УДК 681.322

НОВЫЙ МЕТОД ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ПОСЛЕДОВАТЕЛЬНОСТЕЙ КВАЗИСЛУЧАЙНЫХ ЧИСЕЛ

Рейзлин В.И.

Институт кибернетики Томского политехнического университета, Томск, e-mail: vir@tpu.ru

Разработан криптостойкий метод шифрования информации, основанный на специальных перестановках натурального ряда и применении квазислучайных последовательностей. Рассматривается семейство равномерно распределенных последовательностей, обобщающих аналогичные конструкции Соболя. В таких последовательностях все их последовательные участки определенной длины имеют хорошее распределение. При шифровании данных предлагается использовать специальные перестановки натурального ряда (перемешивания). При этом одна и та же перестановка натурального ряда может быть получена различными перемешиваниями и ни по какому начальному участку перестановки натурального ряда нельзя восстановить последовательности, посредством которых эта перестановка была получена. В связи с этим и непериодичностью квазислучайных последовательностей предлагаемый метод шифрования свободен от проблемы «известного текста». Трудности, связанные с вычислением перестановок, снимаются, если представлять их в виде полиномов над конечными кольцами.

Ключевые слова: шифрование информации, квазислучайные последовательности, псевдослучайные последовательности, криптостойкость, проблема «известного текста»

NEW ENCRYPTION METHOD USING A SEQUENCE OF QUASI-RANDOM NUMBERS

Reizlin V.I.

Institute of Cybernetics, Tomsk Polytechnic University, Tomsk, e-mail: vir@tpu.ru

We have developed a cryptographically strong data encryption method based on special permutations of the natural numbers and the application of quasi-random sequences. We consider a family of uniformly distributed sequences generalizing the similar Sobol's constructions. The successive sections of a certain length in such sequences have a good distribution. We offer to encrypt data to use special permutation natural numbers (mixing). In this case, the same permutation of natural numbers can be obtained by various mixings and no initial permutation portion cannot restore sequences through which this permutation was obtained. In this regard, and what quasi-random sequence is not periodic proposed encryption method is free from the problem of «known text». Difficulties associated with the calculation of permutations removed if present them in the form of polynomials over finite rings.

Keywords: data encryption, quasi-random sequences, pseudorandom sequences, cryptographic strength, problem of «known text»

Шифрование данных – давно и широко применяемый метод защиты информации. Существует довольно много различных способов шифрования, есть даже стандартные – такие, как американские новый стандарт шифрования Advanced Encryption Standard (AES) [9] и старый Data Encryption Standard (DES) [10], или ГОСТ 28147-89 – российский стандарт [1]. Обладая несомненными достоинствами, все они имеют и недостатки, порой весьма существенные. Так, например, старый американский стандарт DES рассчитан на реализацию в специальных электронных устройствах, и это существенно ограничивает возможности его использования, а алгоритм, положенный в основу российского стандарта, настолько громоздок, что его программная реализация чрезвычайно сложна и практически лишена смысла из-за крайне низкого быстродействия. Недостатком же алгоритма AES можно считать его слабое теоретическое исследование, поэтому он может содержать неявные уязвимости, которые могут проявиться только через некоторое время с момента начала его распространения.

Методы шифрования с использованием псевдослучайных чисел

Очень популярными являются методы шифрования с использованием последовательностей псевдослучайных чисел (далее – ПСЧ). Они просты, легко реализуются и модифицируются, имеют высокое быстродействие.

Принцип шифрования очень прост: на данные, подлежащие защите, с помощью операции «исключающее или» байт за байтом, либо слово за словом (или в каком-либо другом порядке) накладывается сгенерированная ПСЧ – шифр. Расшифровка сводится к повторному наложению той же последовательности на зашифрованные данные (для этого-то и применяется «исключающее или»). Зашифрованный текст достаточно труден для раскрытия, если длина шифра превышает длину всего шифруемого текста и если неизвестна никакая значительная часть исходного текста.

Обычно для получения псевдослучайных чисел используют конгруэнтные генераторы, например [2, 11]. Они вырабатывают ПСЧ α_i, описываемые соотношением

$$\alpha_{i+1} = (a \cdot \alpha_i + b) \bmod M,$$

где a и b – специальным образом выбранные константы, а значение M обычно выбирается равным величине наибольшего целого числа, представляемого машинным словом. Очевидно, что последовательности, вырабатываемые по этому правилу, имеют период, равный M. При шифровании больших текстов периодичность приводит к снижению криптостойкости. Можно строить ПСЧ и с большими периодами. Известен ряд генераторов с очень большими периодами [4]. Однако число хороших генераторов как с обычными, так и с большими периодами весьма невелико, что способствует облегчению раскрытия зашифрованных данных.

Построение квазислучайных последовательностей

Можно, однако, использовать все достоинства ПСЧ-шифрования, применяя квазислучайные последовательности вместо псевдослучайных. Эти последовательности не периодичны, что позволяет применять их для шифрования данных произвольного объема. Квазислучайными называют последовательности, распределение элементов в которых в некотором смысле беспорядочно. Это распределение не обязано имитировать независимость соседних значений.

Последовательность X_n точек из d-мерного куба $I^d = [0,1)\times...\times[0,1)$ называется равномерно распределенной в I^d, если для любого блока $B = [a_1,b_1)\times[a_2,b_2)\times ...\times[a_d, b_d)$, где $0 \le a_i,\ b_i \le 1$ выполняется соотношение $\lim\limits_{n\to\infty} \dfrac{|X_n \cap B|}{n} = \coprod\limits_{i=1}^{d}(b_i - a_i)$. Здесь $\coprod\limits_{i=1}^{d}(b_i - a_i)$ означает копроизведение. Другими словами, последовательность равномерно распределена, если при больших n количество ее точек, попавших в какой-либо блок, пропорционально его объему. Если разбить куб на несколько равновеликих частей, то в каждой из них (при достаточно больших n) окажется примерно одинаковое число точек последовательности.

Ряд квазислучайных последовательностей был получен в [13, 15]. Подобные последовательности обычно называют $ЛП_0$-последовательностями, или последовательностями Соболя. В работе [5] получено новое семейство квазислучайных последовательностей, моделирующих хорошее равномерное распределение, как для больших, так и для малых значений числа элементов. Не отступая от традиции, распространим это название и на наши конструкции, так как обозначение «ЛП» в нашем контексте может означать, что *любой последовательный* участок X_n хорошо распределен.

Эти последовательности строятся следующим образом.

Пусть $q = p^n$, где p – простое число. Назовем q-и отрезками ранга s интервалы $\dfrac{t}{q^s} + [0, \dfrac{1}{q^s})$, $0 \le t \le q^s - 1$. Эти отрезки получаются при разбиении интервала $I = [0,1)$ на q^s равных отрезков. Обобщая это определение на многомерный случай, назовем q-ым блоком ранга s параллелепипед $B_1\times...\times B_d$ в d-мерном кубе $I^d = [0,1)\times...\times[0,1)$, где B_i – q-ые отрезки рангов $s_1, s_2, ..., s_q$ соответственно, причем $s_1 + ... + s_q = s$.

Таким образом, q-ые отрезки – это просто одномерные q-ые блоки.

Последовательные участки множества целых неотрицательных чисел $kq^s + \{0, q^s - 1\}$, $k = 0, 1, 2, ...$ назовем q-ыми участками ранга s. Точно так же будем называть и соответствующие участки произвольных последовательностей. Последовательность X_n точек из I^d назовем аналогично [5, 13] ЛП-последовательностью, если каждый ее q-ый участок ранга s имеет ровно по одной общей точке с каждым q-ым блоком того же ранга. Как показано в [5], имеет место теорема 1:

1. Проекции ЛП-последовательности на k-мерные грани куба I^d также являются ЛП-последовательностями, и ЛП-последовательности равномерно распределены в I^d.

Приведем примеры ЛП-последовательностей.

Любое число x из интервала $I = [0, 1)$ можно записать в q-ой системе счисления в виде $x = \sum\limits_{i=0}^{\infty} \dfrac{x_i}{q^{i+1}}$, $0 \le x_n \le q - 1$. Заметим, что q-но рациональные числа, т.е. числа вида $\dfrac{t}{q^s}$, $0 \le t \le q^s - 1$ имеют две различных q-ых записи:

$$x = \sum_{i=0}^{s} \frac{x_i}{q^{i+1}} + \sum_{i=s+1}^{\infty} \frac{q-1}{q^i} \text{ и } x = \sum_{i=0}^{s-1} \frac{x_i}{q^{i+1}} + \frac{x_s + 1}{q^{s+1}} + \sum_{i=s+1}^{\infty} \frac{0}{q^i}.$$

Каждое неотрицательное целое число n можно записать в q-ной системе счисления в виде $n = n_0 + n_1 q + n_2 q_2 + \ldots + n_s q^s$, $0 \le n_i \le q - 1$ и $n \ne 0$. Обозначим номер старшей q-ой цифры как $r(n)$. Число $\tilde{n} = n_s + n_{s-1} q + \ldots + n_0 q^s$ назовем инверсным к n. Сопоставим каждому n q-но рациональное число $h(n) = \frac{\tilde{n}}{q^{r(n)+1}} = \sum_{i=0}^{s} \frac{n_i}{q^{i+1}}$. Таким образом, множество целых неотрицательных чисел вкладывается отображением h в интервал $I = [0,1)$. Очевидно, что последовательность $h(n)$ является одномерной ЛП-последовательностью.

На самом деле справедливо даже более сильное утверждение:

Любые q^s последовательных точек из $(h(n))\big|_{n=0}^{\infty}$ лежат в разных q-ых отрезках ранга s.

Построим теперь целое семейство ЛП-последовательностей.

Каждому целому неотрицательному числу $n = n_0 + n_1 q + \ldots + n_s q^s$, представленному его q-ой записью, сопоставим бесконечномерный вектор $\overline{n} = < n_0, n_1, \ldots, n_s, 0, 0, \ldots >$.

Пусть $A = (a_{ij}) i$, $j \in \{0,1,\ldots,\infty\}$, $0 \le a_{ij} \le q - 1$, бесконечная матрица над конечным полем F_q, такая, что все ее подматрицы $A_s = (a_{ij})$, $i, j \in \{0,1,\ldots,s\}$ не вырождены, и пусть $A(n)$ – число, соответствующее произведению $A \cdot \overline{n} = < \ldots, \sum_{k=0}^{r(n)} a_{mk} n_k \ldots >$, (вычисления здесь проводятся в арифметике поля F_q). Тогда последовательность $h(A(n))$ – ЛП-последовательность и для $h(A(n))$ справедливо утверждение теоремы 1 [5].

Методы шифрования с использованием квазислучайных чисел

Пусть выбрана последовательность $A = \{a_0, a_1, \ldots a_s \ldots\}$, где каждое a_i – натуральное число, большее 1. И пусть $m = 1$, $m_1 = a_0, \ldots, m_s = m_{s-1} \cdot a_{s-1}$. Любое целое положительное число n может быть представлено в виде $n = n_0 + n_1 m_1 + \ldots + n_s m_s$, где n_i – целые числа, удовлетворяющие неравенствам $0 \le n_i \le a_i - 1$. Пусть теперь для каждого i выбрана некоторая перестановка P_i множества $\{0,\ldots, a_i - 1\}$, оставляющая на месте 0.

Бесконечная непериодическая последовательность чисел $\alpha(n) = P_0(n_0) + P_1(n_1) m_1 + \ldots + P_s(n_s) m_s$ может использоваться в качестве шифрующей последовательности вместо ПСЧ. Способ построения таких последовательностей назовем (A, P)-перемешиванием, где P – последовательность рассмотренных выше перестановок. Все способы повышения криптостойкости ПСЧ-методов [6] применимы и для построенных последовательностей. Однако при их бесхитростном применении, например, когда все a_i равны друг другу и все P_i представляют собой одну и ту же перестановку, проблема известного текста, так же как и для ПСЧ-шифрования, является слабостью метода.

Речь идет о следующем. Предположим, что шифр неизвестен, но имеется часть исходного текста и соответствующая ему часть зашифрованного, и кроме этого имеется возможность добавлять записи к тексту и проверять зашифрованный текст до и после добавления известной записи. Если шифр представляет собой последовательность чисел, каждое из которых может быть получено из предыдущего, то весь исходный текст можно восстановить из зашифрованного. Все последовательности, элементы которых вычисляются с помощью рекуррентных соотношений, имеют этот недостаток. Все ПСЧ-последовательности и последовательности, полученные (A, P)-перемешиванием с равными a_i и P_i, рекуррентно вычислимы, и поэтому их вряд ли стоит применять для шифрования данных без дополнительных усовершенствований, ряд из которых описан в [6–8].

В общем случае (A, P)-перемешивание приводит к шифрам, восстановить которые при известном исходном тексте можно лишь, если известна практически вся последовательность A и все перестановки P_i.

Более изощренным, но и более криптостойким является метод, рассматриваемый ниже.

Пусть $D = \{d_0, d_1, \ldots, d_i, \ldots\}$ какая-либо последовательность натуральных чисел, больших 1. Разобьем натуральный ряд на бесконечное число участков ω_i с длинами d_i. Каждое натуральное число n может быть охарактеризовано двумя номерами s и r, где s – номер участка, которому принадлежит n, а r – его порядковый номер на этом участке.

Переставим числа в каждом участке, применив к номерам r некоторую перестановку Q_i множества $\{0,\ldots, d_i - 1\}$, и после этого поменяем порядок следования самих участков, применив к номерам s некоторое (A, P)-перемешивание. Полученную перестановку натурального ряда назовем (A, P, D, Q)-перемешиванием.

Нетрудно проверить следующие утверждения:

1. Одна и та же перестановка натурального ряда может быть получена различными (A, P, D, Q)-перемешиваниями;

2. Ни по какому начальному участку перестановки натурального ряда нельзя восстановить последовательности A, P, D и Q,

посредством которых эта перестановка была получена.

Таким образом (A,P,D,Q)-перемешивание можно эффективно использовать для шифрования текстов любой длины, проблема известного исходного текста при этом не возникает.

Трудности, связанные с вычислением перестановок снимаются, если представлять их в виде полиномов над конечными кольцами. Известно [12], что любая функция над конечным полем может представляться полиномом.

Кроме того, эффективность метода может быть увеличена с помощью параллельных вычислительных технологий [3, 14].

Список литературы

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. URL: http://protect.gost.ru/v.aspx?control=7&id=139177 (дата обращения: 2.12.2014).

2. Вильданов Р.Р., Мещеряков Р.В., Бондарчук С.С. Тесты псевдослучайных последовательностей и реализующее их программное средство // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1. – С. 108–111.

3. Дёмин А.Ю., Рейзлин В.И. Анализ программного обеспечения на основе структурно-графического представления // Проблемы информатики. – 2011. – № 4(12). – С. 6–15.

4. Левитан Ю.Л., Соболь И.М. О датчике псевдослучайных чисел для персональных компьютеров // Математическое моделирование. – 1990. – Т.2, № 8. – С. 119–126.

5. Орлов В.А., Рейзлин В.И. Новое семейство квазислучайных последовательностей // Известия Томского политехнического университета. – 2012. – Т. 320, № 2. – С. 24–26.

6. Спесивцев А.В., Вегнер В.А. Крутяков А.Ю., Серегин В.В., Сидоров В.А. Защита информации в персональных ЭВМ. – М.: Радио и связь. – 1993. – 191 с.

7. Ходашинский И.А., Мещеряков Р.В., Рубанов С.А. Гибридная система обнаружения вторжений на базе нечеткого классификатора с использованием жадного и генетического алгоритмов // Вопросы защиты информации. – 2013. – № 4 (102). – С. 67–72.

8. Ходашинский И.А., Савчук М.В., Горбунов И.В., Мещеряков Р.В. Технология усиленной аутентификации пользователей информационных процессов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2011. – № 2–3. –С. 236–248.

9. FIPS PUB 197: the official AES standard, 2001. Схема доступа: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (дата обращения 2.12.2014).

10. FIPS PUB 46-3, Federal Information Processing Standards Publication: Data Encryption Standard (DES) (25 OCT 1999). Схема доступа: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf (дата обращения 2.12.2014).

11. Knuth Donald E., The Art of Computer Programming, vol. 2, ch. 3, Addison-Wesley, 1968.

12. R. Lidl and H. Niederreiter, Finite Fields (Encyclopedia of Mathematics and its Applications), Addison-Wesley, 1983.

13. H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, Philadelphia: SIAM, 1992.

14. Reyzlin V.I. and Tartakovsky E.A. Solving Problems of Adaptive Optics Using Parallel Algorithms Based on the CUDA Technology, 7th International Forum on Strategic Technology (IFOST-2012), vol. 1, pp. 621-623, Tomsk, September 18-21, 2012.

15. Sobol' I. M., «On the distribution of points in a cube and the approximate evaluation of integrals», Zh. Vychisl. Mat. Mat. Fiz., 7:4 (1967), 784-802.

References

1. GOST 28147-89. Available at: http://protect.gost.ru/v.aspx?control=7&id=139177 (accessed 2 December 2014).

2. Vildanov R.R., Meshcheryakov R.V., Bondarchuk S.S. Proceedings of Tomsk State University of Control Systems and Radioelectronics, 2012, no 1, pp. 108–111.

3. Demin A.Yu. and Reizlin V.I. Problems of Informatics, no 4(12), 2011, pp. 6-15.

4. Levitan Ju.L., Sobol' I.M. Matematicheskoe modelirovanie, 1990, Vol 2, no 8, pp. 119–126.

5. Orlov V.A., Reizlin V.I.. Bulletin of the Tomsk Polytechnic University, 2012, Vol. 320, no 2, pp. 24–26.

6. Spesivcev A.V., Vegner V.A., Krutjakov A.Ju., Seregin V.V., Sidorov V.A. *Zashhita informacii v personal'nyh JeVM* [Data protection in personal computers]. Moscow: Radio i svjaz', 1993. 191 p.

7. Hodashinskij I.A., Meshcheryakov R.V., Rubanov S.A. Voprosy zashhity informacii. no 4(102), 2013. pp. 67–72.

8. Hodashinskij I.A., Savchuk M.V., Gorbunov I.V., Meshcheryakov R.V. Proceedings of Tomsk State University of Control Systems and Radioelectronics, 2011. no 2–3, pp. 236–248.

9. FIPS PUB 197, 2001. Available at: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (accessed 2 December 2014).

10. FIPS PUB 46-3, Federal Information Processing Standards Publication. Available at: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf (accessed 2 December 2014).

11. Knuth Donald E., The Art of Computer Programming, vol. 2, ch. 3, Addison-Wesley, 1968.

12. R. Lidl and H. Niederreiter, Finite Fields (Encyclopedia of Mathematics and its Applications), Addison-Wesley, 1983.

13. H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, Philadelphia: SIAM, 1992.

14. Reyzlin V.I. and Tartakovsky E.A. Solving Problems of Adaptive Optics Using Parallel Algorithms Based on the CUDA Technology, *7th International Forum on Strategic Technology* (*IFOST-2012*), vol. 1, pp. 621–623, Tomsk, September 18-21, 2012.

15. Sobol' I.M., Zh. Vychisl. Mat. Mat. Fiz., 7:4, 1967, pp. 784–802.

Рецензенты:

Погребной В.К., д.т.н, профессор, профессор кафедры «Информатики и проектирования систем», Национальный исследовательский Томский политехнический университет, г. Томск;

Мещеряков Р.В., д.т.н, профессор, профессор кафедры комплексной информационной безопасности электронно-вычислительных систем, Томский государственный университет систем управления и радиоэлектроники, г. Томск.

Работа поступила в редакцию 16.12.2014.