Нови метод за генерисање савршене ендоморфне шифре са минималним бројем кључева

Милош Банђур, Анђелија Раичевић, Ђоко Банђур, Бранкица Поповић

***Садржај* — У овом раду је изложен метод за генерисање теоријски савршено отпорне шифре према криптонападу на основу једног ухваћеног криптограма. Конструисана шифра је ендоморфна и са минималним бројем кључева, што је посебно важно са аспекта практичне реализације. Изведена је расподела вероватноће симбола у шифрованом тексту и извршена анализа шифре са аспекта отпорности према наведеном криптонападу, при чему је доказана њена савршена теоријска отпорност.**

***Кључне речи* — азбука отвореног текста, азбука шифрованог текста, ендоморфна шифра, кључ, кључевни низ, криптоаналитичар, криптограм, криптонапад, отворени текст, савршена шифра, шифра, шифровани текст.**

I. Увод

Шифарски метод који у овом раду предлажемо и анализирамо припада системима са тајним кључем (симетричним криптосистемима).

У теорији криптографске отпорности уведен је појам савршене шифре, као шифре која обезбеђује теоријски савршену отпорност за одређену врсту криптонапада. Клод Шенон је окарактерисао шифре које су савршене у односу на криптонапад на основу једног шифрованог текста које се још и називају - шифре савршене по Шенону [1]-[3]. Клод Шенон је назвао шифру савршеном, ако за било који отворени текст, сазнања која могу да се добију из њему одговарајућег шифрованог текста, не пружају било какву информацију о отвореном тексту, са изузетком, можда, његове дужине. Другим речима, за савршене шифре важи да се апостериорне вероватноће отворених текстова (добијене у току анализе криптограма) подударају са њиховим априорним вероватноћама.

Милош Банђур, Факултет техничких наука у Косовској Митровици, Кнеза Милоша 6, 38220 Косовска Митровица, Србија; (e-mail: bandjo@ptt.rs), тел: 381-28-425320, факс: 381-28-425322.

Анђелија Раичевић, Факултет техничких наука у Косовској Митровици, Кнеза Милоша 6, 38220 Косовска Митровица, Србија; (e-mail: andjraic@eunet.rs), тел: 381-28-425320, факс: 381-28-425322.

Ђоко Банђур, Факултет техничких наука у Косовској Митровици, Кнеза Милоша 6, 38220 Косовска Митровица, Србија; (e-mail: dbandjur@gmail.com), тел: 381-28-425320, факс: 381-28-425322.

Бранкица Поповић, Полицијска академија, Хумска 22, 11080 Београд, Србија, (e-mail: cica@ptt.rs), тел/факс: 381-11-3161444.

Појам савршене шифре уопштен је и за неке друге криптонападе [3]: шифре савршене по К. Шенону отпорне на подметање (имитацију или замену) шифрованог саопштења; шифре савршено отпорне на напад на основу неуређеног скупа криптограма добијених истим кључем ($U(L)-$ отпорне шифре); $U(L)-$ отпорне шифре које поседују најбоље параметре отпорности у односу на подметање; шифре савршено отпорне према нападу на основу неуређеног скупа криптограма од којих неки могу бити добијени шифровањем истог отвореног текста различитим кључевима ($S(L)-$ отпорне шифре); шифре савршено отпорне за уређене скупове отворених и шифрованих текстова ($O(L)-$ отпорне шифре); шифре савршено отпорне у односу на напад на основу познатог отвореног текста ($M(L)-$ отпорне шифре); шифре савршене по кључу.

С једне стране, савршена шифра је посебно добра због тога што испробавањем свих кључева на ухваћени криптограм не постижемо ништа у смислу одређивања отвореног текста. С друге стране, савршене шифре захтевају чување велике количине података везане за кључ, те се стога користе у ситуацијама када је количина података која се шифрује мала, а њихова важност т.ј. тајност неприкосновена.

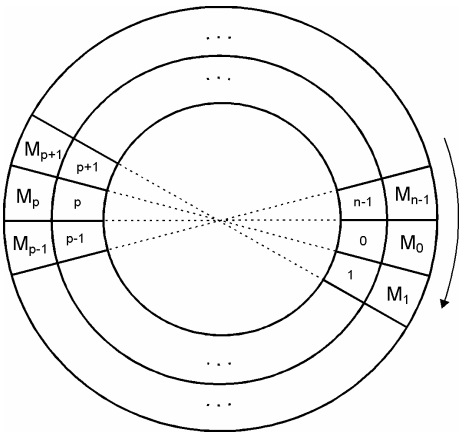
У пракси се углавном користе шифре које нису савршене у теоријском смислу и које поседују одређен степен практичне отпорности према различитим криптонападима.

II. Шифарски алгоритам

Претпостављамо да су азбуке отвореног и шифрованог текста идентичне. Слова азбуке представљамо нумерацијом према природном редоследу у азбуци, тако да за n симбола азбуке A имамо,

$$A = \{0,1,...,n-1\}.$$

Од симбола азбуке A, у природном или неком произвољном редоследу, образујемо кодни прстен $\overline{M}$. Овако организованим симболима доделимо позиције p, од 0 до $n-1$, $p \in \{0,1,...,n-1\}$, тако што се позиција (0) произвољно додели неком симболу, те се у односу на њу, кретањем у изабраном смеру, симболима у кодном прстену додељују растуће позиције.



Сл. 1. Кодни прстен $\overline{M}$

Сликовито представљено (Сл. 1.) , у унутрашњем појасу угаоног сегмента кодног прстена уписујемо позицију p, док се одговарајући садржај позиције M_p (симбол), налази у спољашњем појасу истог угаоног сегмента.

$$\overline{M} = M_0,...,M_{p-1},M_p,M_{p+1},...,M_{n-1},$$
$$M_p \in A = \{0,1,...,n-1\}.$$

У поступку шифровања, симбол шифрованог текста y_i нумерички изражавамо бројем неуспелих серијских компарација у унапред изабраном смеру кретања по кодном прстену, симбола из отвореног текста x_i, са симболима на кодном прстену $\overline{M}$.

Позиција на кодном прстену од које полазимо у поступку шифарског кодовања, односно, поређења симбола којег шифрујемо са симболима на кодном прстену, може узети једну од n вредности из скупа $\{0,1,2,...,n-1\}$,

$$p \in P = \{0,1,...,n-1\}.$$

У поступку дешифровања, на идентичном кодном прстену $\overline{M}$ дешифрујуће стране, декодовање y_i почиње од исте позиције p_i од које је почео и процес шифровања x_i на предаји. Декодовање се остварује одбројавањем онолико позиција у изабраном смеру кретања по прстену колико нумерички износи y_i. Другим речима, x_i је на кодном прстену, удаљен од p_i, мерено бројем позиција у изабраном смеру, за нумеричку вредност симбола y_i.

За отворени текст,

$$X^{(l)} = x_1 x_2 ... x_l,$$

x_i - симбол отвореног текста,

потребно је формирати низ почетних позиција,

$$\overline{p} = p_1, p_2, ..., p_l,$$

p_i - почетна позиција на кодном прстену у поступку шифарског кодовања симбола x_i, где $\overline{p} \in P^l$, P^l је декартов степен скупа P. За $i = \overline{1,l}$, имамо скуп парова $\{(p_i, x_i)\}$, $i = \overline{1,l}$.

Ако је p_i потпуно независно од p_{i-1} и потпуно независно од позиције на којој је окончано шифровање претходног симбола у низу (независно од позиције на којој се у прстену налази x_{i-1}) и ако је при томе подједнако вероватно да свака од n позиција $p \in P$ буде почетна

$$p(p_j) = \frac{1}{n},\ p_j \in P,\ \text{за}\ \forall j \in \{0,1,...,n-1\}, \qquad (1)$$

овај шифарски метод је савршен по К. Шенону, односно шифровањем по овом методу добија се шифровани текст

$$Y^{(l)} = y_1, y_2, ..., y_l,$$

савршено отпоран према криптонападу на основу једног ухваћеног криптограма.

III. Расподела симбола у шифрованом тексту

Расподела симбола у шифрованом тексту $p(y_i = k)$, $k = \overline{0, n-1}$, је

$$\begin{aligned}
p(y_i = 0) &= p(p_i = p_0, x_i = M_0) + \\
&+ p(p_i = p_1, x_i = M_1) + ... \\
&... + p(p_i = p_{n-1}, x_i = M_{n-1}), \\
&... \\
p(y_i = k) &= p(p_i = p_0, x_i = M_k) + \\
&+ p(p_i = p_1, x_i = M_{k+1}) + ... \\
&... + p(p_i = p_{n-1}, x_i = M_{k-1}), \\
&... \\
p(y_i = n-1) &= p(p_i = p_0, x_i = M_{n-1}) + \\
&+ p(p_i = p_1, x_i = M_0) + ... \\
&... + p(p_i = p_{n-1}, x_i = M_{n-2}).
\end{aligned} \qquad (2)$$

Изрази (2) могу се довести на облик,

$$\begin{aligned}
p(y_i = 0) &= p(p_i = p_0) \cdot p\left(x_i = M_0 / p_i = p_0\right) + \\
&+ p(p_i = p_1) \cdot p\left(x_i = M_1 / p_i = p_1\right) + ... \\
&... + p(p_i = p_{n-1}) \cdot p\left(x_i = M_{n-1} / p_i = p_{n-1}\right), \\
&... \\
p(y_i = k) &= p(p_i = p_0) \cdot p\left(x_i = M_k / p_i = p_0\right) + \\
&+ p(p_i = p_1) \cdot p\left(x_i = M_{k+1} / p_i = p_1\right) + ... \\
&... + p(p_i = p_{n-1}) \cdot p\left(x_i = M_{k-1} / p_i = p_{n-1}\right), \\
&... \\
p(y_i = n-1) &= p(p_i = p_0) \cdot p\left(x_i = M_{n-1} / p_i = p_0\right) + \\
&+ p(p_i = p_1) \cdot p\left(x_i = M_0 / p_i = p_1\right) + ... \\
&... + p(p_i = p_{n-1}) \cdot p\left(x_i = M_{n-2} / p_i = p_{n-1}\right),
\end{aligned} \qquad (3)$$

Обзиром да су парови $\{(p_i, x_i)\}$, $i = \overline{1,l}$, састављени од међусобно независних елемената имамо

$$p\left(x_i = M_{j\oplus k} \Big/ p_i = p_j\right) = p\left(x_i = M_{j\oplus k}\right), \quad j,k = \overline{0,n-1} \tag{4}$$

где је $\oplus$ – операција сабирања по $\bmod n$.

Ако применимо постављени услов,

$$p(p_i = p_0) = p(p_i = p_1) = \ldots = p(p_i = p_{n-1}) = \frac{1}{n}, \tag{5}$$

и изразе (4), изрази (3) своде се на

$$\begin{aligned}
p(y_i = 0) &= \frac{1}{n}\cdot\left[\sum_{j=0}^{n-1} p\left(x_i = M_{j\oplus 0} \Big/ p_i = p_j\right)\right] = \\
&= \frac{1}{n}\sum_{j=0}^{n-1} p\left(x_i = M_{j\oplus 0}\right), \\
&\ldots \\
p(y_i = k) &= \frac{1}{n}\cdot\left[\sum_{j=0}^{n-1} p\left(x_i = M_{j\oplus k} \Big/ p_i = p_j\right)\right] = \\
&= \frac{1}{n}\sum_{j=0}^{n-1} p\left(x_i = M_{j\oplus k}\right), \\
&\ldots \\
p(y_i = n-1) &= \frac{1}{n}\cdot\left[\sum_{j=0}^{n-1} p\left(x_i = M_{j\oplus n-1} \Big/ p_i = p_j\right)\right] = \\
&= \frac{1}{n}\sum_{j=0}^{n-1} p\left(x_i = M_{j\oplus (n-1)}\right).
\end{aligned} \tag{6}$$

Како је,

$$\sum_{j=0}^{n-1} p\left(x_i = M_{j\oplus k}\right) = 1, \quad k = \overline{0,n-1}, \tag{7}$$

из (6) следи

$$p(y_i = 0) = \frac{1}{n}, \ldots\ p(y_i = k) = \frac{1}{n}, \ldots\ p(y_i = n-1) = \frac{1}{n} \tag{8}$$

IV. Елементи анализе криптоотпорности шифре

Показали смо математичким извођењем да су симболи у шифрованом тексту y_i једнаковероватни,

$$p(y_i = k) = \frac{1}{n}, \quad k = \overline{0,n-1}. \tag{9}$$

Низ $\overline{p} = p_1 p_2, \ldots, p_l$, $\overline{p} \in P^l$, представља кључевни низ (кључ). Пошто су све почетне позиције независне и једнаковероватне (1), повећањем l за један, број могућих једнаковероватних кључевних низова расте n пута. Увећањем l до бесконачности, број могућих кључева (кључевних низова) расте до бесконачности, (кључ шифре је неограничен), при чему су сви кључеви једнаковероватни. Само шифра са неограниченим кључем може бити савршена по К. Шенону.

Из статистичких особина кључевног низа и правила шифровања произилази да су симболи у шифрованом тексту једнаковероватни (9) и потпуно међусобно статистички независни (декорелисани), без обзира на статистичке особине извора отвореног текста.

Једино што у овом случају критоаналитичар може да уради у поступку декриптовања је да ухваћени криптограм дешифрује применом свих l^n кључевних низова (кључева). За резултат добија свих l^n могућих отворених текстова дужине l, међу којима се налазе и сви смислени отворени текстови те дужине. Обзиром да су сви кључеви једнаковероватни следи да су и сви смислени отворени текстови једнаковероватни. Овим је криптоаналитичарево знање о отвореном тексту после поступка декриптовања исто као и пре тога.

Другим речима, апостериорно знање о отвореном тексту на основу ухваћеног криптограма једнако је априорном знању о отвореном тексту [1]-[3],

$$p\left(\hat{X}^{(l)} = X^{(l)} \Big/ Y^{(l)}\right) = p\left(\hat{X}^{(l)} = X^{(l)}\right). \tag{10}$$

Израз (10) је потребан и довољан услов савршене отпорности шифре према криптонападу на основу једног ухваћеног криптограма, т.ј. савршене отпорности по Клоду Шенону.

Обзиром да су,

$$\left|X^{(l)}\right| = \left|Y^{(l)}\right| = \left|K^{(l)}\right| = n^l,$$

скупови отворених текстова, шифрованих текстова и кључева, респективно, једнакобројни, конструисана шифра је ендоморфна савршена шифра са минималним бројем кључева [3]. Минималност броја кључева важан је фактор практичне реализације савршених шифара.

V. Закључак

Предложени шифарски метод може бити предмет анализе са аспекта отпорности и на друге врсте криптонапада, другим речима, потребно је испитати да ли предложена шифра испуњава и неки други услов савршености шифре, осим доказане савршености по Клоду Шенону.

Литература

[1] Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В., "Основы криптографии", *Учебное пособие,* - Гелиос АРВ, Москва, 2002.

[2] Бабаш А. В., Шанкин Г. П., "Криптография", *Учебное пособие,* -СОЛОН-Р, Москва, 2002.

[3] Зубов А. Ю., "Совершенные шифры", *Учебное пособие,* Гелиос АРВ, Москва, 2003.

Abstract

This paper presents a novel method for generating theoretical perfect cipher resistant to cryptanalytic attacks performed based on one intercepted ciphertext. The constructed cipher is endomorphic with minimal number of keys, which is particularly important from the practical implementation point of view. The probability distribution of the cipher alphabet in ciphertext is determined, and a cipher analysis performed from cryptographic attack point of view, while the cryptosystem theoretical perfect secrecy is proven.

A NEW METHOD FOR GENERATING PERFECT ENDOMORPHIC CIPHER WITH MINIMAL NUMBER OF KEYS

Milos Bandjur, Andjelija Raicevic, Djoko Bandjur, Brankica Popovic