УДК 681.39

ПОТОКОВИЙ ШИФР НА ОСНОВІ ПСЕВДОНЕДЕТЕРМІНОВАНОГО ГЕНЕРАТОРА ГАМИ

Свистун Д.А.
Науковий керівник - д.т.н., проф. Лужецький В.А.

Потокові шифри мають високу швидкість шифрування, яка пропорційна швидкості надходження вхідної інформації. Вони якнайкраще підходять для оперативного криптографічного захисту.

Алгоритм роботи потокового шифру: на потік бітів вхідної відкритої інформації за допомогою операції виключного АБО (додавання за модулем 2) накладається деяка гама, що становить псевдовипадкову послідовність бітів. Операція виключного АБО є абсолютно симетричною, тому для відновлення інформації достатньо виконати те ж саме накладання гами на зашифрований потік.

Головним складовим елементом потокового шифру є генератор гами.

У доповіді розглядається розроблений алгоритм генерування псевдовипадкової послідовності. Суть цього алгоритму полягає в тому, що на кожному кроці аналізується два біти, значення яких визначає відповідне правило генерування гами. Ці біти отримуються за допомогою операції зсуву на два біти вправо регістра R, в якому спочатку знаходиться значення секретного ключа K:

$\{b_0, b_1\} = R >> 2;$

По мірі зсуву значення ключа в робочий регістр заноситься повідомлення. Тобто після аналізу всіх бітів ключа, аналізуються біти повідомлення.

Залежно від значення цих бітів обирається відповідне правило генерування гами (за один крок генерується два біти гами g_0 та g_1).

Правила генерування:

- якщо значення бітів 00: $\{g_0, g_1\} = R>>2;\ R:= \neg R;$
- якщо значення бітів 01: $\{g_0, g_1\} = R>>2;\ R:= R \oplus K;$
- якщо значення бітів 10: $\{g_0, g_1\} = R>>2;\ R:= R\&K;$
- якщо значення бітів 11: $\{g_0, g_1\} = R>>2;\ R:= R \square K.$

Отже, логічні операції застосовуються до ключа та поточного стану генератора. Окрім випадку значення бітів 00: тоді поточне значення генератора просто інвертується.

Саме змінний характер виконуваних операцій для визначення нового стану генератора і враховується в назві генератора – «псевдонедетермінований».