Годишник на секция "Информатика" **Annual of "Informatics" Section**
Съюз на учените в България **Union of Scientists in Bulgaria**
Том 1, 2008, 112-116 **Volume 1, 2008, 112-116**

ИЗПОЛЗВАНЕ НА ОБОБЩЕНО-МРЕЖОВ МОДЕЛ НА КЛАСИЧЕСКА СТРУКТУРА НА КРИПТОГРАФСКА СИСТЕМА ЧРЕЗ ИЗПОЛЗВАНЕ НА СИМЕТРИЧЕН КЛЮЧ

Ивелина Вардева

Университет "Проф. Асен Златаров", Бургас 8000, България
e-mail: iveto@btu.bg

Резюме: В статията се разглежда класическа структура на криптографска система за шифриране на данни. Използван е апарата на обобщените мрежи за моделиране процеса на класическа структура на криптографска система чрез използване на симетричен ключ.

1. Въведение

Криптографията представлява основата на съвременната on-line икономика. Тя дава възможност да се съхранява поверителна информация или да се изпраща през несигурни мрежи по такъв метод, че тя да не може да бъде прочетена от никой, с изключение на този, за когото е предназначена.

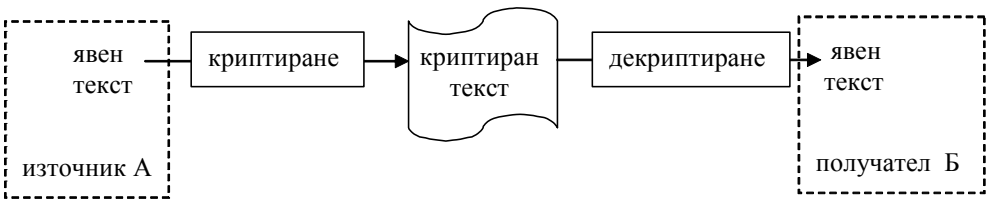
Основната функция на криптографията е да се защитят данните от неоторизиран достъп или неоторизирано подменяне на данните. Функциите на защита криптографията осъществява чрез идентификация на участниците в комуникационния процес посредством обмяна на ключове за удостоверяване на самоличност [7, 8].

Криптирането само по себе си представлява метод за изменение на съобщение по такъв начин, че неговото съдържание да стане неразпознаваемо за всеки, който не разпознава метода на изменение. Декрептирането представлява обратната операция на криптирането т.е. трансформиране на криптираното съобщение в явен вид. Самото правило за преобразуване на данните в неразбираеми и обратното има възстановяване се нарича криптографски алгоритъм. Явен текст наричаме оригиналното съобщение преди да бъде обработено с криптографски алгоритъм. След криптирането на явния текст получената символна поредица наричаме криптиран текст. За да може обмена на данни да е безпогрешен се използват протоколи за верификация т.нар. криптографски протокол [3, 4]. Съвкупността от криптографски протоколи и алгоритми се нарича криптографска система. [7, 8].

Криптографията е метод да се защитава информацията, като се трансформира в нечитаем формат чрез използване на ключове. Криптографския ключ наричаме множеството от символи което се използва за криптиране или декриптиране на съобщенията.

Разгледана е общата структура на криптографска система представена чрез модела на обобщени мрежи [1, 2, 6]. На базата на обобщените мрежи са реализирани оптимални начини за протичане на реалните процеси за криптиране със симетричен ключ [7, 8]. Използвана е класическа едноключова криптографска система за защита на информацията, т.е. използван е един ключ както за криптиране така и за декриптиране. Този ключ е секретен, а самия алгоритъм се нарича алгоритъм със секретен ключ, поради причината, че за криптирането и декриптирането се използва един и същи ключ той се нарича симетричен, а алгоритъма - симетричен алгоритъм. Основно предимство на конвенционалното крептиране е бързината за криптиране и декриптиране на съобщенията, което е особено подходящо да се използва за съобщения, които няма да се изпращат. Конвенционалното криптиране като самостоятелно средство за изпращане на сигурна информация, може да бъде твърде скъпо поради трудностите, свързани с разпространението на ключовете за крайните потребители. За да могат да комуникират сигурно изпращачът и получателят, използващи конвенционална криптография, трябва предварително да имат съгласуване за ключа, който ще използват и да го пазят в тайна между тях. При условие, че те се намират във физически различни региони, трябва да се доверят на някакъв сигурен канал, за да предотвратят разкриването на ключа при предаването. Ако ключа бъде засечен при предаването му, може по-късно да бъде използван за прочитане или модифициране на информацията, подписана и удостоверена с този ключ.

Според [7, 8] основната схема на криптографски алгоритъм с използване на симетричен ключ е:



(1) $C=E_k(P)$, където

P – съобщението в явен вид

E_k – симетричен криптографси алгоритъм и секретен криптографски ключ - криптиране

C – е полученият шифриран текст – криптограмата

(2) $D_k(C)=P$, където

C – е шифриран текст – криптограмата

D_k – симетричен криптографси алгоритъм и секретен криптографски ключ – дешифриране

P – съобщението в явен вид

Изходното съобщение в явен вид се подготвя от източник А за предаване към получателя Б. За да се шифрира явния текст трябва да се обработи със симетричен криптографски алгоритъм и секретен симетричен криптографски ключ, който е общ и за двамата потребители. Източникът А трябва да разполага с необходимите

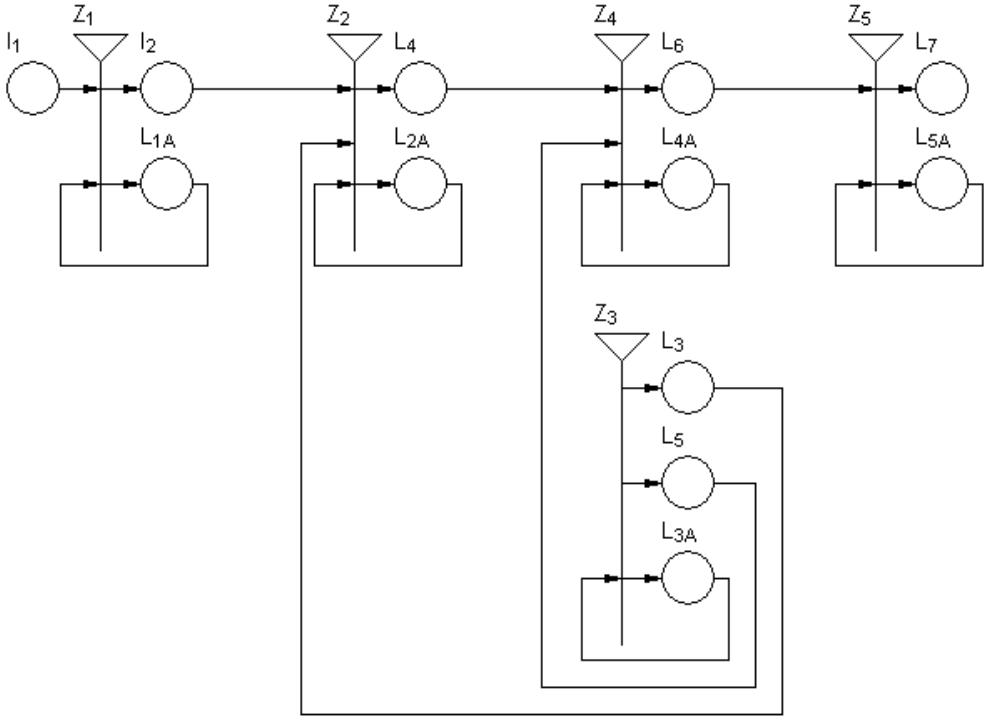
криптографски средства, за да може да криптира явния текст. Полученият шифрован текст се нарича криптограма, която се предава по незащитен канал и се обработва в криптографското устройство на получателя Б със същия криптографски алгоритъм и криптографски ключ, с които източника А криптира явния текст – по този начин се реализира дешифриране, по този метод получателя Б приема съобщението в явен вид [7].

Представянето на основна схема на симетричен ктюриптографски алгоритъм чрез използване на модела на обобщените мрежи [1, 2, 6] ни дава възможност за моделиране на целия криптографски процес.

2. Обобщено мрежови модел

Първоначално са дадени следните ядра включени в обобщената мрежа:

- на позиция l_1 влиза - α_{1}- ядро с характеристика „явен текст”.
- на позиция L_{1A} – α_2 - ядро с начална характеристика “явен текст за изпращане”;
- на позиция L_{3A} - γ - ядро с начална характеристика “криптографски ключове и алгоритми”;
- на позиция L_{5A} – α_3 - ядро с начална характеристика “получен явен текст”;



Фиг. 1

Разработен е обобщен мрежови модел с въведено множеството от преходи А които:

A= { Z_1, Z_2, Z_3, Z_4, Z_5}, където преходите описват следните процеси:

Z_1 = “ Задачи извършени от източник А”

Z_2 = “ Задачи извършени от криптографско устройство 1”

Z_3 = “ Задачи извършени от генератора на ключове”

Z_4 = “ Задачи извършени от криптографско устройство 2”

Z_5 = “ Задачи извършени от източник Б”

Преходите имат следното описание:

$Z_1 = < \{l_1, L_{1A}\}, \{l_2, L_{1A}\}, R_1, M_1, \vee(l_1, L_{1A}) >$

$R_1 =$

	l_2	L_{1A}
l_1	*false*	*true*
L_{1A}	*true*	*true*

Влизащото ядро α_1 се добавя към ядрото α_2, постъпващо в позиция L_{1A}. Ядрото α_2 (от позиция L_{1A}) се разцепва на две еднакви α_2’ и α_2” ядра, които постъпват съответно в позиции l_2 и L_{1A}. След прехода ядрото α_2” (от позиция l_2) излиза със следната текуща характеристика „изпращане на явен текст”.

$Z_2 = < \{ l_2, l_3, L_{2A}\}, \{l_4, L_{2A}\}, R_2, \vee(l_3, \wedge(l_2, L_{2A})) >$

$R_2 =$

	l_4	L_{2A}
l_2	*true*	*false*
l_3	*false*	*true*
L_{2A}	*true*	*true*

Влизащите ядра α_2” (от позиция l_2) и γ’ (от позиция L_{2A}) се сливат в едно δ ядро, което получава новата си характеристика въз основа на (1).

$Z_3 = < \{L_{3A}\}, \{ l_3, l_5, L_{3A}\}, R_3, \vee(L_{3A}) >$

$R_3 =$

	l_3	l_5	L_{3A}
L_{3A}	$W_{3A,3}$	$W_{3A,5}$	*true*

$W_{3A,3}$= “съгласуван е симетричен криптографски ключ и алгоритъм”;

$W_{3A,5} = W_{3A,3}$;

Ядрото γ (от позиция L_{3A}) се разцепва на две еднакви γ’ и γ” ядра, които постъпват съответно в позиции l_3 и l_5. Ядрата γ’ и γ” получават характеристика „симетричен криптографски ключ и алгоритъм”.

Прехода Z_3 се активира на първа стъпка на модела.

$Z_4 = < \{l_4, l_5, L_{4A}\}, \{ l_6, L_{4A}\}, R_4, \vee(l_5, \wedge(l_4, L_{4A})) >$

$$R_4 = \begin{array}{c|cc} & l_6 & L_{4A} \\ \hline l_4 & true & false \\ l_5 & false & true \\ L_{4A} & true & true \end{array}$$

Влизащите ядра δ (от позиция l_4) и γ" (от позиция L_{4A}) се сливат в едно α_2" ядро, което получава новата си характеристика въз основа на (2).

$Z_5 = < \{l_6, L_{5A}\}, \{l_7, L_{5A}\}, R_5, \vee(L_{5A}) >$

$$R_5 = \begin{array}{c|cc} & l_7 & L_{5A} \\ \hline l_6 & false & true \\ L_{5A} & true & true \end{array}$$

Влизащото ядро α_2" се разцепва на две еднакви α_{21}'' и α_{22}" ядра. Едното пеминава през преходаи постъпва в позиция l_7 , а другото се слива ядрото α_3, в позиция L_{5A}. След прехода ядрото от позиция l_7излиза със следната характеристика „явен текст".

3. Заключение

Основното предимство на конвенционалното криптиране е, че то е много бързо и е много полезно е при криптиране на информация, която няма да се изпраща през обществената незащитена мрежа Internet – т.е. предаване на шифрирани данни по несигурен канал. Конвенционалното криптиране като самостоятелно средство за изпращане на сигурна информация, само по себе си е много скъпо поради трудностите, свързани с разпространяването на ключовете за изпращащата и приемащата работни станции.

Обобщено-мрежовия модел описва основната концепция от теорията на криптографията за конвенционално криптиране чрез класическа структура на криптографска система с използване на симетричен ключ. Модела позволява разглежда различните етапи от протичането на процеса и позволява неговата симулация и поведението му в бъдеще.

Литература

[1] Atanassov, K., Generalized nets, World Scientific, Singapore, New Jersey, London1991

[2] Piper, F., Murphy, S., „Cryptography: A Very Short Introduction", Oxford University Press 2002

[3] Vardeva, I., Sotirov, S., Generalized Net model of SSL with intuitionistic fuzzy estimations, Notes on IFS Proceendings of the Eleventh International Conference on Intuitionistic Fuzzy Sets, Sofia , 28-30 April 2007, Volume 13

[4] Vardeva,. I, SSL modeling by the apparatus of Generalized Net, Sixth Int. Workshop on GNs, Sofia, 17 Dec. 2005, 29-33

[5] Wheeler, D., Secure Programming for Linux and Unix HOWTO, 2002

[6] Атанасов, К., „Въведение в теорията на обобщените мрежи”, Бургас 1992г.
[7] Нонинска, И., “Криптография”, София 2005 г.
[8] Христов, Х., Трифонов, В., „Надеждност и сигурност на комуникациите”, София 2005 г.