1. ТЕСТИРОВАНИЕ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Специальная лаборатория включает два блока заданий:

1) Статистический анализ выходных последовательностей блочного алгоритма шифрования.

2) Статистический анализ выходных последовательностей физического генератора случайных чисел.

1.1. Статистический анализ выходных последовательностей блочного алгоритма шифрования

Одним из способов оценки стойкости криптографических алгоритмов является статистическое тестирование их выходных последовательностей. Обнаружение в выходных последовательностях статистически значимых отклонений от свойств дискретной равномерно распределенной последовательности свидетельствует о наличии у криптоалгоритмов нежелательных свойств, использование которых может привести к компрометации криптоалгоритма.

Этапы конкурсов AES и NESSIE, наряду с оценкой стойкости и эффективности предложенных алгоритмов, включали проведение статистического тестирования выходных последовательностей криптоалгоритмов [4, 3] с помощью специальных методов [1, 2].

1.1.1. Сценарии тестирования блочного алгоритма

Пусть $F_K \colon V_n \to V_n$ — алгоритм блочного шифрования с ключом $K \in V_m$. При проведении статистического тестирования на конкурсе AES выходные последовательности алгоритма F_K строились для решения следующих задач.

Исследование вероятностных свойств выходной последовательности режима простой замены при произвольном выборе открытого текста и ключа. Выходная последовательность длиной N блоков для алгоритма F_K строится по следующему правилу:

$$Y_i = F_K(X_i),$$
$$X_i, Y_i \in V_n, \quad K \in V_m, \quad i = \overline{1, N},$$

где $\{X_i\}$ — независимые равномерно распределенные на V_n случайные вектора; K — случайно выбранный из V_m ключ.

Такой тип выходных последовательностей позволяет оценить вероятностные свойства шифртекста, обеспечиваемые алгоритмом при зашифровании в режиме простой замены произвольного открытого текста на случайном ключе.

Исследование вероятностных свойств выходной последовательности режима простой замены при специальном выборе открытого текста и ключа. Выходная последовательность длиной N блоков для алгоритма F_K строится по следующему правилу:

$$Y_i = F_K(X_i),$$
$$X_i, Y_i \in V_n, \quad K \in V_m, \quad i = \overline{1, N},$$

где $\{X_i\}$ и K выбирались следующими способами:

1) в качестве $\{X_i\}$ из V_n выбирались вектора с малым весом Хэмминга (0, 1 или 2), K выбирался случайным образом из V_m;

2) в качестве $\{X_i\}$ из V_n выбирались вектора с большим весом Хэмминга (n, $n-1$, $n-2$), K выбирался случайным образом из V_m;

3) $\{X_i\}$ выбирались случайным образом из V_n, в качестве K из V_m выбирался вектор с малым весом Хэмминга (0, 1 или 2);

4) $\{X_i\}$ выбирались случайным образом из V_n, в качестве K из V_m выбирался вектор с большим весом Хэмминга (m, $m-1$, $m-2$).

Такой тип выходных последовательностей позволяет оценить свойства “перемешивания” и “рассеивания” алгоритма шифрования.

Исследование размножения ошибки при изменении ключа в режиме простой замены. Выходная последовательность длиной $m \cdot N$ блоков для алгоритма F_K строится по следующему правилу:

$$Y_{i,j} = F_{K_i}(X) \oplus F_{K_i \oplus \Delta K^{(j)}}(X),$$
$$X, Y_{i,j} \in V_n, \quad K, \Delta K^{(j)} \in V_m, \quad i = \overline{1, N}, \quad j = \overline{1, m},$$
$$\Delta K^{(j)} = \left(\Delta K_t^{(j)}\right), \quad \Delta K_t^{(j)} = \{1, \text{ если } t = j;\ 0 \text{ иначе}\}, \quad t = \overline{1, m},$$

где $X = (0, \ldots, 0)' \in V_n$, $\{K_i\}$ — независимые равномерно распределенные на V_m случайные вектора.

Такой тип выходных последовательностей позволяет оценить чувствительность алгоритма шифрования к внесению ошибок в ключ.

Исследование размножения ошибки при изменении открытого текста в режиме простой замены. Выходная последовательность длиной $n \cdot N$ блоков для алгоритма F_K строится по следующему правилу:

$$Y_{i,j} = F_K(X_i) \oplus F_K(X_i \oplus \Delta X^{(j)}),$$
$$X_i, Y_{i,j}, \Delta X^{(j)} \in V_n, \quad K \in V_m, \quad i = \overline{1,N}, \quad j = \overline{1,n},$$
$$\Delta X^{(j)} = \left(\Delta X_t^{(j)}\right), \quad \Delta X_t^{(j)} = \{1, \text{ если } t = j;\ 0 \text{ иначе}\}, \quad t = \overline{1,n},$$

где $\{X_i\}$ — независимые равномерно распределенные на V_n случайные вектора; $K = (0, \ldots, 0)' \in V_m$.

Такой тип выходных последовательностей позволяет оценить чувствительность алгоритма шифрования к внесению ошибок в открытый текст.

Исследование корреляции открытого текста и зашифрованного текста в режиме простой замены. Выходная последовательность длиной N блоков для алгоритма F_K строится по следующему правилу:

$$Y_i = X_i \oplus F_K(X_i),$$
$$X_i, Y_i \in V_n, \quad K \in V_m, \quad i = \overline{1,N},$$

где $\{X_i\}$ — независимые равномерно распределенные на V_n случайные вектора; K — случайно выбранный из V_m ключ.

Такой тип выходных последовательностей позволяет корреляцию между открытым и зашифрованным текстом алгоритма шифрования.

Исследование вероятностных свойств выходной последовательности в режиме цепочной обработки. Выходная последовательность длиной N блоков для алгоритма F_K строится по следующему правилу:

$$Y_i = F_K(Y_{i-1}), \quad Y_0 = (0, \ldots, 0)' \in V_n,$$
$$Y_i \in V_n, \quad K \in V_m, \quad i = \overline{1,N},$$

где K — случайно выбранный из V_m ключ.

Выходная последовательность $\{Y_i\}$ соответствует зашифрованию открытого текста $\{X_i\}$, состоящего из нулевых векторов $X_i = (0, \ldots, 0)' \in V_n$, в режиме цепочной обработки с синхропосылкой Y_0.

Такой тип выходных последовательностей позволяет оценить вероятностные свойства шифртекста, обеспечиваемые алгоритмом при зашифровании в режиме цепочной обработки на случайном ключе.

1.1.2. Задание

Указать возможные отклонения от модели чисто случайной последовательности у построенных выборок. Выбрать из [6, 5] набор критериев, способных обнаруживать такие отклонения, и программно реализовать. Провести анализ построенных выборок для блочного алгоритма, разработанного на с/л «Криптографические методы», (с полным и уменьшенным числом тактов). Сделать вывод о стойкости блочного алгоритма.

ЛИТЕРАТУРА

[1] National Institute of Standards and Technology. — NIST Special Publication 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000.

[2] NESSIE report. List of general NESSIE test tools. nes/doc/sag/wp2/d03/1. — 2000. http://www.cryptonessie.org.

[3] *Soto J., Bassham L.* Randomness testing of the Advanced Encryption Standard finalist candidates. — 2000. http://www.nist.gov/aes/.

[4] *Soto J.* Randomness testing of the AES candidate algorithms. — 1999. http://www.nist.gov/aes/.

[5] *Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В.* Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003. — 320 с.

[6] *Харин Ю. С., , Агиевич С. В.* Компьютерный практикум по математическим методам защиты информации. — Минск: БГУ, 2001. — 190 с.