

- Пароль формируется за счет добавления и/или преобразования отдельных элементов в формируемом поле в каждом узле дерева. Количество вариантов формирования пароля в этом случае увеличивается в $\prod_i a_i$ раз, где a_i – количество узлов на i -м уровне дерева.

Для повышения стойкости системы парольной защиты данных можно также использовать алгоритм многопрограммной генерации парольного доступа с последовательным алгоритмом запуска программ. При этом в зависимости от ввода комбинации символов в данном случае на выполнение будут запускаться последовательно ряд программ из набора ПГП. В этом случае может быть реализован некий сценарий доступа к системе, при реализации которого от пользователя потребуется ввод ряда ответов на поставленные вопросы, что обеспечит последовательное выполнение ПГП в соответствии с заданным алгоритмом.

Известно, что при наборе пароля, хотя он, как правило, на экране не отображается, следует всё же избегать чужих глаз. Предлагаемый алгоритм программной генерации пароля предоставляет возможность легко справиться с данной задачей. Для этого необходимо программу генерации пароля оформить в виде макроса MS Word или MS Excel. Тогда порядок ввода пароля может быть следующим:

- пользователь вызывает, например, текстовый документ, содержащий встроенный макрос генерации паролей;
- при загрузке документа либо при выполнении определенных действий с текстом макрос запускается на выполнение и генерирует пароль, который записывает в буфер обмена Office;
- сгенерированный макросом пароль из буфера обмена вводится в поле ввода пароля и очищается буфер обмена.

Еще одно достоинство предлагаемого алгоритма заключается в том, что сгенерированный пароль можно передавать в поле ввода через буфер обмена. При этом не используется клавиатура, что является дополнительной степенью защиты пароля пользователя от так называемых программ «клавиатурных шпионов».

IV Результаты

Авторами разработан на языке ASP.net ряд простых, но эффективных программ генерации паролей. Данные программы используются для реализации как однопрограммного, так и многопрограммного алгоритма парольного доступа к данным. Опыт использования предложенных алгоритмов показал, что их применение не только не усложняет задачу парольного доступа к данным, но в отдельных случаях облегчает процедуру ввода пароля.

V Выводы

Описанный алгоритм, с одной стороны, облегчает пользователю решение проблемы запоминания и хранения стойких паролей, а с другой стороны – повышает стойкость системы хранения данных к несанкционированному доступу за счет использования максимально сложной символьной комбинации пароля.

Литература: 1. Бэнкс М. А. Информационная защита ПК: Перевод с английского – К.: ВЕК+, 2001 – 272 с. 2. Скляр Д. В. Искусство защиты и взлома информации. – СПб.: БХВ – Петербург, 2004 – 288 с. 3. Кнут Д. Искусство программирования для ЭВМ. Т. 1. Основные алгоритмы. – М.: Мир, 1976, 734 с.

УДК 681.3.06

ЛИНЕЙНЫЙ СТОХАСТИЧЕСКИЙ АЛГОРИТМ ШИФРОВАНИЯ, БАЗИРУЮЩИЙСЯ НА КАНОНИЧЕСКОМ РАЗЛОЖЕНИИ СЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Игорь Атаманюк

Николаевский государственный аграрный университет

Анотація: Розглянуто метод шифрування, який дозволяє перетворити повідомлення, що передається, в послідовність некорельованих значень, що суттєво ускладнює задачу відтворення початкових даних. Алгоритм базується на канонічному розкладі випадкової послідовності, що досліджується.

Summary: An encoding method has been achieved as the result of the following work. The method allows us to transform a sending message into a sequence of the uncorrelated values. This makes the solution of basic data extrapolation essentially harder. The algorithm is based on canonical decomposition of researching casual sequence.

Ключові слова: Алгоритм шифрування, лінійні стохастичні зв'язки.

I Введение

Одним из перспективных направлений защиты информации, как известно [1, 2], является использование стохастических алгоритмов – методы защиты информации, прямо или косвенно основанные на использовании генераторов псевдослучайных последовательностей. В настоящее время существует два наиболее существенных класса стохастических методов: 1) стохастические алгоритмы, основанные на использовании свойств эллиптических кривых (Elliptic Curves (EC)) [1, 3 – 4]; 2) дихотомические генераторы псевдослучайных последовательностей [1, 5].

Методы первого класса являются наиболее математически обоснованными, однако остается открытым вопрос о существовании односторонней функции [6] (зная принцип ее работы и фрагмент выходной последовательности, но не имея в наличии ключевой информации, криптоаналитик для определения предыдущего выбранного элемента последовательности не может предложить лучшего способа, чем использование жребия). Существуют только функции-кандидаты, претендующие называться односторонними. Примером такого преобразования является дискретное логарифмирование, осуществляемое на группе точек эллиптической кривой. Для точек эллиптической кривой вводится операция сложения, которая играет ту же роль, что и операция умножения в криптосистемах, основанных на задаче факторизации больших чисел (криптосистема RSA) и задаче дискретного логарифма в конечных полях (криптосистема Эль-Гамала).

Основу алгоритмов второго класса составляют дихотомические операторы, иначе D-операторы. Один из типовых вариантов реализации D-генераторов, преобразующих предыдущий бит B_{i-1} в B_i , представляется самосинхронизирующимся трехпараметрическим оператором $R_H(P_{i-1}, Q_{i-1}, D_{i-1}, H) : B_{i-1} \rightarrow \{B_i, P_i, Q_i, D_i\}$, с коэффициентом H и косвенным выходом $r_i = Q_{i-1} \oplus P_{i-1}$ или $r_i = Q_{i-1} \oplus D_{i-1}$, составленным из операторов:

$$B_i = B_{i-1} \oplus P_{i-1}, \quad P_i = (2^g \cdot Q_{i-1}) \oplus D_{i-1} \quad (g \geq 2), \\ Q_i = B_{i-1} \oplus H, \quad D_i = (2 \cdot (Q_{i-1} \wedge P_{i-1})) \vee 1.$$

Основными достоинствами D-операторов является эффективная программная и аппаратная реализация и возможность построения на их основе всех симметричных криптографических примитивов. Однако в силу свойств, присущих регулярным D-операторам, младшим битам формируемых на их основе дихотомических последовательностей присуща существенно выраженная корреляция, которая убывает от младших битов D-последовательности к старшим [5].

Таким образом, в настоящее время остается актуальной проблема совершенствования стохастических методов защиты данных.

Цель работы – получение алгоритма шифрования, преобразующего исходное сообщение в шифркод, который не обладает линейными вероятностными связями, то есть представляет собой совокупность некоррелированных значений, что существенно усложняет раскрытие зашифрованного текста.

II Математическая постановка задачи и её решение

Предположим, что для некоторого словаря $\overline{X}_l = \{x(1), \dots, x(l)\}$ (соответствие между символами и их числовыми значениями может быть выбрано, например, $x_i = i$) стохастические связи букв $X(i) = x_j, j = \overline{1, l}$ в словах характеризуются матрицей $M[X(i), X(j)], i, j = \overline{1, l}$ (взаимосвязь букв в различных словах является слабой и ею можно пренебречь). Необходимо получить алгоритм шифрования, преобразующий каждое слово $X(i), i = \overline{1, l}$ (l – количество букв в слове) исходного сообщения в шифркод стохастически независимых в рамках линейных связей значений $V_i, i = \overline{1, l}$.

Соответствие между первой буквой $X(1)$ последовательности $X(i)$, $i = \overline{1, I}$ и значением V_1 шифрключа может быть выбрано произвольным образом, например, $V_1 = X(1)$.

Второе значение представим в виде

$$V_2 = X(2) - V_1\varphi_1(2), \quad (1)$$

где $\varphi_1(2)$ - неслучайная координатная функция, удовлетворяющая условию $M[V_1V_2] = 0$, что дает

$$\varphi_1(2) = \frac{M[V_1X(2)]}{M[V_1^2]} = \frac{M[X(1)X(2)]}{M[X^2(1)]} \quad (2)$$

Третье значение V_3 шифрключа определяется из соотношения

$$V_3 = X(3) - V_1\varphi_1(3) - V_2\varphi_2(3), \quad (3)$$

где $\varphi_1(3), \varphi_2(3)$ вычисляются из условий $M[V_1V_3] = 0, M[V_2V_3] = 0$.

Очевидно, что

$$\varphi_1(3) = \frac{M[V_1X(3)]}{M[V_1^2]} = \frac{M[X(1)X(3)]}{M[X^2(1)]}, \quad (4)$$

$$\varphi_2(3) = \frac{M[V_2X(3)]}{M[V_2^2]}. \quad (5)$$

Учитывая выражение (1), получаем

$$\varphi_2(3) = \frac{M[X(2)X(3)] - M[X^2(1)]\varphi_1(2)\varphi_1(3)}{M[X^2(2)] - M[X^2(1)]\varphi_1^2(2)}, \quad (6)$$

Для V_4 справедливо

$$V_4 = X(4) - V_1\varphi_1(4) - V_2\varphi_2(4) - V_3\varphi_3(4). \quad (7)$$

Координатные функции $\varphi_1(3), \varphi_2(3), \varphi_3(4)$ обеспечивают выполнение условий $M[V_1V_4] = 0, M[V_2V_4] = 0, M[V_3V_4] = 0$:

$$\varphi_1(4) = \frac{M[V_1X(4)]}{M[V_1^2]} = \frac{M[X(1)X(4)]}{M[X^2(1)]}, \quad (8)$$

$$\varphi_2(4) = \frac{M[V_2X(4)]}{M[V_2^2]} = \frac{M[X(2)X(4)] - M[X^2(1)]\varphi_1(2)\varphi_1(4)}{M[X^2(2)] - M[X^2(1)]\varphi_1^2(2)}, \quad (9)$$

$$\varphi_3(4) = \frac{M[V_3X(4)]}{M[V_3^2]}. \quad (10)$$

С использованием (3) находим соотношение для определения $\varphi_3(4)$ в окончательном виде

$$\varphi_3(4) = \frac{M[X(3)X(4)] - M[X^2(1)]\varphi_1(3)\varphi_1(4)M[X(3)X(4)] - M[X^2(1)]\varphi_1(3)\varphi_1(4)}{M[X^2(3)] - M[X^2(1)]\varphi_1^2(3) - M[X^2(2)]\varphi_2^2(3)}. \quad (11)$$

Таким образом, для одинаковых нижних индексов координатные функции имеют одинаковую форму записи (выражения (2), (4), (8) и (4), (6), (10)).

Обобщая рассуждения на произвольное число букв $X(i)$, $i = \overline{1, I}$, получаем следующие соотношения для V_i :

$$V_i = X(i) - \sum_{v=1}^{i-1} V_v\varphi_v(i), i = \overline{1, I}, \quad (12)$$

$$\varphi_v(i) = \frac{M[V_v X(i)]}{M[V_v^2]} = \frac{M[X(v)X(i)] - \sum_{j=1}^{v-1} M[V_j^2] \varphi_j(v) \varphi_j(i)}{M[V_v^2]}, \quad (13)$$

$$M[V_v^2] = M[X^2(v)] - \sum_{j=1}^{v-1} M[V_j^2] \varphi_j^2(v). \quad (14)$$

С помощью выражений (12) – (14) слово $X(i) = x(i)$, $i = \overline{1, I}$ преобразуется в шифр-последовательность некоррелированных случайных коэффициентов V_i , $i = \overline{1, I}$.

Таким образом, получен алгоритм шифрования, который позволяет скрыть линейные вероятностные связи исходного сообщения, что существенно усложняет криптоаналитику задачу раскрытия зашифрованного текста.

Выражения (7) – (9) являются одной из разновидностей канонического разложения случайной последовательности [7].

Значения $M[X(i), X(j)]$, $i, j = \overline{1, 10}$ и $\varphi_v(i)$, $v, i = \overline{1, 10}$ для украинского толкового словаря представлены соответственно в табл. 1 и 2.

Таблица 1 – Значения $M[X(i), X(j)]$, $i, j = \overline{1, 10}$ для украинского толкового словаря

	1	2	3	4	5	6	7	8	9	10
1	211,3	156	168,2	172,9	175	174,8	173,3	171,4	172,9	178,8
2	156	208,7	149,3	162,2	162,5	161,9	159,6	158,6	158,2	164,5
3	168,2	149,3	217,3	173,5	174,1	174,7	173,3	170,9	173,5	178,8
4	172,9	162,2	173,5	244,5	182,4	180,6	180,9	178,7	180,5	187,2
5	175	162,5	174,1	182,4	246,2	184,9	179,4	181	182,2	191,2
6	174,8	169,9	174,7	180,6	184,9	249,8	184,7	174,8	184,6	187,8
7	173,3	159,6	173,3	180,9	179,4	184,7	249,5	181,6	173,2	192,9
8	171,4	158,6	170,9	178,7	181	174,8	181,6	246,6	183,6	175,5
9	172,9	158,2	173,5	180,5	182,2	184,6	173,2	183,6	252,8	191,5
10	178,8	164,5	178,8	187,2	191,2	187,8	192,9	175,5	191,5	269,4

Таблица 2 – Значения $\varphi_v(i)$, $v, i = \overline{1, 10}$ для украинского толкового словаря

	1	2	3	4	5	6	7	8	9	10
1	1	0,74	0,79	0,82	0,83	0,83	0,82	0,81	0,82	0,85
2	0	1	0,27	0,37	0,36	0,35	0,34	0,34	0,33	0,35
3	0	0	1	0,35	0,34	0,35	0,35	0,34	0,36	0,36
4	0	0	0	1	0,22	0,20	0,23	0,22	0,23	0,24
5	0	0	0	0	1	0,21	0,15	0,19	0,19	0,23
6	0	0	0	0	0	1	0,19	0,08	0,19	0,15
7	0	0	0	0	0	0	1	0,18	0,03	0,21
8	0	0	0	0	0	0	0	1	0,19	-0,02
9	0	0	0	0	0	0	0	0	1	0,18
10	0	0	0	0	0	0	0	0	0	1

Значения в табл. 1 и 2 получены при однократном использовании слова и не отражают частоту появления слова в определенном тексте. Для практического использования алгоритма шифрования (12) – (14) необходимо, естественно, накапливать базу знаний вероятностных параметров по множеству текстов определенной тематики.

Алгоритм (12) – (14) допускает дальнейшие модификации, улучшающие его стойкость, в частности применение системы омофонов для маскировки частот появления коэффициентов V_i , $i = \overline{1, I}$. Для скрытия вероятностных связей более высоких порядков могут быть использованы соответствующие канонические разложения [8 – 9].

III Выводы

Анализ стохастических методов шифрования данных показал, что существующие алгоритмы не позволяют полностью скрыть вероятностные связи исходного сообщения и, таким образом, совершенствование данных методов является актуальной проблемой.

В работе рассмотрен метод шифрования, который позволяет преобразовать передаваемое сообщение в последовательность некоррелированных значений, что существенно затрудняет задачу вскрытия исходных данных. Алгоритм базируется на каноническом разложении исследуемой случайной последовательности.

Предложенный метод шифрования проверен для украинского языка. В качестве исходных данных для определения параметров алгоритма был использован украинский толковый словарь (22 тыс. слов).

В работе также предложены дальнейшие пути совершенствования полученного алгоритма шифрования.

Литература: 1. Иванов М. А., Чугункова И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.: КУДИЦ-ОБРАЗ, 2003. – 240 с. 2. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. - М.: КУДИЦ-ОБРАЗ, 2001. – 361 с. 3. Alfred Menezes., Minghua Qu., Scott Vanstone. IEEE P1363, Part 4: Elliptic Curve Systems. 1995. 4. Gong G., Lam C.C.Y. Linear Recursive Sequences over Elliptic Curves. 2001.<http://citeseer.ist.psu.edu/449444.html>. 5. Кулаков И. А. Стохастические системы и их применение в криптографии. Дихотомические последовательности и генераторы. – Материалы 8-ой конференции «РусКрипто'2006». 6. Введение в криптографию / Под общ. ред. В. В. Яценко. М.: МЦНМО, 2000. 7. Пугачев В. С. Теория случайных функций и ее применение. - М.: Физматгиз, 1962. - 720 с. 8. Атаманюк И. П. Полиномиальный алгоритм оптимальной экстраполяции параметров стохастических систем. //Управляющие системы и машины. – 2002. - №1. 9. Атаманюк И. П. Алгоритм реализации нелинейной случайной последовательности на базе ее канонического разложения. //Электронное моделирование. - 2001. - №5. с. 38 - 46.

УДК 621.391:519.7:510.5

АЛГОРИТМ ФОРМИРОВАНИЯ МАТРИЦ НАД ПРИМАРНЫМ КОЛЬЦОМ ВЫЧЕТОВ ДЛЯ ПОСТРОЕНИЯ ПРОТОКОЛОВ МНОЖЕСТВЕННОГО РАЗДЕЛЕНИЯ СЕКРЕТА, РЕАЛИЗУЮЩИХ ЗАДАННУЮ ИЕРАРХИЮ ДОСТУПА

Андрей Волошин

Институт специальной связи и защиты информации НТУУ “КПИ”

Аннотация: Предложен алгоритм формирования матриц над примарным кольцом вычетов, предназначенных для построения линейных совершенных протоколов множественного разделения секрета для заданной иерархии доступа. Указанный алгоритм обобщает известный ранее алгоритм формирования матриц над конечным полем для синтеза линейных протоколов разделения одного секрета и имеет меньшую временную сложность по сравнению с тривиальным алгоритмом.

Summary: Perfect linear multi-secret sharing schemes over primary residue ring construction algorithm is proposed. Early known secret sharing schemes over finite field construction method is generalized by proposed algorithm. This algorithm has calculation complexity, which less compare with trivial algorithm.

Ключевые слова: Криптографическая защита информации, протокол множественного разделения секрета, иерархия доступа, кольцо вычетов.

I Введение

Протокол или схема разделения секрета (ПРС) представляет собой криптографический протокол, позволяющий “разделить” некоторый секретный параметр (секрет) среди множества участников протокола таким образом, чтобы только некоторые, заранее определенные (разрешенные) коалиции участников могли восстановить его значение при объединении хранящейся у них индивидуальной секретной информации (проекции секрета). Протокол разделения секрета, в котором участники запрещенных коалиций не могут