УДК 004.056.2

Олег КРУК, Михайло ГОЛЕМБЙОВСЬКИЙ, Василь БАСІСТИЙ

Західноукраїнський національний університет

МАТЕМАТИЧНА МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ СИМВОЛЬНОГО РОЗЩЕПЛЕННЯ

Вступ. Проблеми захисту інформації віддавна турбували людське суспільство. Потреба у захисті інформації виникла з необхідності таємної передачі військових, дипломатичних та інших повідомлень [1]. Вона зародилась майже одночасно з самою технологією письма. Криптографія стала широко застосовуватися не тільки в державних, дипломатичних, військових сферах, але також в банківських, комерційних та інших додатках [2]. Шифрування − практичний спосіб представлення секретної інформація з метою її захисту від незаконного читання та модифікації.

На сьогоднішній день багато із відомих методів захисту даних грунтуються на операції ділення націло з остачею [3]. Однак у цих методах не розглядалося питання багатократного застосування цієї операції для кожного символу з метою підвищення рівня безпеки і створення додаткових труднощів для контролю повідомлень, що передаються зі сторони несанкціонованого користувача. Тому вивчення альтернативи у вигляді процедури розщеплення слід визнати дуже актуальною задачею.

Мета: розробити математичну модель захисту інформації на основі символьного розщеплення.

1. Математична модель захисту інформації на основі символьного розщеплення

Розщеплення при потоковій передачі означає заміну кожного символу в послідовності на ланцюжок чисел. Розщеплення забезпечує глибокий захист інформації, що передається від дій різного роду зловмисників.

Розщеплення передбачає, що кожному вихідному символу відповідає k чисел, де k - рівень розщеплення. Більш того, одержуваний захищений текст досить важкий для розкриття, оскільки в гамі захисту база r є змінною і той самий символ буде представлений при розщепленні щоразу різними поєднаннями. Ця властивість у галузі захисту інформації є новою.

Якщо одержувачу відомий ключ захисту, то розщеплення довільного символу S є ін'єктивним і оборотним, що відкриває можливість однозначного відновлення цього символу на приймальному кінці.

Нехай база r перевищує максимальне значення кодів у вибраній кодовій таблиці символів. Тоді розщепленням рівня k для символу S з кодом a відповідно до зазначеної кодової таблиці і r називається представлення S у вигляді ряду відповідних цілих чисел $\delta^{(2)}, \delta^{(3)}, \delta^{(4)}, \ldots, \delta^{(k-1)}, \delta^{(k)}, q^{(k)}$. Тут числа $\delta^{(i)}$ обчислюються за такою формулою:

$$\delta^{(i)}=r \bmod q^{(i-1)}, \text{ де } q^{(i-1)}=\left\lfloor \frac{r}{q^{(i-2)}} \right\rfloor, i=2, 3, \ldots, k. \quad (1)$$

Назвемо отриманий таким чином ряд цілих чисел $\delta^{(2)}, \delta^{(3)}, \delta^{(4)}, \ldots, \delta^{(k-1)}, \delta^{(k)}$,

$q^{(k)}$ результатом розщеплення.

Захист тексту та його відновлення відбуваються за допомогою ГПВЧ, який вважається відомим і на приймальному, і на передаючому кінці. Зазвичай мається на увазі, що ГПВЧ створює непередбачувану послідовність псевдовипадкових чисел для зовнішнього спостерігача.

Від ГПВЧ надходить величина r_i, необхідна як під час передачі з використанням розщеплення, так і при відновленні кожного символу. В результаті розщеплення в момент t створюються цілі числа $\delta^{(2)}$, $\delta^{(3)}$, $\delta^{(4)}$, …, $\delta^{(k-1)}$, $\delta^{(k)}$, $q^{(k)}$. Передбачається, що величина $r_i>0$ перевершує максимальне значення символів за обраною кодовою таблицею.

У нашій моделі потім надходять випадкові величини r_{i+1}, r_{i+2}, r_{i+3}, …, r_{i+k}, які використовуються для додаткового захисту кожного компонента розщеплення цього символу шляхом гамування.

Тоді модель кроку захисту символу $S(t)$ з кодом $a(t)$ приводить до такого результату:

$$Y=\begin{cases} r_i \oplus a, \ \text{при} \ \ k=1; \\ \delta^{(2)},\delta^{(3)},\delta^{(4)},...,\delta^{(k-1)},\delta^{(k)},q^{(k)}, \ \text{при} \ \ k>1. \end{cases} \tag{2}$$

При гамуванні отримується такий результат захисту:

$$\begin{cases} \delta^{(j)} \oplus r_{i+j-1}, \ \ \text{де} \ \ j=2,3,...,k; \ \ \text{при}\, k>1; \\ q^{(k)} \oplus r_{i+k}. \end{cases} \tag{3}$$

Модель кроку відновлення символу після гамування дає такий результат:

$$\begin{cases} \delta^{(j)} \oplus r_{i+j-1}, \ \ \text{де} \ \ j=2,3,...,k; \ \ \text{при}\, k>1; \\ q^{(k)} \oplus r_{i+k}. \end{cases} \tag{4}$$

Тоді результат відновлення розщепленого символу:

$$\begin{cases} r_i \oplus Y, \ \ \text{при} \ \ k=1; \\ \dfrac{\left(r_i-\delta^{(j)}\right)}{q^{(j)}}, \ \ \text{де} \ \ j=k,k-1,...,3,2; \ \ \text{при}\, k>1. \end{cases} \tag{5}$$

Звідси процедура узагальненого розщеплення, при якій на кожному кроці формування величин використовується нова величина $r_i>q^{(i)}$, матиме такий вигляд:

$$\begin{cases} \delta^{(2)},\delta^{(3)},\delta^{(4)},...,\delta^{(k-1)},\delta^{(k)},q^{(k)}, \ \text{де} \\ \delta^{(2)}=r_1 \bmod a, \ q^{(2)}=\left\lfloor \dfrac{r_1}{a} \right\rfloor; \\ \delta^{(3)}=r_2 \bmod q^{(2)}, \ q^{(3)}=\left\lfloor \dfrac{r_2}{q^{(2)}} \right\rfloor; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \delta^{(k)}=r_{k-1} \bmod q^{(k-1)}, \ q^{(k-1)}=\left\lfloor \dfrac{r_{k-2}}{q^{(k-2)}} \right\rfloor; \\ q^{(k)}=\left\lfloor \dfrac{r_{k-1}}{q^{(k-1)}} \right\rfloor. \end{cases} \tag{6}$$

Правило відновлення вихідного символу під час використання методу узагальненого розщеплення та відомому векторі значень $\vec{r}$ полягає в послідовному відновлення величин, що входять до (6), у зворотному порядку в порівнянні з їх надходженням на приймальний вузол. Результат відновлення узагальненого розщепленого символу матиме такий вигляд:

$$\begin{cases} \dfrac{\left(r_i - \delta^{(j)}\right)}{q^{(j)}}, \quad \text{де} \quad j = k, k-1, \ldots, 3, 2; \quad \text{при } k > 1; \\ \qquad\qquad i = k-1, k-2, \ldots, 2, 1 \quad \text{при } k > 1. \end{cases} \tag{7}$$

2. Схеми методу захисту інформації на основі символьного розщеплення

Узагальнена схема симетричного методу захисту на основі символьного розщеплення показано рисунку 1.

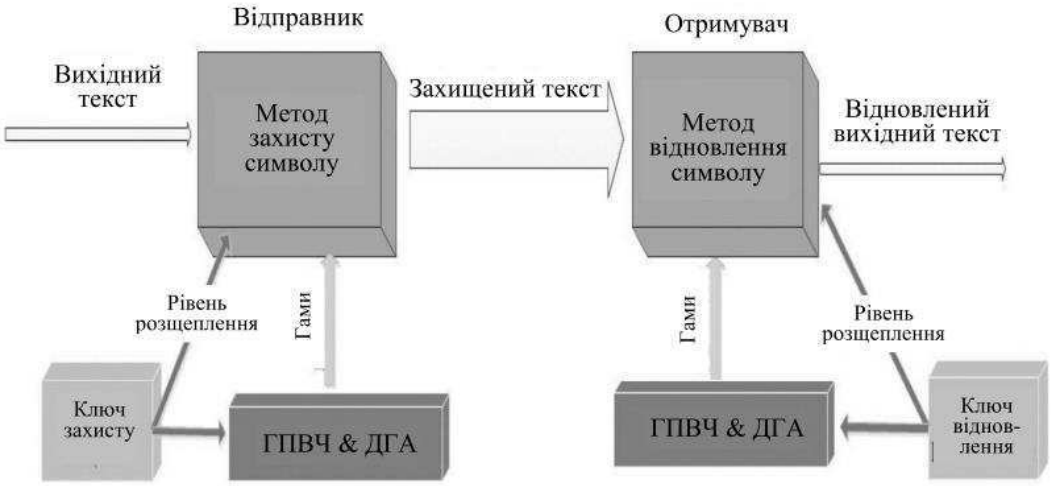

Рисунок 1 - Узагальнена схема методу захисту на основі символьного розщеплення

На рисунках 2 і 3 показано блок-схему методу розщеплення при k=1 та k≥2.

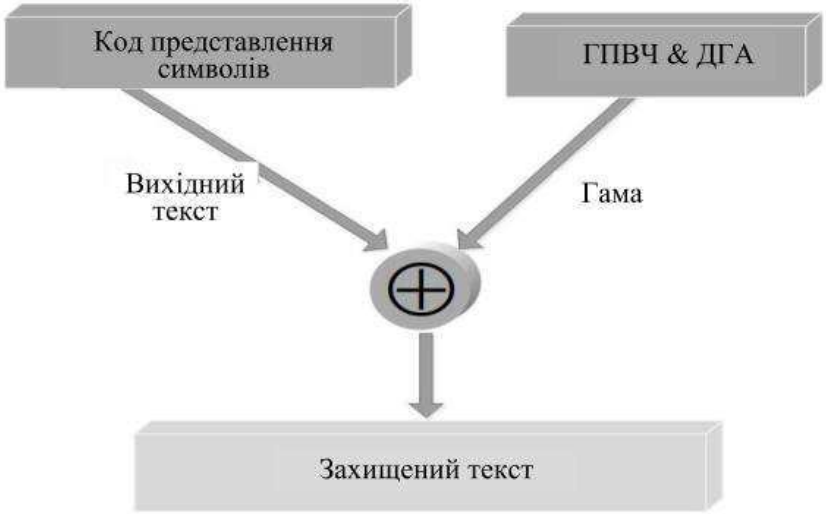

Рисунок 2 - Блок-схема методу розщеплення при k=1

В симетричних алгоритмах захисту із символьним розщепленням для захисту та відновлення повідомлення використовується один і той самий блок інформації (тобто ключ).

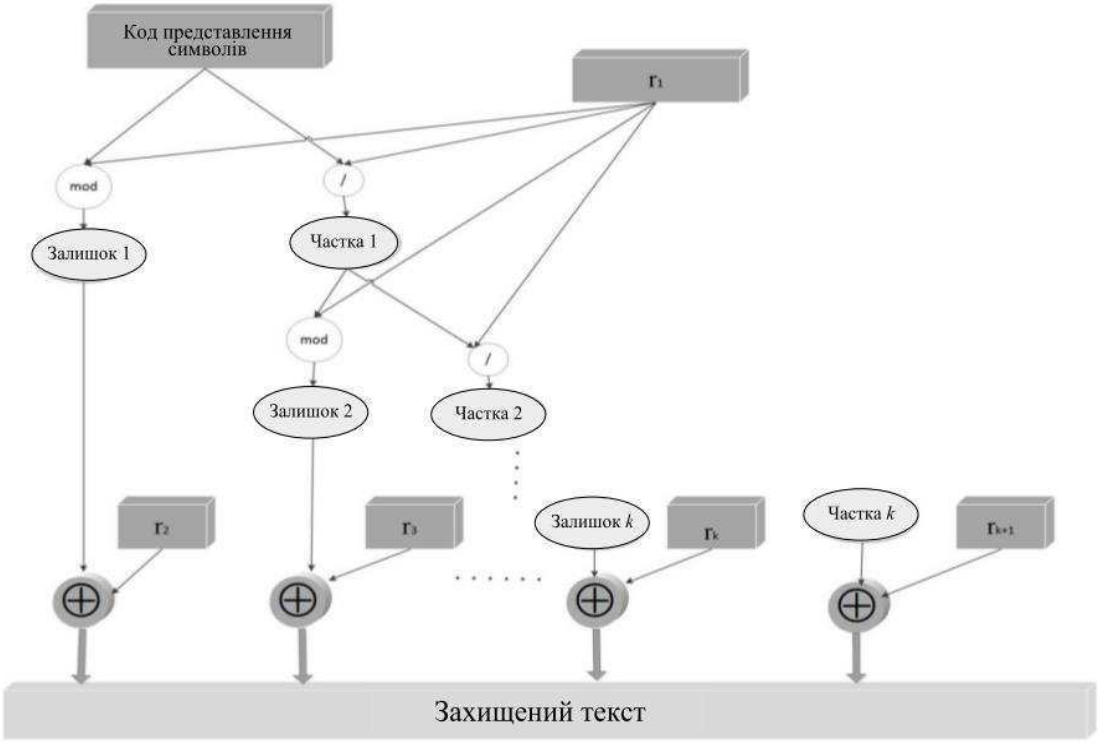

Рисунок 3 - Блок-схема методу розщеплення при k рівнях, $k \geq 2$

Ключ захисту містить інформацію про детермінований генетичний алгоритм, параметри ГПВЧ та рівні розщеплення. Параметри детермінованого генетичного алгоритму та ГПВЧ використовуються на етапі створення бази r у запропонованій процедурі розщеплення.

Метод розщеплення забезпечує більш надійний захист від криптоаналітичних атак, заснованих на підрахунку частот появи літер в захищеному тексті. Цей метод також слабо залежить також від розподілу ймовірностей літер у природній мові.

Висновок. Розроблено математичну модель захисту інформації на основі символьного розщеплення.

Перелік використаних джерел.

1. Rubin F. Secret Key Cryptography: Ciphers, from Simple to Unbreakable. Manning, 2022. 344c.

2. Samuel S., Wagstaff Jr. Cryptanalysis of Number Theoretic Ciphers. RC Press, 2019. 336c.

3. Kasianchuk M.M., Yakymenko I.Z., Nykolaychuk Y.M. Symmetric Cryptoalgorithms in the Residue Number System. Cybernetics and Systems Analysis. 2021. Vol. 57, №2. P. 329-336