© Luzhetskiy V. Gorbenko I. Substitution cipher based on pseudo non-determined gamma generator // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 159-163.

ШИФР ЗАМІНИ НА ОСНОВІ ПСЕВДОНЕДЕТЕРМІНОВАНОГО ГЕНЕРАТОРА ГАМИ

Володимир Лужецький, Іван Горбенко

Вінницький національний технічний університет, Україна

ЛУЖЕЦЬКИЙ Володимир Андрійович, д.т.н.

Рік та місце народження: 1950 рік, м. Ставрополь, Росія.
Освіта: Таганрозький радіотехнічний інститут, 1972 рік.
Посада: завідувач кафедри захисту інформації з 2002 року.
Наукові інтереси: кодування та ущільнення даних, криптографія.
Публікації: понад 180 наукових публікацій, серед яких монографії, навчальні посібники, наукові статті та патенти на винаходи.
E-mail: lva_zi@mail.ru

ГОРБЕНКО Іван Сергійович

Рік та місце народження: 1989 рік, м. Вінниця, Україна.
Освіта: Вінницький національний технічний університет, 2011 рік.
Посада: аспірант кафедри захисту інформації.
Наукові інтереси: криптографія.
Публікації: 1 наукова стаття, 3 матеріали тез доповіді
E-mail: milyaga89@gmail.com

Анотація. *Шифр заміни здійснює перетворення шляхом заміни символів або інших частин відкритого тексту на аналогічні частини шифрованого тексту. Шифри з використанням гамування мають високу криптографічну стійкість, однак суттєвим недоліком є висока складність виконуваних операцій та, як наслідок, значно нижча швидкість шифрування, порівняно з шифрами на основі накладання гами. У даній статті запропоновано метод шифрування інформації з використанням генератора гами, який враховує секретний ключ та відкрите повідомлення. Отримані результати дозволяють підвищити швидкість шифрування, порівняно з блоковими шифрами в режимах зворотного зв'язку за шифротекстом та за виходом, забезпечуючи при цьому стійкість шифрування, порівнянну зі стійкістю блокових шифрів.*

Ключові слова: *генератор гами, секретний ключ, відкрите повідомлення, шифротекст, криптографічна стійкість, швидкість шифрування.*

Вступ

Одним із основних методів криптографічного захисту інформації є шифрування, тобто оборотне перетворення інформації з метою приховування її від неавторизованих осіб, але з наданням авторизованим особам доступу до неї [1].

К. Шеннон довів, що будь-який шифр можна представити у вигляді комбінації двох основних операцій – заміни та перестановки [2]. Шифр заміни та шифр перестановки є найпростішими (та найдавнішими) видами шифрів.

Класичний шифр заміни – це шифр, в якому кожен символ відкритого повідомлення заміняється деяким, фіксованим за даного ключа, символом того ж алфавіту [1]. Такий шифр здійснює перетворення шляхом заміни символів або інших частин відкритого тексту на аналогічні частини шифрованого тексту.

В комп'ютерній криптографії одним з варіантів побудови шифру заміни є використання таблиці заміни [3]. Недоліком такого способу є те, що однакові символи відкритого тексту замінюються на однакові символи шифротексту. Таким чином, шифр є вразливим до статистичного аналізу, а також до атаки нав'язування зловмисником відкритого тексту. Іншим варіантом є виконання заміни шляхом накладання на відкрите повідомлення гами – деякої псевдовипадкової послідовності, яка формується на основі секретного ключа [3]. Накладання гами може бути реалізоване як будь-яка арифметична операція.

Шифр на основі гамування, на відміну від шифру на основі таблиці заміни, є стійким до статистичного аналізу. Однак такий шифр є вразливим до атак на генератор гами, зокрема до атаки нав'язування зловмисником відкритих повідомлень.

Як правило, для формування гами використовується генератор псевдовипадкових послідовностей (ПВП) на основі регістра зсуву зі

зворотним зв'язком (РЗЗЗ), оскільки цей генератор є простим у реалізації та має високу швидкодію, що важливо при шифруванні в режимі реального часу (у потоковому шифруванні). Але такий генератор не є стійким: знаючи частину відкритого повідомлення та шифротекст, зловмисник може відновити частину гами, а знаючи її – сформувати всю гаму [4]. Для усунення цього недоліку в сучасних потокових шифрах використовуються поєднання декількох генераторів на основі РЗЗЗ. Це забезпечує підвищення криптографічної стійкості, однак вимагає додаткових апаратних витрат.

Блокові шифри в режимах шифрування зі зворотним зв'язком за шифротекстом (Ciphertext Feedback, CFB) та зі зворотним зв'язком за виходом (Output Feedback, OFB) здійснюють формування гами на основі секретного ключа та повідомлення [5]. В режимі CFB зашифрований попередній блок використовується для зашифрування наступного блоку. В режимі OFB для аналогічної мети використовується частково перетворений попередній блок [5]. Ці режими шифрування забезпечують високу криптографічну стійкість, однак суттєвим недоліком таких підходів до формування гами є висока складність виконуваних операцій та, як наслідок, значно нижча швидкість шифрування, порівняно з шифрами на основі накладання гами. Так, зазначені підходи передбачають виконання 3,5 ч 5 операцій на 1 біт [6-8].

Метою дослідження є підвищення швидкості шифрування з використанням генератора гами, що враховує секретний ключ та повідомлення.

Постановка задач дослідження

Для досягнення мети дослідження потрібно розв'язати такі задачі:

1) Розробити метод шифрування з використанням генератора гами, що враховує секретний ключ та відкрите повідомлення.

2) Отримати для розробленого методу оцінки криптографічної стійкості та швидкості шифрування та порівняти їх з відповідними оцінками відомих методів шифрування.

Розробка методу шифрування

Шифру на основі гамування відповідає така математична модель:

$$Cf = \{\mathbf{M}, \mathbf{C}, \mathbf{K}, \mathbf{G}\},$$

де **M** – множина відкритих повідомлень; **C** – множина шифротекстів; **K** – множина секретних ключів; **G** – множина псевдовипадкових послідовностей (гами), що формується на основі секретного ключа.

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:

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

Пропонується метод шифрування на основі накладання гами, в якому для формування гами використовується секретний ключ та відкрите повідомлення, тобто гама формується на основі функції:

$$g_i = f(k_0, ...k_{q-1}, m_0, ..., m_{i-q}).$$

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:

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

Тобто для перших q байтів гама є виключно функцією ключа, а для всіх наступних байтів – лише функцією відкритого повідомлення. Для формування гами можуть використовуватись лише попередні байти відкритого повідомлення, оскільки при розшифруванні поточного байту, вони вже відомі.

Згідно К. Шеннона [2], абсолютно стійкий шифр – це шифр, в якому знання шифротексту не дозволяє покращити оцінку відповідного відкритого тексту. Для абсолютно стійкого шифру дешифрування (злам) еквівалентне за успіхом простому вгадуванню відкритого тексту за відсутності будь-яких додаткових даних. Для реалізації такого шифру необхідно, щоб кожен символ (розряд) відкритого тексту впливав на кожен символ шифрованого тексту, тобто зміна лише одного (будь-якого) символу відкритого тексту повинна призводити до повної зміни шифротексту.

В шифрі заміни, побудованому з використанням генератора гами, який враховує лише секретний ключ, зміна одного розряду відкритого тексту призводить до зміни лише одного – відповідного йому розряду шифротексту, тобто кожен символ відкритого тексту впливає лише на один символ шифротексту. Це пов'язано з тим, що описані підходи до побудови шифрів заміни передбачають формування гами лише на основі одного значення, невідомого для зловмисника – секретного ключа. Відкрите повідомлення не бере участі у формуванні гами.

В шифрі, побудованому на основі описаного вище підходу, кожен розряд байту відкритого повідомлення впливає лише на кожен розряд відповідного байту шифротексту, а також на кожен розряд байту шифротексту, для шифрування якого даний байт відкритого повідомлення є гамою.

Основний недолік такого підходу полягає у

тому, що метод шифрування на основі цього підходу є нестійким у випадку, якщо зловмиснику відома частина відкритого повідомлення. Для усунення цього недоліку необхідно поєднувати такий шифр заміни із перестановкою байтів відкритого повідомлення, для чого може бути використаний метод формування перестановок, описаний в [9]. Іншим недоліком описаного методу є його детермінованість: порядок вибору байтів ключа та відкритого повідомлення є фіксованим.

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: значення "0" відповідає вибору байту з ключа, значення "1" – вибору з відкритого повідомлення.

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

Номер байту *j*, який вибирається, може визначатись певною послідовністю розрядів ключа або за допомогою деякого генератора псевдовипадкових чисел (ПВЧ).

Перевагою такого підходу є псевдо-недетермінований порядок вибору елементів ключа або відкритого повідомлення для формування гами, що знижує імовірність успішної атаки на генератор гами, побудований на основі цього підходу. Однак підхід має інший недолік: для формування байту гами або не використовується відкрите повідомлення, або ключ використовується лише для формування ознаки (залежно від того, з ключа чи з повідомлення здійснюється вибір).

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:

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

де * – деяка бінарна операція.

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

а також код для формування гами *B*.

Секретний ключ має дві складових. Одна складова використовується в якості початкового стану генератора ПВП на основі РЗЗЗ:

$$s_0 = K,$$

а друга складова – у якості коду для формування гами B:

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

Тобто при формуванні 0-го байту гами g_0 використовується лише складова ключа (оскільки використання відкритого повідомлення унеможливить розшифрування). Тому для початкової ітерації гама є лише функцією ключа:

$$G = f(K).$$

Формування байту гами здійснюється таким чином. На основі стану генератора s_i формуються вектор вибору байтів коду формування гами w_b та вектор вибору операцій w_o. Для формування обох векторів певним чином визначається ознака, наприклад: значення старшого розряду байту; значення молодшого розряду байту; кількість одиничних розрядів у байті (парна кількість відповідає значенню 0, непарна – значенню 1).

Перевагою останнього варіанту є врахування усіх розрядів, але недоліком є необхідність виконання додаткових операцій для обчислення кількості одиничних розрядів.

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

$$w_b = \{a_j\}.$$

Якщо a_j = 1, то відповідний байт коду *B* бере участь у формуванні гами, а якщо a_j = 0, то 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. Тобто, при шифруванні 1-го байту повідомлення код B має вигляд:

$$B = \{k_1, k_2, ..., k_{q-1}, m_0\},$$

при шифруванні 2 байту:

$$B = \{k_2, k_3, ..., k_{q-1}, m_0, m_1\},$$

а починаючи з *q*-го байту ($i \geq q$) код B складається виключно з байтів відкритого повідомлення:

$$B = \{m_{i-q}, m_{i-q+1}, ..., m_{i-1}\}.$$

Таким чином, починаючи з 1-го байту у формуванні гами одночасно беруть участь секретний ключ та відкрите повідомлення. Шифр з використанням такого підходу до формування гами залишається стійким у випадку, коли зловмиснику відома частина відкритого повідомлення.

Оцінка стійкості та швидкості розробленого шифру

Розглянемо запропонований метод шифрування з точки зору вимоги стійкості. Метод не забезпечує ідеальної ситуації, коли кожен розряд відкритого повідомлення впливає на кожен розряд шифротексту, однак усувається недолік, що один розряд відкритого повідомлення впливає лише на один розряд шифротексту. В запропонованому підході кожен розряд окремого байту відкритого повідомлення впливає на кожен розряд відповідного байту шифротексту та усіх наступних байтів. Таким чином, кожен розряд 0-го байту відкритого повідомлення впливає на кожен розряд усіх байтів шифротексту, кожен розряд 1-го байту відкритого повідомлення впливає на кожен розряд усіх байтів шифротексту, окрім 0-го і т.д. Кожен розряд останнього байту відкритого повідомлення впливає лише на кожен розряд останнього байту

шифротексту. Отже, кожен з n розрядів відкритого повідомлення впливає, в середньому, на $\frac{n}{2}$ байтів або 4*n* розрядів шифротексту. Для відновлення *i*-го блоку повідомлення, зловмиснику потрібно знати *i* – 1 попередніх блоків.

Для розробленого шифру Статистичний аналіз шифротексту як двійкової послідовності з використанням статистичних тестів NIST (частотний побітовий аналіз, частотний блоковий тест, тест на послідовність однакових бітів, тест на періодичність) показує, що така послідовність відповідає критеріям випадковості. Крім того, стійкість розробленого шифру є порівнянною із стійкістю блокових шифрів в режимах CFB та OFB, оскільки вхід та вихід функції шифрування не відповідають безпосередньо відкритому повідомленню та шифротексту відповідно, але враховують попередні блоки відкритого повідомлення та секретного ключа [10].

Оцінка швидкості шифрування визначається на основі кількості виконуваних операцій на 1 біт Отже, підхід передбачає: формування нового стану генератора ПВП; зсув коду формування гами; формування вектору w_b; формування вектору w_o; формування байту гами – виконання операцій, визначених вектором w_o; власне шифрування – додавання байту гами до байту повідомлення.

Дії 1 та 2 виконуються за 1 машинний такт кожна, тобто як 1 операція. У випадку, якщо ознакою для формування векторів w_b та w_o є значення старших або молодших розрядів, дії 3 та 4 передбачають накладання маски (операція логічного "І", яка також виконується за 1 такт).

Дія 5 передбачає виконання q – 1 бінарних операцій. Дія 6 виконується за 1 такт (операція додавання за модулем 2). Таким чином, загальна кількість операцій однієї ітерації для 64-розрядного ключа (q = 8) складає:

$$N = 1+1+8+1+\frac{8}{2}+1 = 16 .$$

Оскільки шифрування здійснюється на рівні байтів, то кількість операцій на 1 біт складає:

$$N_1 = \frac{16}{8} = 2 ,$$

відповідно, що значно менше, порівняно зі значеннями для підходів, використаних у блокових шифрах. Для порівняння, шифр AES в зазначених режимах шифрування здійснює 3,7 ч 4 операції на 1 біт (залежно від розрядності ключа) [6], шифр ГОСТ 28147-89 в режимах гамування та гамування зі зворотним зв'язком – 5 операцій [7], а шифр Serpent – 4,1 операції [8].

Висновки

Запропонований метод шифрування забезпечує досягнення мети дослідження. Він забезпечує вищу криптографічну стійкість, порівняно зі звичайними шифрами на основі накладання гами, оскільки для формування гами використовується не лише секретний ключ, але й повідомлення (як і в окремих режимах блокового шифрування). Тому кожен розряд відкритого повідомлення впливає не лише на відповідний йому розряд шифротексту, але й на інші розряди інших блоків шифротексту.

Крім того, метод забезпечує вищу швидкість шифрування, порівняно з блоковими шифрами в режимах, які передбачають накладання гами (CFB та OFB), оскільки передбачає виконання значно меншої кількості операцій на 1 біт (лише 2 операції, на відміну від 3,7 ч 4 для сучасних блокових шифрів).

Література

[1] Нечаев В.И. Элементы криптографии. Основы теории защиты информации. — М.: Высшая школа, 1999.

[2] Шеннон К. Работы по теории информации и кибернетике. — М.: Изд. иностр. лит., 1963. — 830 с.

[3] Шнайер Б. Подстановочные шифры // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си — М.: Триумф, 2002. — 816 с.

[4] Kelsey J., Schneier B., Wagner D. and Hall C. Cryptanalytic Attacks on Pseudorandom Number Generators — Fast Software Encryption, Fifth International Workshop Proceedings (March 1998), Springer-Verlag, 1998, pp. 168-188.

[5] NIST Computer Security Division's (CSD) Security Technology Group (STG) (2013). Block cipher modes. Cryptographic Toolkit. NIST. Retrieved April 12, 2013.

[6] Баричев С. Г., Гончаров В. В. Стандарт AES. Алгоритм Rijndael. — М.: Горячая линия — Телеком, 2002 — с. 30-35.

[7] Винокуров А. Описание алгоритма шифрования ГОСТ 28147-89. — М. : Монитор, 1995 — 25 с.

[8] Винокуров А. Serpent. Основные параметры – М. : Монитор, 1999 – 21 с.

[9] Лужецький В.А. Метод формування перестановок довільної кількості елементів / В.А. Лужецький, І.С. Горбенко // Захист інформації. — 2013. — №3 — С.262-267.

[10] Головашич С. Анализ безопасности режимов блочного симметричного шифрования / С. Головашич, О. Лебедев // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — Вип. 2. — 2001.

УДК 003.26:004.056.5 (045)

Лужецкий В.А. Горбенко И.С. Шифр замены на основе псевдонедетерминированного генератора гаммы

Аннотация. *Шифр замены осуществляет преобразование путем замены символов или других частей открытого текста на аналогичные части шифрованного текста. Шифры с использованием гаммирования имеют высокую криптографическую стойкость, однако существенным недостатком является высокая сложность выполняемых операций и, как следствие, значительно ниже скорость шифрования по сравнению с шифрами на основе наложения гаммы. В статье предложен метод шифрования информации с использованием генератора гаммы, который учитывает секретный ключ и*

открытое сообщение. Полученные результаты позволяют повысить скорость шифрования, по сравнению с блоковыми шифрами в режимах обратной связи по шифротексту и обратной связи по выходу, обеспечивая при этом криптографическую стойкость, сравнимую со стойкостью блоковых шифров.
Ключевые слова: *генератор гаммы, секретный ключ, открытое сообщение, шифротекст, криптографическая стойкость, скорость шифрования.*

Luzhetskiy V., Gorbenko I. Substitution cipher based on pseudo non-determined gamma generator
Abstract. *Substitution ciphers replace symbols or other parts of the plaintext to ciphertext similar parts. Ciphers using cryptographic gamma have high security level, but a significant disadvantage is the high complexity of the operations and, consequently, much lower speed encryption versus ciphers based overlay gamma. This paper is dedicated to developed information ciphering method using gamma generator which considers the secret key and the open message. The obtained results allow increasing the ciphering speed compared with the block ciphers in ciphertext feedback and output feedback modes, meanwhile providing the cryptographic persistence which is comparable with the block ciphers persistence*
Key words: *gamma generator, secret key, open message, ciphertext, cryptographic security, ciphering speed.*

Отримано *09 квітня 2014 року*, затверджено редколегією *29 квітня 2014 року*