

**ПРИЛОЖЕНИЕ НА ТЕОРЕМАТА ЗА ОСТАТЪЦИТЕ ПРИ ЗАЩИТА НА
ДАННИТЕ В ИНФОРМАЦИОННИТЕ СИСТЕМИ****APPLICATION OF THEOREM OF RESIDUALS FOR DATA PROTECTION
IN INFORMATION SYSTEMS****Мариана Ванкова**

ТУ-Габрово

Кат. " Приложна информатика "

Abstract

The main reason for creating of an automatic information system is to be provided necessary data of people working in a particular organization. The theorem of residuals allows data protection when processed.

Keywords: theorem of residuals, module codes.

ВЪВЕДЕНИЕ

В съвременните условия на обществена дейност съществено значение придобиват въпросите, свързани с изграждането, използването и приложението на различни технически средства и системи за управление на тази дейност. Компютърната техника със своите възможности за едновременно и скоростна обработка на големи информационни масиви, се явява една предпоставка за успешно решаване на тези въпроси.

Разрастването на компютърната индустрия, увеличаването броя на производителите на компютърна техника и различни периферни устройства за въвеждане, извеждане и съхраняване и обмен на информация, води до все по-широко използване на компютърните системи в различни сфери на нашето ежедневие. Като потвърждение на голямото значение на тези въпроси, могат да се посочат разработваните системи за информационно обслужване в такива области, като образование, здравеопазване, транспорт, търговска и туристическа дейност, реклама, банково и застрахователно дело и др.

Информационната система представлява компютъризирана система, която намира приложение за събиране, съхранение, обработка на данни и вземане на решение.

Основните компоненти при обработването на информацията могат да бъдат структурирани до следните пет групи: хора, процедури, хардуер, софтуер и данни.

Основна причина за създаването на една автоматизирана информационна система, е да бъде осигурена необходима информация на хората работещи в дадена организация. Потребителите са тези които директно оперират с информация. Поради това при създаването на всяка информационна система е необходимо максимално да се задоволят нуждите на потребителите на тази система, за да може тя с успех да изпълнява своите функции и предназначение.

Основните функции на всяка информационна система могат да се структурират по следния начин:

- въвеждане на данни с различна структура в системата;
- осигуряване на бърз достъп до съхраняваната информация;
- бърза обработка и анализ на съхраняваните данни;
- извеждане на исканата от потребителя информация;
- редактиране и модифициране на извежданата информация.

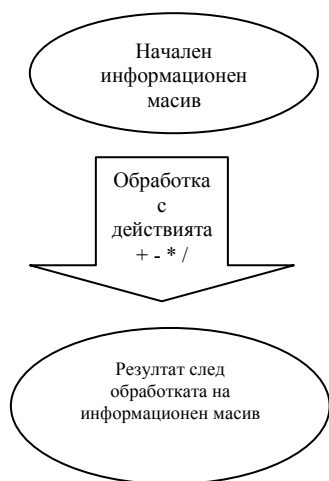
Голямото многообразие от ресурси и едновременно достъп на потребители с различни

права и способности е причина за неупълномощен достъп до данните в информационните системи [1]. Това налага търсене на начини и средства за предотвратяване на този нежелан достъп.

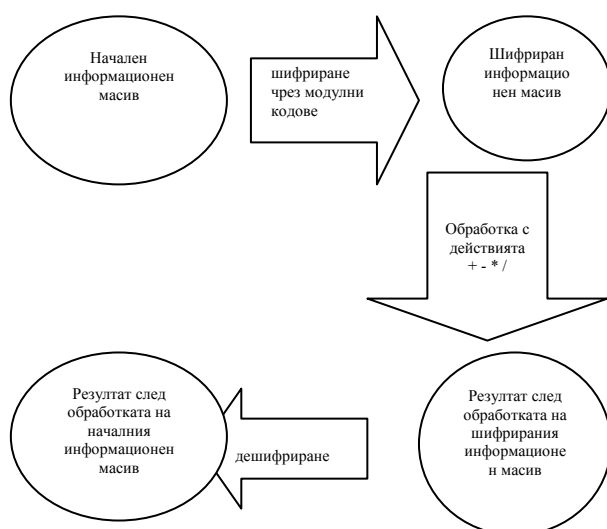
В представения доклад се разглежда обработката на данни в информационни системи защитени посредством теоремата за остатъците.

ОБРАБОТКА НА ДАННИ В ЗАЩИТЕН ВИД

На фиг. 1а. и 1б. се представя обработката на информацията в незащитен и защитен вид.



Фиг.1а. Обработка на данни в незащитен вид



Фиг.1б. Обработка на данни в защитен вид

Ако примерен информационен масив от данни се шифрира и получените след обра-

ботката с посочените действия резултати се дешифрират (фиг. 1б.), се получава резултат, който би се получил ако първоначалния масив се обработва със същия математически апарат от действия показан на фиг. 1а.

Съгласно китайската теорема за остатъците, всяко цяло положително число не по-голямо от произведението на определени модулни числа може еднозначно да се възстанови, ако са известни разликите спрямо тези модулни числа.

Получаване на модулна форма на числото X като модулни числа C₁, C₂, C₃ се представя по следния начин:

$$\begin{aligned}\frac{X}{C_1} &= Q_1 + \frac{R_1}{C_1} \\ \frac{X}{C_2} &= Q_2 + \frac{R_2}{C_2}\end{aligned}\quad (1)$$

$$\frac{X}{C_3} = Q_3 + \frac{R_3}{C_3}$$

където: X- число, C₁, C₂, C₃ – модулни числа. Модулната форма на числото XX по C₁, C₂, C₃ включва R₁, R₂, R₃.

За да е възможно еднозначно представяне на числата в диапазона 0 ≤ C < (C₁, C₂, C₃) е необходимо C₁, C₂, C₃ да бъдат взаимно прости числа.

Модулната форма на числото XX по C₁, C₂, C₃ включва R₁, R₂, R₃ и би се представила по следния начин:

$$|XX|_{C_1 C_2 C_3} = R_1 R_2 R_3 \quad (2)$$

Нека като модулни числа (C) се приемат C₁=3, C₂=4 и C₃=5. Всички числа в диапазона 0 ≤ C < 60 (C₁.C₂.C₃=60) могат съгласно китайската теорема за остатъците да бъдат представени чрез своите модулни разлики спрямо числата C₁, C₂, C₃.

Модулното представяне на числата 37 и 53 спрямо стойностите за C₁=3, C₂=4 и C₃=5 ще изглежда по следния начин:

$$\begin{aligned}37:3 &= 12.3 + 1 & 37:4 &= 9.4 + 1 & 37:5 &= 7.5 + 2 \\ 53:3 &= 17.3 + 2 & 53:4 &= 13.4 + 1 & 53:5 &= 10.5 + 3\end{aligned}$$

Конкретните модулни представяния на числата 37 и 53 ще изглеждат:

$$\left| 37 \right|_{3,4,5}=112 \quad \left| 53 \right|_{3,4,5}=213$$

където $\left| XX \right|_{C_1, C_2, C_3}$ е модулна форма на числото X по C_1, C_2, C_3 .

Тази форма на представяне ще бъде означена като модулен код на числото XX спрямо числата C_1, C_2, C_3 .

МОДУЛНИТЕ КОДОВЕ КАТО СРЕДСТВО ЗА ЗАЩИТА НА ДАННИТЕ

Нека примерен информационен масив от данни да се представи като една съвкупност от отделни числа X_i ($i=1,2,3..n$)

При защита данните в информационната система всяка една отделна част се разглежда като число, което трябва да се замени със своя модулен код по три предварително определени взаимно прости числа C_1, C_2 , и C_3 . Всяка отделна част се заменя с модулния си код:

$$X_i \Leftrightarrow R_{i,1} R_{i,2} R_{i,3}$$

където " $\Leftrightarrow$ " е еднозначно съответствие между X_i и $R_{i,1} R_{i,2} R_{i,3}$.

Модулните числа C_1, C_2 , и C_3 имат смисъл на ключ [4,5]. Процесът на дешифриране (фиг. 1б.), при известен модулен код и ключ, се свежда до решаване на обратната задача: по три числа $R_{i,1} R_{i,2}$ и $R_{i,3}$ и елементите C_1, C_2 , и C_3 от ключа да се намерят такива числа Q_1, Q_2 , и Q_3 за които са в сила следните равенства:

$$X=C_1.Q_1+R_1 \quad (3)$$

$$X=C_2.Q_2+R_2$$

$$X=C_3.Q_3+R_3$$

Обработвайки защитената информация посредством теоремата за остатъците трябва отделни цифри от модулното представяне да се обработват по модул спрямо съответното модулно число без да се реализира "заем" или пренос към съседна цифра.

Ако приемем, че модулното представяне е направено спрямо числата $C_1=5$ и $C_2=6$ според теоремата за остатъците всички числа в диапазона 0-29 могат да се представят като модулни кодове от две цифри. $\left| X_1 X_2 \right|_{5,6}$. Първата цифра X_1 може да приеме стойност в диапазона 0-4 и втората цифра от модулното представяне в диапазона 0-5.

При изпълнение на действията посочени на фиг. 1б. над информацията представена като модулни кодове спрямо числата $C_1=5$ и $C_2=6$, първите цифри (X_1) се обработват по модул 5, а вторите (X_2) по модул 6.

МОДУЛНИ КОДОВЕ И АРИТМЕТИЧНИ ДЕЙСТВИЯ

Особеностите на модулните кодове за всяко от действията (събиране, изваждане, умножение и деление) могат да се онагледят с няколко примера.

На фиг. 2. е реализирано действие сумиране

	$C_1=5$	$C_1=3$
	$C_2=6$	$C_2=5$
		$C_3=7$
7_{10}	21	120
+	+	+
9_{10}	43	042
$\overline{16}_{10}$	$\overline{14}$	$\overline{112}$

Фиг. 2. Изпълнение на действие сумиране

На фиг. 3. е реализирано действие изваждане

	$C_1=5$	$C_1=3$
	$C_2=6$	$C_2=5$
		$C_3=7$
32_{10}	22	224
-	-	-
21_{10}	13	010
$\overline{11}_{10}$	$\overline{15}$	$\overline{214}$

Фиг. 3. Изпълнение на действие изваждане

На фиг. 4. е реализирано действие умножение

	$C_1=5$	$C_1=3$
	$C_2=6$	$C_2=5$
		$C_3=7$
12_{10}	20	025
*	*	*
5_{10}	05	205
$\overline{60}_{10}$	$\overline{00}$	$\overline{004}$

Фиг. 4. Изпълнение на действие умножение

На фиг. 5. е реализирано действие деление

	$C_1=5$	$C_1=3$
	$C_2=6$	$C_2=5$
		$C_3=7$
48_{10}	30	036
:	:	:
12_{10}	20	025
$\overline{6_{10}}$	$\overline{10}$	$\overline{016}$

Фиг. 5. Изпълнение на действие деление

ЗАКЛЮЧЕНИЕ

Разглежданият метод за шифриране чрез използване на модулни кодове, може да се използва за защита на данни в информационните системи. Целесъобразно е информационните масиви да се разделят на блокове и всеки да се защитава с отделни комбинации от ключове от две нива.

Ключовете от първото ниво могат да се използват за защита на първия блок от информационния масив, а ключът от второ ниво ще определи зависимостта по която ще се променя големината на отделните блоко-

ве X_i от информационния масив, както и зависимостта по която ще се променят ключовете (C_i), дължината на всеки от ключовете и неговата стойност.

Възможността за обработка на данните в защитен вид може да се използва и при други операции от действия. Действието умножение и деление може да се представи като операции сумиране и изваждане, степенуването като последователност от умножение и сумиране, коренуването като последователност от деление изваждане. От тук следва изводът, че освен показаните възможности могат да се извършват и други математически обработки трансформирайки действия от по-висок ред в действия от по-нисък ред.

ЛИТЕРАТУРА

- [1] Антонов П. "Криптография в компютърните комуникации", Варна, 2000.
- [2] Блейхут Р. – "Быстрые алгоритмы цифровой обработки сигналов"; Москва; "Мир"; 1989.
- [3] Fumy W., Landrock P. – "Principles of Key Management"; IEEE Jornal on Selected Aresa in Communications; vol. 11;N. 5; 1993.
- [5] Menezes A., Oorschot P., "Handbook of Applied Cryptography", CRC Press, 1996.