecivosti),
- Kvalitet prenete informacije u pogledu brzine, dometa i kašnjenja signala,
- Jednostavnost i efikasnost upotrebe, odnosno što veća nezavisnost od krajnjih korisnika.

Zahtevi, u pogledu algoritma i ključeva, koji se nameću na osnovu do sada iznetog su:

- Implementirati *link encryption* hardversko rešenje sa zasebnim uređajima čiji se interfejsi lako prilagođavaju optičkim vlaknima, terminalnim i SDH multiplekserima i ATM komutatorima,
- Obezbediti što veći uticaj na parametre kriptografskog algoritma, dužinu ključa i upravljanja ključevima, od strane administratora,
- Primeniti kompleksan simetrični blokovski kriptografski algoritam koji razviti modifikacijom AES algoritma,

- Omogućiti permanentno praćenje sigurnosti algoritma u toku funkcionisanja i razvijati nove alternativne algoritme,
- Algoritam čuvati u tajnosti, a pored toga sigurnost sistema bazirati i na tajnosti ključeva,
- Koristiti ključ dužine 128 bita sa mogućnošću povećanja do 256 bita, a u perspektivi i veće dužine,
- Upravljanje ključevima realizovati posredstvom menadžment centra koji će imati i ulogu KDC-a, a čije mesto projektovati u centru za nadzor i upravljanje telekomunikacionom mrežom.

U skladu sa, do sada iznetim zahtevima, potrebno je ispitati tržište i izvršiti izbor kripto uređaja, i to:

- Za transportni deo mreže, takve da u komunikacionom delu budu multiprotokolarni i transparentni, tj. da pored SDH i Carrier Etherneta, mogu obrađivati i druge vrste signala (bazirane na xWDM multipleksiranju) do 10 Gbit/s protoka,
- Za pristupni deo mreže za link encryption PDH pritočnih signala od 2 i 34 Mbit/s.

U pogledu bezbednosti kompletnog rešenja, potrebno je istaći sledeće zahteve:

- Upravljački softver uređaja mora dozvoljavati lokalni i daljinski pristup za više nivoa korisnika, i to: administrator, kriptooperater i kontrolor.
- Obavezna identifikacija korisnika putem lozinke prilikom pristupa uređajima,
- Zabrana automatskog prelaska u otvoreni režim rada,
- Zaštita od kompromitujućeg elektromagnetnog zračenja što podrazumeva oklapanje uređaja i opremanje adekvatnim filtrima na napajanju i interfejsima,
- Zaštita od fizičkog pristupa kripto parametrima u uređaju koja može biti realizovana *tamper proof* režimom.

4.3 PROJEKTOVANJE SISTEMA ZAŠTITE

Projektovanje sistema zaštite predstavlja kompleksan proces, koji bi u realnoj situaciju, s obzirom na važnost projekta, izvodio projektni tim imenovan od vladinog tela zaduženog za sprovođenje nacionalnog programa za zaštitu informacija. Podela projekta na faze mogla bi se izvršiti na sledeći način:

- Analiza sistema zaštite,
- Oblikovanje sistema zaštite i
- Implementacija sistema zaštite.

Cilj projekta je da ostvari realizaciju, odnosno uvođenje novog sistema zaštite informacija na spojnom putu u optičkoj telekomunikacionoj mreži državnih organa kao sastavnog dela slojevitog sistema zaštite podataka. Princip koji ćemo poštovati prilikom projektovanja je da ovakav sistem zaštite, po svojoj prirodi, ima ograničenu primenu na profesionalne sisteme i da rešenje do koga se projektovanjem dođe predstavlja jedno od mogućih rešenja.

4.3.1 ANALIZA SISTEMA ZAŠTITE

U prvoj fazi potrebno je koncipirati projekat tj. iz projektne ideje razviti koncepciju projekta. Takođe je potrebno izvršiti utvrđivanje i analizu činjeničnog stanja.

Optička mreža koju razmatramo namenjena je za obezbeđenje telekomunikacionih servisa državnim organima bezbednosnog sektora. Savremeni oblici ugrožavanja bezbednosti poput terorizma, oružanih pobuna i organizovanog kriminala u svojoj pozadini nose pretnje po telekomunikacioni sistem jedne države. Pored svih drugih oblika, zaštita podataka na spojnim putevima od neovlašćenog pristupa je nezaobilazan oblik zaštite tog sistema. Nivo poverljivosti informacija koje su sastavni deo servisa navedenih državnih organa je od najvišeg interesa za sistem odbrane i nacionalnu bezbednost.

Optička vlakna koja se koriste predstavljaju vlasništvo javnog telekomunikacionog provajdera i nemaju razvijene sisteme za otkrivanje fizičkog pristupa i prisluškivanja i kao tekva predstavljaju krajnje nebezbednu sredinu.

Mreža je organizovana u transportni SDH STM-4 prsten sa *add/drop* segmentima. Svaki od navedenih organa, po hijerarhijskoj dubini ima svoje telekomunikacione mreže koje, osim optičkih vlakana, koriste i druge spojne puteve (žične, radio-relejne, radio i satelitske).

U transportnom delu, koji je organizovan u prsten, mreža se sastoji od SDH multipleksera modularnog tipa sa integrisanim funkcijama ADM (*Add/Drop Multiplexing*), DXC (*Digital Cross Connect*) i *TM (Terminal multipexing)*. Prstenasta struktura mreže omogućava automatsku regeneraciju u slučaju prekida optičkog vlakna ili ispada nekog od čvorova. Celokupna mreža ima obezbeđen daljinski nadzor i upravljanje primenom TMN (*Telecommunication Management Network*).

U pristupnom delu postoji više terminalnih SDH i PDH multipleksera i ATM komutatora. Svaki od organa ima razvijenu sopstvenu LAN mrežu. Trenutni kapaciteti mreže zadovoljavaju potrebe zadejstvovanih servisa, ali se u narednom periodu planira uvođenje novih, po kapacitetu prenosa zahtevnijih servisa, zbog čega će biti neophodna dogradnja mreže multiplekserima većih bitskih brzina i uvođenje xWDM multipleksera u cilju povećanja informacionog kapaciteta.

Primenjeni sistemi za zaštitu na aplikativnom i mrežnom nivou predstavljaju dobar, ali ne i dovoljan oslonac bezbednosti informacija s obzirom na stepen njihove tajnosti. Zaštita govora, koja se do sada obavljala putem krajnjih uređaja za zaštitu govora posredstvm PSTN (*Public Switched Telephone Network)*, predstavlja nepraktično rešenje s obzirom na veliku potrebu bezbednosnih struktura za zaštitom govornih informacija.

4.3.2 OBLIKOVANJE SISTEMA ZAŠTITE

U drugoj fazi projektovanja definiše se optimalna koncepcija i struktura sistema zaštite optičke telekomunikacione mreže. U ovoj fazi, projekat se, radi efikasnosti, može razbiti na više projekata podsistema ili na projektne segmente uz obaveznu usklađenost ciljeva i koncepcija pojedinih projekata ili segmenata. U tom pravcu, sistemskim pristupom treba izvršiti dekomponovanje sistema na sastavne delove ili podsisteme, izvršiti detaljnu analizu tokova informacija između tih podsistema i primeniti višekriterijumski pristup u ocenjivanju uspešnosti funkcionisanja pojedinih delova.

Oblikovanje sistema zaštite, u konkretnom slučaju, postiže se kroz sledeće projektne segmente:

- Izbor kriptografskog algoritma,
- Određivanje dužine ključeva i načina upravljanja ključevima,
- Izbor kripto uređaja i
- Verifikaciono testiranje.

Izbor kriptografskog algoritma za konkretno rešenje koji ćemo primeniti zavisiće od:

- Zahtevanog nivoa zaštite, koji je definisan politikom zaštite, a koji proizilazi iz zahteva korisnika,
- Komunikacionih karakteristika mreže, čija je analiza izvršena i
- Raspoloživih tehnologija i/ili raspoloživih finansijskih sredstava.

Imajući u vidu sve što je izneto u teorijskim osnovama o kriptografskim algoritmima, simetrični blokovski kriptografski algoritam u cilju boljeg postizanja tajnosti i efikasnosti sistema je logičan izbor za model mreže koji razmatramo. Međutim treba posmatrati uticaj simetričnog algoritma na slobodu izbora dužine ključeva, način upravljanja ključevima kao i njegovu prilagodljivost različitim topologijama mreže. Simetrični algoritmi su, sa aspekta telekomunikacija, najprimenljiviji u *link encryption* konfiguracijama, što s obzirom na kompleksnost posmatrane mreže, otvara dilemu složenosti njegove primene za *multipoint* organizaciju sistema zaštite za kojim imamo potrebu na pojedinim pristupnim delovima mreže.

Razvoj samog algoritma je predmet analize koja po mnogome prevazilazi okvire ovog rada, a sistemskim posmatranjem u okviru konkretnog projekta predlažemo:

- Posebno razvijen algoritam na bazi AES algoritma čiji razvoj unapred planirati,
- Sigurnost sistema zaštite zasnivati na tajnosti algoritma i tajnosti ključeva.

Pri svemu tome mora se imati u vidu da nijednim algoritmom, bez obzira na njegovu snagu, ne postižemo konačnu zaštitu, jer se dektiptorske sposobnosti protivnika ne mogu uvek dovoljno proceniti. Zbog toga je potrebno neprekidno pratiti i unapređivati kriptografski algoritam kao fundamentalni element sistema zaštite, a sam sistem zaštite shavatiti kao neprekidan proces čiji je cilj dostizanje što višeg nivoa zaštite.

Izbor dužine ključa imaće direktan uticaj na sigurnost kompletnog sistema zaštite. Zbog toga je važno sagledati sve aspekte pri ovom izboru. Kao polazne osnove za određivanje dužine ključa treba uzeti:

- Stepen tajnosti informacija koje se štite,
- Vreme aktuelnosti tajnih informacija i
- Procenu resursa protivnika.

Ukoliko bi nam u potpunosti bili poznati resursi protivnika, imali bi smo lak zadatak da na osnovu njih proračunamo graničnu dužinu ključa koja je za određeni nivo tajnosti i vreme aktuelnosti tajnih informacija, adekvatna. Napadi na dužinu ključa jesu napadi "grubom silom" i predstavljaju ispitivanje svih mogućih ključeva, a njihov uspeh zavisi od procesorske moći kriptoanalitičara. Pošto snagu protivnika možemo samo da je pretpostavimo, ostaju nam druga dva bitna faktora koji utiču na dužinu ključa. Ukoliko znamo da naše tajne informacije imaju vrednost koja prevazilazi cenu ulaganja protivnika u sistem za pretragu "grubom silom", tada moramo povećavati dužinu ključa. Vreme aktuelnosti tajne je takođe veoma bitno. Ukoliko je to vreme duže od vremena potrebnog za pretraživanje svih mogućih ključeva, pod pretpostavkom da je cena napada "opravdana", ponovo moramo povećavati dužinu ključa. Povećanje dužine ključa negativno utiče na performanse kompletnog sistema, pa je pronalaženje optimalne dužine izuzetno kompleksno.

U telekomunikacionoj mreži koju posmatramo, kao što je rečeno, prenošene informacije su od izuzetnog značaja. Njihova aktuelnost, zavisno od servisa, može biti različita, od veoma kratke do trajne. Iz ovog rezloga izvršićemo uslovnu podelu mreže na dva segmenta, prvi u kome se prenose informacije sa dužim periodom i drugi sa kraćim periodom aktuelnosti. Prvi deo mreže se uglavnom poklapa sa transportnim delom, dok informacije sa kraćom aktuelnošću više cirkulišu u pristupnim delovima, ali i kroz celu mrežu. To nam omogućava da primenimo dve dužine ključeva u dva različita kripto uređaja a koje ćemo paralelno implementirati u transportni i pristupni deo mreže.

Sa izabranim algoritmom, imajući u vidu važnost štićenih informacija kao i teorijska istraživanja o procenama napada "grubom silom" predlažemo upotrebu ključeva sa izborom dužine od 128 do 256 bita, s tim što bi početna projektovane dužine za pristupni deo bila 128 bita, a za transportni 256 bita.

Način upravljanja je drugi bitni element vezan za ključeva. Napadač će, prema procenama, svestan da vodimo računa o dužini ključa, izbegavajući napad „grubom silom", mnogo češće pokušati da drugim metodama otkrije sam ključ. Izborom i primenom kvalitetnog upravljanja ključevima minimiziraju se takvi pokušaji napadača. Savremena rešenja na tržištu nude centralizovano upravljanje svim kriptološkim parametrima pa i ključevima. Prihvatanje ovakvog rešenja je neminovno radi ispunjavanja uslova efikasnosti i nezavisnosti od lokalnog operatera. Ipak, zahtevi koji moraju biti ispunjeni kao preduslov izbora ovakvog načina upravljanja ključevima su: inicijalno lokalno punjenje kripto parametara, periodično lokalno unošenje tajnih UK, obavezna autentifikacija lokalnih operatera, jasno definisan odnos između lokalnog i udaljenog operatera odnosno administratora.

Izbor kripto uređaja predstavlja završno razmatranje u cilju objedinjavanja do sada iznetih činjenica i pretpostavki. Ispitivanjem tržišta, na osnovu iznetih zahteva i dosadašnjih iskustava, izbor usmeravamo ka proizvodima sledećih firmi:

- Crypto AG (Švajcarska),
- Čajavec a.d. Banja Luka (Bosna i Hercegovina),
- Iritel a.d. Beograd (Srbija).

Dva nespojiva zahteva: Potreba uticaja na kreiranje algoritma kao prvi i obezbeđenje zaštite na visokim bitskim brzinama kao drugi zahtev, čine izbor kriptouređaja kompleksnim i izdižu ga na politički nivo. Sa tehničkog aspekta istovremena primena proizvoda svatri proizvođača nije neizvodljiva.

Konačan predlog rešenja za kriptografsku zaštitu podataka u posmatranoj optičkoj telekomunikacionoj mreži glasio bi:

- Implementirati proizvode Crypto AG za zaštitu linkova na većim bitskim brzinama u transportnom delu mreže,
- Implementirati proizvode Čajavec a.d. i Iritel a.d. za zaštitu E1 i E3 linkova u pristupnom delu mreže, ali i u *point to point* komunikacijama za pojedine servise,

Karakteristike uređaja prikazane su u završnom delu rada, a predloženi način implementacije u mrežu prikazan je na slici 21. Pre nabavke i početka implementacije potrebno je izvršiti verifikaciona testiranja za koje postoje posebne procedure, a usmerene su ka proveri ispunjavanju standarda i propisa od strane konkretnih proizvoda.

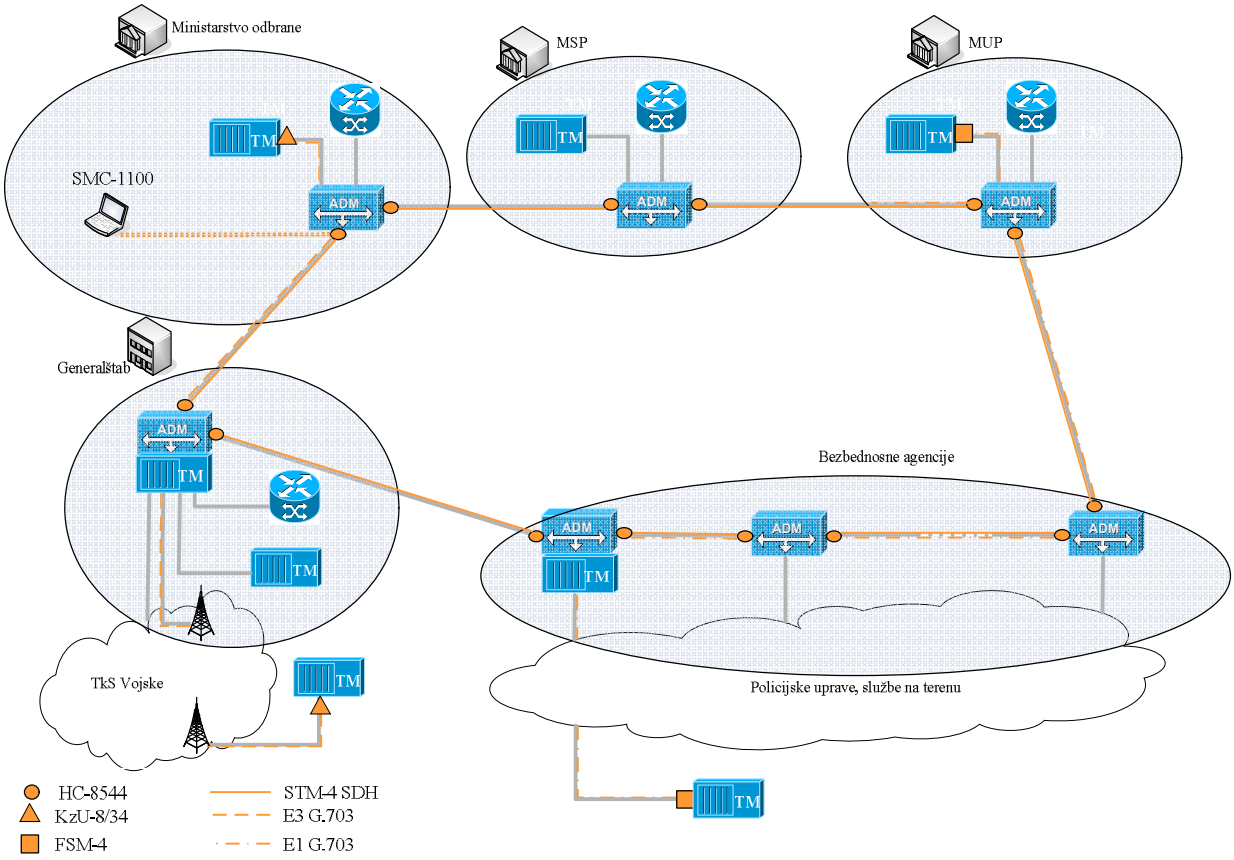
4.3.3 IMPLEMENTACIJA SISTEMA ZAŠTITE

Uvođenje novog sistema zaštite je veoma osetljiva aktivnost koja se mora pažljivo planirati i izvoditi po fazama, jer greške načinjene na početku uvođenja mogu kompromitovati njegovu ulogu, a i samu tajnost podataka. Zbog osetljivosti prelaza sa starog na novi sistem zaštite, ukoliko je to moguće, primenjuje se metod paralelnog rada, gde se zbog sigurnosti, uz novi sistem izvesni period zadržava i stari. Implementacija sistema zaštite podrazumeva obuku kadrova, testiranje sistema, puštanje u rad i funkcionisanje.

Obuku kadrova neophodno je izvršiti samo sa administratorima sistema zaštite i operaterima. Od samog početka implementacije oni moraju biti maksimalno uključeni. Prednost ovog rešenja je potpuna transparentnost u odnosu na krajnje korisnike čija edukacija za korišćenje može biti samo u vidu kratkih bezbednosnih uputstava.

Testiranje sistema zaštite u ovoj fazi mora da se odvija po posebnom planu. Važno je napomenuti da se zaključci iz verifikacionog testiranja moraju potvrditi.

Puštanje u rad realizuje se po delovima, a s obzirom na prstenastu strukturu mreže ne dolazi do prekida sobraćaja u transportnom delu mreže. Veoma važne aktivnosti prilikom puštanja u rad jesu: učitavanje kriptografskih parametara u uređaje i uvezivanje menadžment centra sa kripto uređajima.



Slika 21 Implementacija kripto uređaja u optičku telekomunikacionu mrežu

Funkcionisanje sistema zaštite nakon puštanja u rad mora biti intenzivno praćeno od strane projektnog tima ili drugih stručnih organa. Eventualne anomalije moraju biti odmah uočene i shvaćene, a njihova posledice sanirane zbog čega se odmah mora sačiniti akcioni plan za korigovanje sistema. U toku praćenja funkcionisanja sistema centralnu pažnju treba usmeriti na sigurnost i tajnost algoritma i bezbednost generisanja, distribucije, zamene i uništavanja ključeva.

4.4 PREGLED DOSTUPNIH REŠENJA NA TRŽIŠTU

U prethodnom delu, u kome su iznešeni osnovni zahtevi za kriptouređajima, nije razmotreno jedno od bitnih pitanja od koga zavisi stepen ispunjenje samih zahteva: Da li će rešenja primenjena u sistemu zaštite biti domaće ili strane proizvodnje? Iz navedenog pitanja, koje je više u domenu politike, proizilazi i niz drugih praktičnih pitanja i problema čije rešenje treba tretirati kao polazne osnove za izradu platforme ugovaranja sa proizvođačem.

Državnom politikom treba definisati pravce u kojima usmeriti aktivnosti, a kontinuitet te politike je važan zbog potrebe za stalnim povećanjem kapaciteta i kompatibilnosti postojećih sa novim rešenjima. Činjenica je da mnoge zemlje razvijaju sopstvene proizvode osloncem na domaće istraživačke i razvojne kompanije iz ove oblasti nad kojima vlade tih zemalja mogu ostvariti određeni vid kontrole radi sprečavanja spoljnih uticaja koji imaju za cilj provaljivanja u sistem zaštite i dolazak u posed tajnih informacija, što u konačnom i jeste svrha samog sistema zaštite. Međutim, mnogo je više onih zemalja, koje sa sopstvenim potencijalima, nisu u mogućnosti da razviju dovoljno kvalitetna rešenja, te se opredeljuju na uvoz. Zemlje u razvoju, kakva je naša, imaju ograničene potencijale, tako da su domaća rešenja vrlo retka i tek u razvoju. U ovom delu rada, sa tehničkog aspekta biće nepristrasno analizirana i strana i domaća rešenja. Prilikom analize treba imati u vidu da kompanije samo delimično objavljuju sopstvena dostignuća.

Nedostaci koja strana rešenja nose su sledeća:

- Nedovloljan i nejasan uticaj na kreiranje kriptografskog algoritma,
- Nedovoljno poznavanje sistemskog softvera u uređajima,
- Nemogućnost uticaja na dužinu ključeva,
- Mogućnost skrivenih vrata,
- Nemogućnost potpune verifikacije.

Ono što je pozitivno kod stranih proizvođača je:

- Obezbeđenje kriptozaštite na visokim bitskim brzinama,
- Razvijen sistem upravljanja ključevima,
- Sopstveno generisanje UK (tajnih ključeva),
- Posedovanje military verzija uređaja.

Kada govorimo o mogućnostima razvoja domaćih rešenja, svi nedostaci koji su navedeni za strana rešenja mogli bi biti predupređeni. Međutim, političke prilike u poslednjim godinama i usporen privredni razvoj onemogućili su stvaranje proizvoda koji bi pratili svetske trendove. Osnovni i gotovo nepremostiv problem predstavlja nemogućnost realizacije kriptozaštite na visokim bitskim brzinama.

4.4.1 CRYPTO AG

Crypto AG je švajcarska kompanija koja je stekla vodeće mesto u informatičko-komunikacijskoj bezbednosti za korisnike sa najvišim bezbenosnim potrebama. Najvažnije karakteristike koje ova kompanija ističe u nastupu na svetskom tržištu su:

- Veliko iskustvo kompanije i masovnost primene rešenja u svetu,
- Finansijska i pravna nezavisnost i nepostojanje izvoznih restrikcija i
- Obezbeđenje obuka i servisne podrške.

Iz bogate palete bezbednosnih rešenja izdvojene su HC-84xx i HC-85xx familije uređaja za zaštitu širokopojasnih telekomunikacionih mreža.

4.4.1.1 Karakteristike uređaja

U tabeli 5 prikazana su rešenja Crypto AG za *Link* i *Broadband* enkripciju iz grupa HC-84xx i HC-85xx, a u nastavku će biti prikazane njihove zajedničke karakteristike:

- Šifrovanje na spojnom putu u punom dupleksu do brzina od čak 10 Gbit/s,
- Potpuna transparentnost za servise,
- Automatska kriptološka sinhronizacija i resinhronizacija,
- Algoritam HCA-480 kod HC-84xx i HC-820 kod HC-85xx, prilagodljivi specifičnim zahtevima naručioca,
- Mogućnost kreiranja 10^{506} različitih početnih uslova za algoritam,
- Ugrađen generator slučajnih brojeva,
- Korisnički definisan MCK (*Master Communication Keys*), koji služi za generisanje komunikacijskog ključa (CK), čuva se u *tamper-proof* bezbednosnom modulu,
- Mogućnost kreiranja 10^{38} različitih MCK,
- Mogućnost unosa ključeva preko korisničkog interfejsa,
- *Beckup* ključeva na SDC (*Security Data Carrier*),
- *Offline* i *online* upravljanje ključevima pomoću SMC (*Security Management Centre*),
- Čitač smart kartica za učitavanje i snimanje podataka,
- *Tamper-proof* dizajn uređaja u 19“-nim jedinicama„
- Ručni i *Browser-based* korisnički RS-232 RJ45 interfejs,
- RJ12 alarmni interfejs,
- Lokalni i linijski interfejsi usklađeni sa preporukama ITU-T i IEEE,
- Upravljanje pomoću SNMPv1 protokola (*Simple Network Management Protocol),*
- Ugrađena oprema za testiranje i dijagnostiku,
- Temperaturni opseg od 0^0 do 50^0 C.

Link	Type	Application		Broadbend	Type	Application
T1	HC-8411	SatCom Leased Line Microwave WAN		Gigabit Ethernet	HC-8440	LAN, MAN, WAN, SAN, Leased Line Microwave SONET/SDH
E1	HC-8410			STM-1	HC-8441	
Fractional E1	HC-8420			STM-4	HC-8444	
E3	HC-8430			STM-1/STM-4	HC-8544	
T3	HC-8431			STM-16	HC-8545	
				STM-64	HC-8546	

Tabela 5. HC-84xx i HC-85xx uređaji Crypto AG

4.4.1.2 Security management

Secutity mangement center SMC-1100 (slika 22) nudi visok nivo bezbednosti pri upravljanju kriptoparametrima u mreži realizovanoj sa HC-84xx uređajima. Omogućava centralizovano upravljanje ključevima. SMC 1100 obuhvata:

- Upravljačku aplikaciju (*Management Application*) sa zaštićenim bazama podataka (*Secure Database*) za upravljanje kriptografskim parametrima, realizovanu pod Windows OS. Pruža korisnički interfejs administratoru za unos, pregled, *update* i distribuciju kriptografskih parametara namenjenih kripto uređajima. Podaci mogu biti distribuirani *offline* pomoću smart kartica i *online* preko posebnog hardvera.
- Bezbednosni modul (*Security Module*) namenjen za izvršenje svih bezbednosnih funkcija kao što su šifrovanje, kontrola pristupa i generisanje ključeva. Realizovan je kao hardver u *tamper-proof* okruženju sa integrisanim HCA-480 ili HCA-820 algoritmom i generatorom slučajnih brojeva.
- Distributer podataka (*Message Sheduler*) namenjen je za bezbednosno upravljanje podacima i distribuciju podataka do uređaja. Neophodno je da kroz mrežu bude povezan sa svim kripto uređajima kojima se upravlja.
- Čitač kartica (*Smart Card Reader*) koji omogućava bezbedno učitavanje, skladištenje i *offline* distribuciju.



Slika 22. SMC 1100

Da bi upravljanje ključevima bilo što bezbednije tj. da bi tajni simetrični ključ kojim se šifruju poruke sa sigurnošću ostao tajan, i pored ugrađenog generatora slučajnih brojeva, Crypto AG u sistemima sa HC-84xx i HC-85xx uređajima koristi 5 vrsta ključeva:

Master communication key (MCK) je tajni ključ definisan od strane administratora namenjen za davanje početnih uslova generatoru slučajnih brojeva za generisanje CK (*Communication key*) kojim se vrši šifrovanje komunikacije između kripto uređaja.

Master management key (MMK) definisan od strane administratora namenjen za zaštitu podataka na SDC kada se kripto parametri skladište ili distribuiraju *offline*.

Master unit key (MUK) je individualan za svaki kripto uređaj. Kada je prisutan u uređaju, može se koristiti za distribuciju MCK.

Master registration key (MRK) je tajni ključ definisan od strane administratora namenjen za generisanje MUK za svaki pojedinačan kripto uređaj.

Master factory key (MFK) je difoltni ključ definisan od strane proizvođača namenjen za zaštitu podataka na rezervnim SDC.

4.4.2 MOGUĆA DOMAĆA REŠENJA

U izveštaju o poslovanju za 2010. godinu, Iritel a.d., čija je osnovna delatnost razvoj i proizvodnja telekomunikacione opreme za domaće tržište, objavljuje završetak razvoja i verifikaciju uređaja FSM4 kao jednu od glavnih aktivnosti. Na Telfor-u 2011. restriktivno je dato samo nekoliko informacija o ovom uređaju:

FSM4 – Fleksibilni sigurnosni modul, uređaj za šifrovanje visokih performansi:

- Šifruje do 4 nezavisna E1 kanala sa G.703 interfejsima,
- Šifrovanje tačka – tačka, sinhrono sa simetričnim ključem,
- Automatska i univerzalna sinhronizacija šifre za sve tipove algoritma,
- Algoritmi: Blok i *stream* šifratori / standardni i vlastiti,
- Dužina ključa do 512 bita (zavisno od primenjenog algoritma),
- Celokupna jedinica je oklopljena i zaštićena od otvaranja,
- Provera uređaja i linka zatvaranjem odgovarajućih petlji,
- IP tip menadžmenta. Uređaj ima ugrađen Web server i SNMP agent,
- Ugradnja u fleksibilne multipleksere FM8 i FM2.

Primena ovakvog rešenja je ograničena na zaštitu E1 linkova i prilagođavanje Etherneta TDM strukturi, ali pošto predstavlja jedno od retkih domaćih rešenje, privlači veliku pažnju.

U serijama uređaja Iritela KFE (Ethernet preko TDM), KTP (TDM preko IP/MPLS) i MGE (upravljivi Etherenet svičevi) opciono će se ugrađivati AES 128/192/256 moduli za šifrovanje podesivi za različite TDM signale (E1, E3, X.21/V.11 NRZ, V35) sa fleksibilnim ključem i pristupnom kontrolom.

S obzirom da su razvoj i verifikacija ovih domaćih rešenja tek završeni, neophodno ih je što pre uzeti u razmatranje. Nedostatak koji se odmah uočava je ograničen protok što bi morao biti podsticaj za pronalaženje novih rešenja za veće bitske brzine. Najlogičnije bi bilo da razvoj novih domaćih rešenja bude inicaran i stimulisan od državnih institucija koje će, u najvećoj meri, ta rešenja u budućnosti i implementirati u svoje telekomunikacione sisteme.

4.4.3 OSTALA PRIMENLJIVA REŠENJA

Čajavec a.d. je Banjalučka kompanija koja egzistira još iz zajedničke države sa military rešenjima za kriptozaštitu, a svoje iskustvo i dostignuća danas, kroz proizvode nastoji plasirati na tržište Bosne i Hercegovine i Srbije.

Rešenja prikazana na slici 23, prema prezentaciji proizvođača, imaju algoritam implementiran u programibilnoj strukturi XILINX. To omogućava korisniku da implementira vlastiti (*custom*) algoritam. Ovaj podatak čini proizvode Čajaveca zanimljivim, pogotovo za vojnu upotrebu.



MCDU-2 **KzU 8/2k** **KzU 8/34**

Slika 23. Specijalni uređaji Čajavec a.d.

Najvažnije karakteristike prikazanih uređaje su sledeće:

- Ugrađen generator slučajnog niza kod KzU 8/2k i KzU 8/34 i pseudoslučajni generator kod MCDU-2,
- Generisanje 128-bitnog UK (unutrašnjeg ključa) kojim se vrši šifrovanje vrši se ugrađenim generatorom koji se inicijalizuje SK (spoljašnjim ključem) dužine 1024 bita,
- Autorizacija više vrsta korisnika preko lokalnog interfejsa (tastatrurl, displej i čitač smart kartica),
- SPI bus (*Serial Peripherial Interface)* komunikacija upravljačkog interfejsa sa unutrašnjosti uređaja,
- Obezbeđen rad u punom dupleksu,
- Tipovi interfejsa:
    - MCDU-2: G.703 75/120 Ohm do 2048 kbit/s (64, 128, 256, 512, 1024 ili 2048 kbit/s), pri čemu se ulazna brzina automatski detektuje
    - KzU 8/2k (radi dvokanalno):
      - G.703: 75/120 Ohm E1, 75 Ohm E3,
      - EUROCOM A/B, AMI-code, ±0.5V, 130 Ohm, 2048 kbit/s (i druge brzine u opsegu 256 kbit/s - 4096 kbit/s),
      - V.11 - do 10 Mbit/s.
    - KzU 8/34:
      - Podržava interfejse identične KzU 8/2k,
      - G.703 75 Ohm, E3.

- Izbor vrste interfejsa programski ili automatski na bazi detektovanih signala,
- Postojanje oklopa koji obezbeđuje zaštitu od KEMZ-a,
- Izuzetne mehaničke karakteristike svojstvene military standardima (otpornost na vibracije, padove i ekstremne klimatske uslove).

5. ZAKLJUČAK

U ovom radu je ukazano na nužnost zaštite podataka u optičkim telekomunikacionim mrežama na nižim slojevima OSI modela ne zanemarujući zaštitu na mrežnom i aplikativnom nivou. Takođe je identifikovana potreba za razvojem sopstvenih kriptografskih rešenja radi postizanja potpune sigurnosti. Predmet istraživanja rada jeste iznalaženje najoptimalnijih rešenja za implementaciju u sistem zaštite konkretne telekomunikacione mreže i upoznavanje sa javno dostupnim rešenjima u svetu i kod nas.

U osnovi zaštite podataka u telekomunikacionim mrežama nalazi se kriptografija. Kriptografija je veoma složena i dinamična oblast koja teorijske osnove nalazi u matematici, a u praksi se bazira na upotrebi kriptografskog sistema koji se sastoji od kriptografskog algoritma, jednog ili više ključeva, sistema za upravljanje ključevima i podataka u vidu otvorene i šifrovane poruke. Praktična primena kriptografije je sve šira u raznim oblastima informacionih tehnologija pa i u telekomunikacionim mrežama. Ona zahteva upotrebu savremenih i sigurnih kriptografskih algoritama čije stvaranje čini suštinu kriptografije. Dužina ključa se permanentno povećava sa rastom procesorske moći i dekriptorskih sposobnosti potencijalnih napadača. Manipulacija sa ključevima je veoma bitna zbog očuvanja njihove tajnosti pa zahteva posebnu pažnju.

Zbog svojih fizičkih i funkcionalnih karakteristika, ove mreže su veoma često izložene različitim vrstama pretnji i napada. Sprečavanje ugrožavanja bezbednosti informacija koje se njima prenose podrazumeva implementaciju simetričnog kriptografskog sistema. Da bi se implementiralo određeno rešenje, najpre se moraju, na bazi analize komunikacionih karakteristika mreže, izneti zahtevi koje to rešenje treba da ispunjava, a zatim izvršiti izbor jednog od nekoliko mogućih rešenja.

Profilisanje konkretnog rešenja proističe iz sledeća dva zahteva:

- Mora se postići zahtevani nivo zaštite s obzirom na važnost informacija što podrazumeva potpunu kontrolu svih elemenata kriptografskog sisstema,
- Primenjeno rešenje ne sme ugroziti kvalitet prenetih informacija.

Ako se žele zaštititi kompletni podaci na spojnom putu, neminovna je upotreba stranih komercijalnih proizvoda koji omogućavaju zaštitu na visokim bitskim brzinama. Međutim, oni sa sobom nose određni nivo nesigurnosti zbog nedovoljnog poznavanja sistemskog softvera i nedovoljnog uticaja na kreiranje algoritma.

U suprotnom, ako se selektivno štite samo određene komunikacije, moguć je razvoj i implementacija domaćih rešenja sa mnogo skromnijim komunikacionim karakteristikama, ali sa većim mogućnostima kontrole kriptografskih elemenata. Za prelazni period moguće je implementirati oba rešenja istovremeno uz jasnu viziju razvoja sopstvenih proizvoda za veće bitske brzine. Razvoj domaćih rešenja trenutno je limitiran ekonomskim razvojem, skromnim iskustvima kao i nedovoljnom spremnošću države da ulaže u razvoj i proizvodnju u ovoj oblasti. Ukoliko se želi osigurati bezbednost informacija važnih za nacionalnu bezbednost i suverenost zemlje morali bi se učiniti konkretniji koraci na tom planu.

LITERATURA

[1] Bruce Schneier, *Applied cryptography,* Second Edition, John Wiley & Sons, 1996, USA,

[2] Dragan Pleskonjić, Nemanja Maček, Borislav Đorđević, Marko Carić, *Sigurnost računarskih sistema i mreža*, Mikro knjiga, 2007, Beograd,

[3] Milan Milosavljević, Gojko Grubor *Osnove zaštite informacija, metodološko-tehnološke osnove,* Univerzitet SINGIDUNUM, 2010, Beograd,

[4] Marija Furdek, *Physical-Layer Attacks in Optical WDM Networks and Attack-Aware Network Planning*, Dept. of Telecommunications, Faculty of Electrical Engineering and Computing, University of Zagreb,

[5] Mladen Veinović, Miroslav Ćajić, Bogdan Brkić, *Upravljanje kriptološkim ključevima*, 8. Naučni skup sa međunarodnim učešćem Sinergija 2011,

[6] CarNet CERT, LS&S, *DES Algoritam*, 2003, Zagreb,

[7] www.crypto.ch/ (Visited November 2011),

[8] www.cajavecsu.com/ (Visited November 2011),

[9] www.iritel.com/ (Visited November 2011),

[10] http://www.armedforces-int.com/article/ (Visited September 2011),

[11] Vladimir M. Čorak, *Uvod u SDH mreže*, VF Tel. d.o.o, 1995, Beograd,

[12] Regis J. (Bud) Bates, *Broadband Telecommunications Handbook*, McGraw−Hill, 2002, USA,

[13] Petar Uzunović, *Elektronske poslovne komunikacije*, Univerzitet Singidunum,

[14] Andreja Samčović, Goran Marković, *Transportne mrežne tehnologije za distribuciju IPTV sadržaja*, Saobraćajni fakultet, 2010, Beograd,

[15] Dejan M. Gvozdić, *Trendovi razvoja optičkih telekomunikacionih sistema,* Elektrotehnički fakultet, Beograd

[16] Dario Franolić, Milorad Jokanović, *Transportni Ethernet Carrier Ethernet*, Telekom Srbija a.d, Beograd,

[17] Petar Knežević, Miroslav Ilić, Ninko Radivojević, *O primeni Carrier Ethernet i NG-SDH tehnologija u transportnim mrežama,* Iritel a.d. Beograd,

[18] Jovan Radunović i Petar Matavulj, *Tehnološki izazov u optičkim telekomunikacijama*, Elektrotehnički fakultet, Beograd,

[19] Danojlić, M.,Nebojša, *Perspektive razvoja DWDM metro mreža*, Telefonkabl a.d, Beograd,

[20] *FTTH Council Europe, Annual Report April 2010 – April 2011*,

[21] European FTTH Forecast, 2010 – 2015.