ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 29 МАТЕМАТИКИ Выпуск 1
2022

А. В. Анашкин, П. В. Кожухов (Москва, Лаб. ТВП). **О контрольном примере стандарта ГОСТ Р 34.12-2015 (часть II).**

УДК 519.719.2 DOI https://doi.org/10.52513/08698325_2022_29_1_??

Резюме: Контрольный пример из ГОСТ Р 34.12-2015 и ГОСТ Р 34.12-2018 для алгоритма шифрования «Кузнечик» в режиме простой замены задействует не все переходы используемой подстановки π. Предлагаются новые значения ключа и блока открытого текста, которые устраняют указанный недостаток.

Ключевые слова: ГОСТ Р 34.12-2015, ГОСТ Р 34.12-2018, алгоритм шифрования «Кузнечик», блочный шифр, контрольный пример «Кузнечик», переходы в подстановке алгоритма «Кузнечик».

Национальный стандарт ГОСТ Р 34.12-2015, а также созданный на его основе межгосударственный стандарт ГОСТ Р 34.12-2018 содержат описание двух алгоритмов блочного шифрования «Магма» и «Кузнечик» в режиме простой замены [1, 2]. В Приложении приводятся контрольные примеры: результаты зашифрования одного блока открытого текста на одном ключе для каждого из алгоритмов — «Магма» и «Кузнечик».

В [3] показано, что для приведенных в контрольном примере приложения значения ключа и входного вектора алгоритма «Магма» возникает следующая ситуация: двенадцать переходов из 128 (=8 × 16,8 — подстановок, 16 — переходов) не влияют на значения выходного вектора. Также в работе [3] приведены значения ключа и входного вектора, которые приводят к «задействованию» всех переходов всех подстановок алгоритма «Магма». Далее мы решаем аналогичную задачу для алгоритма «Кузнечик».

В алгоритме «Кузнечик» используется только одна подстановка $\pi : V_8 \to V_8$ на множестве двоичных векторов длины 8, которая имеет 256 переходов. В режиме простой замены контрольного примера эта подстановка используется $(9 \cdot 16 + 4 \cdot 8 \cdot 16 = 41 \cdot 16 = 656$ раз.

Пусть входной блок X и ключ K фиксированы. Через ξ обозначим количество значений аргумента (адресов, если рассматривать подстановку как массив) подстановки π, которые не были использованы при вычислении блока шифрованного текста $Y = E_K(X)$. Понятно, что величина $\xi = \xi(X, K)$ есть функция от двух аргументов X и K.

При случайном равновероятном выборе одного из аргументов при фиксированном другом, а также при одновременном случайном равновероятном и независимом выборе каждого из аргументов, величина $\xi = \xi(X, K)$ становится случайной величиной.

Распределение ξ задается количеством пустых ящиков в схеме размещения $m(= 656)$ различных дробинок по $n(= 256)$ различным ящикам и описывается формулой:

$$\mathbf{P}\{\xi = k\} = \frac{C_n^k(\sum_{s=0}^{(n-k)-1}(-1)^s C_s^{n-k}((n-k)-s)^m)}{n^m}, \qquad k = 0, \ldots, n$$

[4].

Математическое ожидание случайной величины ξ задается формулой:

$$\mathbf{E}\,\xi = n\Big(1 - \frac{1}{n}\Big)^m$$

и при заданных значениях параметров равно $\mathbf{E}\,\xi = 19,4\ldots$, при этом дисперсия равна $\mathbf{D}\,\xi = 14,28\ldots$

Вероятность того, в подстановке будет «задействован» каждый из 256 переходов, составляет:

$$p_0 = \mathbf{P}\{\xi = 0 \approx 3,63 \cdot 10^{-9}\}.$$

В случае выбора блока открытого текста и ключа согласно части А.1 Приложения не будут задействованы 26 переходов, практически $\frac{1}{10}$ часть от общего количества. Изменение значений подстановки π в найденных позициях не изменяет ни результат зашифрования, ни значения промежуточных данных после каждой итерации (часть А.1.4).

Если, как и для алгоритма «Магма» [3], дополнить контрольный пример зашифрованием еще одного блока открытого текста либо расшифрованием иного, отличного от приведенного в части А.1.5 блока шифрованного текста, то распределение случайной величины ξ изменится. В этом случае $m = 1312$ и значения $\mathbf{E}\,\xi$, $\mathbf{D}\,\xi$ и p_0 будут равны $E\xi = 1,52\ldots$, $D\xi = 1,46\ldots$, $p_0 = 0,22\ldots$.

Одновременно отметим одно существенное отличие алгоритма «Кузнечик» от алгоритма «Магма». В алгоритме «Магма» процедура выработки итерационных ключей тривиальная — ключи (части исходного ключа) дублируются через восемь итераций алгоритма. В алгоритме «Кузнечик» используется более сложная процедура выработки итерационных ключей. В частности, в этой процедуре $4 \cdot 8 \cdot 16 = 512$ раз происходит обращение к подстановке π.

В этой связи проведенные нами экспериментальные исследования состояли из двух этапов:

1) проводился поиск ключа K, который давал бы минимальное количество «незадействованных» переходов в подстановке π на этапе выработки итерационных ключей;

2) для найденного ключа проводился поиск входного блока X для которого совокупное (т. е. с учетом и алгоритма выработки итерационных ключей) количество «незадействованных» переходов в подстановке π было бы минимальным.

Ключи K на первом этапе и входные блоки X на втором этапе выбирались случайно и равновероятно.

Такой подход существенно ускорил нахождение ключа и блока такого открытого текста для контрольного примера алгоритма блочного шифрования «Кузнечик», который обеспечивал бы обращение к каждому аргументу подстановки π.

Найденный ключ

$$K = \text{a4edddfff08f08b876e3a5affa216a50755672a2ad0a6b28d8d51b73e9a56799}$$

на шаге выработки итерационных ключей оставлял «незадействованными» только 11 переходов в подстановке π, которые задействовались уже при зашифровании блока

$$X = \text{09e36a83358cf657d9b65c37bbefe714}.$$

Форма представления данных соответствует формату данных стандартов [1, 2].

СПИСОК ЛИТЕРАТУРЫ

1. Федеральное агентство по техническому регулированию и метрологии. Национальный стандарт Российской Федерации ГОСТ Р 34.12-2015. Информационная технология «Криптографическая защита информации». Блочные шифры. Издание официальное. М.: Стандартинформ, 2015, 25 с. // Federal Agency on Technical Regulating and Metrology. Russian Federation, National Standard of the Russian Federation GOST R 34.12-2015. Information Technology «Cryptographic Data Security». Block Ciphers. Official Release. Moscow: Standardinform, 2015, 25 p. (In Russian).

2. Межгосударственный совет по стандартизации, метрологии и сертификации. Межгосударственный стандарт ГОСТ Р 34.12-2018. Информационная технология «Криптографическая защита информации». Блочные шифры. Издание официальное. М.: Стандартинформ, 2018, 12 с. // Interstate Council for Standardization, Metrology and Certification. Interstate Standard GOST R 34.12-2018. Information Technology «Cryptographic Data Security». Block Ciphers. Official Release. Moscow: Standardinform, 2018, 12 p. (In Russian).

3. *Анашкин А. В.* О контрольном примере стандарта ГОСТ Р 34.12-2015. — Обозрение прикл. и промышл. матем., 2020, т. 27, в. 2, с. 133–135. // *Anashkin A. V.* On the testing example in the GOST R 34.12-2015 encryption standard. — OPPM Surv. Appl. Ind. Math., Moscow, 2020, v. 27, is. 2, p. 133–135. (In Russian).

4. *Колчин В. Ф., Севастьянов Б. А., Чистяков В. П.* Случайные размещения. М.: «Наука», 1976, 223 с. // *Kolchin V. F., Savast'yanov B.A., Chistyakov V. P.* Random allocations. M.: Nauka, 1976, 222 p. (In Russian).

UDC 512.643.8 DOI https://doi.org/10.52513/08698325_2022_29_1_1

Anashkin A. V., Kozhukhov P. V. (Moscow, TVP Laboratories). **O kontrole standarta rosta GOST R 34.12-2015 (chast' II).**

Abstract: In the testing example from GOST R 34.12-2015 as well as GOST R 34.12-2018 for KUZNECHIK block cipher in ECB mode not all transitions are possible in the substitution π. New key K and plaintext block X have been found which are devoid of noted flaw.

Keywords: GOST R 34.12-2015, GOST R 34.12-2018, block cipher, «Kuznechik» encryption algorithm, testing example of «Kuznechik», transitions of substitution in «Kuznechik» algorithm.