УДК 004.056.55

Лужецький В. А.
Дехтяренко М. С.

МЕТОД ПОТОКОВОГО ШИФРУВАННЯ

Вінницький національно технічний університет

Анотація

Запропоновано метод потокового шифрування на основі перестановок байтів повідомлення та їх замін, що базується на використані генератора псевдовипадкових чисел. Такий генератор реалізується з використанням двох лічильників імпульсів і регістрів зсуву з лінійним зворотним зв'язком.

Ключові слова: Криптографія, потокові шифри, конфіденційність інформації, генератори псевдовипадкових чисел, псевдовипадкові послідовності.

Abstract

The stream ciphering method, which uses message bytes permutations and their further substitution performed on the basis of pseudorandom numbers is proposed. Such generator is implemented using two counters of clock impulses and the linear feedback shift register.

Keywords: Cryptography, stream ciphers, confidentiality, pseudo-random number generators, pseudorandom sequence.

Вступ

Розвиток сучасних ґаджетів, які дозволяють в режимі реального часу здійснювати покупки онлайн, сплачувати платежі, керувати банківськими рахунками, керувати пристроями підключеними до інтернету (наприклад розумний будинок), висуває вимогу забезпечення захисту інформації, що передається [1, 2].

Саме тому актуальною є розробка методів потокового шифрування, які забезпечують швидку обробку великих потоків інформації та простоту програмної й апаратної реалізації в різноманітних пристроях з обмеженими обчислювальними можливостями.

Метою роботи є розроблення методу потокового шифрування на основі перестановки байтів відкритих даних.

Опис методу шифрування

Метод потокового шифрування, що пропонується передбачає шифрування даних, що представлені у вигляді масиву

$$\mathbf{M} = \{m_0, m_1, m_2, \dots, m_{n-1}\},$$

і видачу результатів у вигляді потоку даних, представлених байтами.

При цьому реалізуються перестановки елементів масиву і накладання гами. Особливість перестановок полягає в тому, що вони реалізуються в потоковому режимі. Тобто з масиву даних зчитуються байти з певними номерами і після накладання передаються, як результат шифрування.

Для формування номерів байтів використовується генератор псевдовипадкових чисел (ГПВЧ). Ідея побудови цього генератора полягає у такому. Набір чисел від 0 до n – 1, що відповідають номерам байтів масиву **M**, розбивають на дві частини. Одна частина це числа від 0 до $\frac{n}{2} - 1$, друга частина від $\frac{n}{2}$ до n - 1. Вибір чисел з цих частин відбувається псевдовипадковим чином на основі послідовності 0 та 1, що формуються регістром зсуву з лінійним зворотним зв'язком [3].

Для першої частини формування числа забезпечує лічильник Ліч0, який здійснює лічбу від *0* до $\frac{n}{2} - 1$, а для другої частини – Ліч1, який здійснює лічбу від $\frac{n}{2}$ до n - 1.

У табл. 1 наведено приклад формування ПВЧ з діапазону від 0 до 15. Тут початковий стан Ліч0 – 0, а Ліч1 – 8. Якщо на виході регістра зсуву з лінійним зворотним зв'язком (РЗЗЛЗЗ) формується символ 1, то псевдовипадковим числом є число, що відповідає стану лічильника Ліч1, а у разі формування символу 0 псевдовипадкове число визначається, як стан лічильника Ліч0.

Таблиця 1 – Приклад формування псевдовипадкових чисел.

Вихід РЗЗЛЗЗ	Ліч0	Ліч1	Псевдовипадкові числа
1	0	8 8+1=9	8
0	0 0+1=1	9	0
0	1 1+1=2	9	1
1	2	9 9+1=10	9
0	2 2+1=3	10	2
1	3	10 10+1=11	10
1	3	11 11+1=12	11

Гама формується, як послідовність байтів, що також є послідовністю ПВЧ від 0 до 255. Принцип формування гами аналогічний принципу формування номерів байтів при їх зчитуванні.

Результат зашифрування байту визначається за формулою:

$$C_i = m_p \oplus g$$

де m_p – байт з номером p (число сформовано ГПВЧ номерів), g – байт, що сформований генератором гами**.**

Складові секретного ключа визначають початковий стан та поліном РЗЗЛЗЗ, порядок функціонування Ліч0 і Ліч1 (пряма лічба або зворотня).

Висновки

Запропонований метод потокового шифрування відрізняється від відомих використанням оригінальних генераторів псевдовипадкових чисел для перестановок і замін байтів даних, що зашифровуються, які побудовані за однаковим принципом.

Апаратна та програмна реалізація запропонованого шифру є достатньо простою.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Every day big data statistics – 2.5 quintillion bytes of data created daily [Електронний ресурс]. – Режим доступу: http://www.vcloudnews.com/every-day-big-data-statistics-2-5-quintillion-bytes-of-data-created-daily/
2. Поточные шифры / А. В. Асосков [и др.]; под общ. ред. А. В. Асосков. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с.
3. Иванов, М. А. Теория применения и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В.Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

Лужецький Володимир Андрійович – д.т.н., проф., завідувач кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Дехтяренко Микола Сергійович – факультет інформаційних технологій та комп'ютерної інженерії, група БС-14б, Вінницький національний технічний університет, м. Вінниця, e-mail: mykoladekhtiarenko@gmail.com

Volodymyr A. Luzhetskyy – Doctor Sc. (Eng), Professor, Head of Information Protection Department, Vinnytsia National Technical University, Vinnytsia.

Mykola S. Dekhtiarenko – Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: mykoladekhtiarenko@gmail.com