УДК 004.056

ШИФР ЗАМІНИ НА ОСНОВІ ПСЕВДОНЕДЕТЕРМІНОВАНОГО ГЕНЕРАТОРА ГАМИ

І. С. Горбенко, аспірант
Вінницький національний технічний університет

К. Шеннон довів, що будь-який шифр є комбінацією операцій заміни та перестановки. В комп'ютерній криптографії шифр заміни може будуватись на основі таблиці заміни (недоліком є те, що однакові символи відкритого повідомлення замінюються на однакові символи шифротексту), а також на основі накладання гами.

Для формування гами використовується, як правило, генератор псевдовипадкових послідовностей (ПВП) на основі регістра зсуву зі зворотним зв'язком (РЗЗЗ). Однак цей генератор не забезпечує високої стійкості, оскільки, знаючи частину гами, зловмисник має можливість відновити всю гаму. Для підвищення стійкості використовують комбінацію декількох генераторів, однак це призводить до збільшення витрат ресурсів.

Блокові шифри в режимах CFB та OFB формують гаму на основі секретного ключа та повідомлення, але такий підхід передбачає виконання складних операцій, наслідком чого є низька швидкість шифрування.

Пропонується метод формування гами, який враховує секретний ключ та відкрите повідомлення та забезпечує високу швидкість шифрування.

Відкрите повідомлення M розбивається на n блоків розрядності 2^d, де d – ціле додатне число:

$$M = \{m_0, m_1, ..., m_{n-1}\}.$$

Гама та шифротекст також складаються з n блоків такої самої розрядності, як блоки відкритого повідомлення:

$$G = \{g_0, g_1, ..., g_{n-1}\}$$

$$C = \{c_0, c_1, ..., c_{n-1}\}$$

Операція зашифрування полягає у додаванні блока гами до блоку відкритого повідомлення за модулем 2:

$$c_i = m_i \oplus g_i, \qquad i = 0,1,...,n-1.$$

Для розшифрування потрібно здійснити аналогічну дію – до шифротексту додати ту саму гаму за модулем 2:

$$m_i = c_i \oplus g_i, \qquad i = 0,1,...,n-1.$$

Найпростіший варіант формування гами полягає в такому. Нехай секретний ключ K складається з q байтів:

$$K = \{k_0, k_1, ..., k_{q-1}\}.$$

Тоді байти гами від 0-го до (q-1)-го включно формуватимуться з ключа, а усі наступні – з попередніх блоків відкритого повідомлення:

$$g_i = \begin{cases} k_i, & \text{якщо } i < q \\ m_{i-q}, & \text{якщо } q \le i < n \end{cases}$$

Згідно К. Шеннона, абсолютно стійкий шифр – це шифр, в якому знання шифротексту не дозволяє покращити оцінку відповідного відкритого тексту. Для реалізації такого шифру необхідно, щоб кожен символ відкритого тексту впливав на кожен символ шифрованого тексту. Для описаного вище підходу ця вимога не виконується, оскільки кожен розряд відкритого повідомлення впливає лише на 1 байт шифротексту. Крім того, описаний підхід передбачає детермінований порядок вибору елементів відкритого повідомлення та ключа.

Інший підхід до формування гами передбачає використання псевдовипадкового порядку вибору байту для формування гами: з ключа або з відкритого повідомлення – залежно від певної ознаки r. В якості такої

ознаки може бути, наприклад, значення чергового розряду (біту) ключа:.

$$g_i = \begin{cases} k_j, & \text{для} \quad r = 0 \\ m_j, & \text{для} \quad r = 1 \end{cases}.$$

Перевагою є псевдонедетермінований порядок вибору елементів імовірність успішної атаки на генератор гами. Але підхід має інший недолік: для формування байту гами або не використовується відкрите повідомлення, або ключ використовується лише для формування ознаки.

Пропонується підхід до формування гами, який передбачає одночасне використання секретного ключа та відкритого повідомлення, тобто гама є функцією:

$$G = f(K, M).$$

Формування байту гами здійснюється за формулою:

$$g_i = a_0 b_{i-1} * a_1 b_{i-2} * ... * a_{n-1} b_{i-n},$$

де * – деяка бінарна операція. У формуванні гами беруть участь коефіцієнти a_j:

$$a_j = \{0,1\}; \qquad j = 0,1,..., q-1,$$

а також код для формування гами B:

$$B = \{b_0, b_1, ..., b_{q-1}\}.$$

На початку секретний ключ задається в якості початкового стану s_0 генератора ПВП на основі РЗЗЗ:

$$s_0 = K,$$

На основі стану генератора s_i формуються вектор вибору байтів коду формування гами w_b та вектор вибору операцій w_o.

Вектор вибору байтів має розрядність q та складається з коефіцієнтів a_j, кожен з яких приймає значення 0 або 1:

$$w_b = \{a_j\}; \qquad a_j = \{0,1\}; \qquad j = 0,1,..., q-1.$$

Значення 1 свідчить про те, що відповідний байт коду B бере участь у формуванні гами, а значення 0 – що

відповідний байт не використовується.

Вектор вибору операцій вказує, яка бінарна операція * здійснюється для формування байту гами:

- значення 0 відповідає операції додавання за модулем 2;
- значення 1 відповідає операції додавання за модулем 2^d.

Після того, як черговий байт повідомлення було зашифровано, генератор ПВП формує новий стан s_i, а також відбувається зсув коду B з відкиданням старшого байту та доповненням попереднім байтом повідомлення:

$$B = \{k_1, k_2, ..., k_{q-1}, m_0\};$$
$$B = \{k_2, k_3, ..., k_{q-1}, m_0, m_1\};$$
$$\dots$$
$$B = \{m_{i-q}, m_{i-q+1}, ..., m_{i-1}\};$$
$$\dots$$
$$B = \{m_{n-q}, m_{n-q+1}, ..., m_{n-1}\}.$$

Розроблений метод забезпечує вищу стійкість шифрування, ніж звичайні шифри на основі накладання гами, оскільки генератор гами задовольняє статистичним тестам NIST, а кожен розряд відкритого повідомлення впливає в середньому на $4n$ розрядів шифротексту.

Розроблений метод забезпечує підвищення швидкості шифрування, порівняно з блоковими шифрами, оскільки передбачає виконання лише 2 операцій на 1 біт, тоді як сучасні блокові шифри (AES, Serpent та ГОСТ 28147-89) в режимах з гамуванням виконують 3,7 ÷ 5 операцій на 1 біт.