УДК 004.056.004.94

ТЕОРЕТИКО-ИГРОВОЙ МЕТОД ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ ДАННЫХ С РАНДОМИЗИРОВАННЫМ ПРИМЕНЕНИЕМ АЛГОРИТМОВ DES И RSA

В.С. Моисеев, Л.Т. Моисеева

Для повышения информационной безопасности предлагается оригинальный подход к рандомизированному использованию в информационных системах широко распространенных алгоритмов шифрования и дешифрования данных DES и RSA.

Ключевые слова: математическая модель игры, решение игры, физическая смесь стратегий, метод Монте-Карло.

Стандарты шифрования и дешифрования данных DES и RSA к настоящему времени стали мировыми стандартами в области защиты информации [1]. Алгоритмы этих стандартов, обладающие за счет их высокой стойкости достаточно широким распространением в различных информационных системах (ИС), практически с моментов времени их появления постоянно подвергаются попыткам их «взлома».

В статье предлагается метод их совместного рандомизированного (случайного) использования в разнообразных информационных системах, использующих web-технологии (распределенные АСУ и САПР, технологические и платежные системы и др.), позволяющий повысить их стойкость к информационным атакам «хакеров».

В связи с тем, что интересы «хакера» и Администратора информационной безопасности (ИБ) системы противоположны, предлагается для реализации этого метода использовать математический аппарат теории игр [2, 3] и существующие подходы к получаемым оптимальным стратегиям [3].

Отметим, что предлагаемый подход не рассматривался в основополагающей работе [2] по использованию теоретико-игровых методов в защите информации.

Математическая модель и решение задачи

Рассмотрим игру с нулевой суммой размерности (2×2).

В качестве игроков будем рассматривать Администратора ИБ, который имеет следующие стратегии:

A_1 – применение в ИС модуля, реализующего алгоритм DES;

A_2 – применение в ИС модуля, реализующего алгоритм RSA

и «хакера» со стратегиями:

B_1 – использование аппаратно-программных средств (АПС) «взлома» [1] алгоритма DES;

B_2 – использование АПС «взлома» алгоритма RSA.

Будем считать, что стойкость рассматриваемых алгоритмов оценивается затратами времени T_1 и T_2 на их «взлом».

Считается, что если «хакер» знает о применении в ИС алгоритма DES (стратегия A_1), то он, используя стратегию B_1, затрачивает на ее «взлом» T_1 ед. вр.

Если на стратегию A_1 «хакер» отвечает стратегией B_2, то его затраты времени на «взлом» будут равны $(T_2 + T_1)$ ед. вр. Последнее означает, что, использовав без успеха АПС для «взлома» алгоритма RSA и поняв свою ошибку, «хакер» применяет АПС «взлома» алгоритма DES.

Аналогичным образом представляется взаимодействие в рассматриваемой игре стратегий A_2, B_1 и B_2.

Следуя приведенным выше утверждениям, сформируем платежную матрицу игры [3], представленную в виде табл. 1.

Таблица 1

«Хакер»	Пользователь	
	A_1	A_2
B_1	T_1	$T_1 + T_2$
B_2	$T_2 + T_1$	T_2

Цель игры состоит в том, что Администратор ИБ стремится выбрать стратегию, позволяющую максимизировать затраты времени на «взлом» ИС, а «хакер» – стратегию, минимизирующую такие затраты.

Из табл. 1 видно, что таких единственных (чистых) стратегий у игроков нет, то есть игра не имеет седловой (максиминной) точки для цены игры ν [2, 3].

В теории игр доказано [2, 3], что любая игра с нулевой суммой имеет решение в смешанных стратегиях, когда находящиеся в распоряжении игроков стратегии применяются с некоторыми вероятностями.

Будем описывать такие стратегии для Администратора ИБ с помощью вероятностей p_1 и p_2 применения им стратегий A_1 и A_2.

Для определения значений p_1 и p_2 и неизвестного значения цены игры ν будем решать следующую задачу линейного программирования, сформированную на основе платежной матрицы игры (см. табл. 1):

$$\nu \to \max; \tag{1}$$

$$T_1 p_1 + (T_1 + T_2) p_2 \le \nu; \tag{2}$$

$$(T_2 + T_1)\, p_1 + T_2 p_2 \le \nu; \tag{3}$$

$$p_1 + p_2 = 1; \tag{4}$$

$$0 \le p_1 \le 1, \quad 0 \le p_2 \le 1, \quad \nu \ge 0. \tag{5}$$

В основу этой модели положены соответствующие результаты из раздела по информационной безопасности работы [4].

В связи с малой размерностью сформированной математической модели построим аналитическое решение задачи (1)-(5).

Поскольку максимум целевой функции любой задачи линейного программирования достигается на границе множества допустимых решений [3], перепишем условия (2), (3) в виде равенств:

$$T_1 p_1 + (T_1 + T_2) p_2 = \nu; \tag{6}$$

$$(T_2 + T_1)\, p_1 + T_2 p_2 = \nu. \tag{7}$$

Приравнивая их левые части, имеем:

$$T_1 p_1 + (T_1 + T_2) p_2 = (T_2 + T_1)\, p_1 + T_2 p_2.$$

Преобразуем это выражение следующим образом:

$$p_1(T_1 - T_2 - T_1) = p_2(T_2 - T_1 - T_2).$$

Проводя несложные преобразования, получим равенство вида:

$$p_1 T_2 = p_2 T_1. \tag{8}$$

Искомые переменные p_1 и p_2 должны дополнительно удовлетворять условиям (4) и (5).

Преобразуем равенство (4) к виду:

$$p_2 = 1 - p_1 \tag{9}$$

и с учетом этого перепишем выражение (8) в следующей форме:

$$p_1 T_2 = (1 - p_1) T_1.$$

Разрешая это уравнение относительно переменной p_1, получим первое решение задачи (1)-(5) вида:

$$p_1^0 = \frac{T_1}{T_1 + T_2}. \tag{10}$$

Второе решение формируется с помощью выражений (9) и (10) как:

$$p_2^0 = 1 - \frac{T_1}{T_1 + T_2} = \frac{T_2}{T_1 + T_2}. \tag{11}$$

Из вида выражений (10), (11) следует выполнение ограничений (5).

Полученные оптимальные значения вероятностей практически означают, что в $p_1^0 \cdot 100\%$ случаев должен использоваться алгоритм DES и в $p_2^0 \cdot 100\%$ – алгоритм RSA.

Оптимальное значение цены игры ν^0 может быть получено путем подстановки решений (10), (11) в любое из равенств (6) или (7).

Используя выражение (6), получим:

$$\nu^0 = T_1 \frac{T_1}{T_1 + T_2} + (T_1 + T_2) \frac{T_2}{T_1 + T_2} = \frac{T_1^2 + T_1 T_2 + T_2^2}{T_1 + T_2}. \quad (12)$$

Можно показать, что аналогичный результат получается при использовании формул (7), (10), (11).

Отметим, что величина ν^0 определяет математическое ожидание (среднее значение) затрат времени «хакера» на «взлом» системы, в которой с вероятностями p_1^0 и p_2^0 применяются алгоритмы DES и RSA. При этом значение ν^0 будет больше любой из величин T_1 и T_2.

Общую оценку выигрыша применения предлагаемого подхода к защите данных можно представить как

$$\Delta T = \frac{T_1 + T_2}{\max(T_1, T_2)}. \quad (13)$$

Способы реализации оптимальных смешанных стратегий

Рассмотрим вопросы реализации полученных решений в виде *физической смеси стратегий* A_1 и A_2 [3].

Потребуем, чтобы минимальное значение длины интервала времени действия алгоритмов DES и RSA определялось как:

$$\Delta t < \min(T_1, T_2). \quad (14)$$

Конкретное значение Δt выбирается с четом максимума затрат времени на шифрацию и дешифрацию используемых в ИС данных с помощью этих алгоритмов.

Пусть $[0, \tau]$ – интервал времени, на котором с вероятностями p_1^0 и p_2^0 должна осуществляться смена алгоритмов DES и RSA. Здесь τ – время обмена значительными объемами конфиденциальных данных между абонентами системы и (или) с ее распределенной базой данных.

Потенциальное число таких переключений вычисляется по формуле вида:

$$N = \frac{\tau}{\Delta t}. \quad (15)$$

Сформируем на интервале $[0, \tau]$ сетку моментов времени с шагом, равным Δt:

$$0 < t_1 < t_2 < \ldots < t_{N-1} < t_N,$$

где узлы сетки вычисляются с помощью следующего рекуррентного выражения:

$$t_j = j\Delta t, \; j = \overline{(0, N)}. \quad (16)$$

Количество n_1 и n_2 применений на интервале времени $[0, \tau]$ рассматриваемых алгоритмов можно определить из следующих выражений:

$$n_1 = [Np_1^0]; \; n_2 = [Np_2^0], \quad (17)$$

где $[(\cdot)]$ – операция округления числа $(\cdot)$ до целого значения по «правилу 0,5».

Отметим, что полученные значения должны удовлетворять равенству:

$$n_1 + n_2 = N. \quad (18)$$

Периодичность применения алгоритмов DES и RSA на интервале времени [0, τ] вычислим следующим образом:

$$\Delta\theta_1 = \frac{\tau}{n_1};\ \Delta\theta_2 = \frac{\tau}{n_2}. \tag{19}$$

Определим максимальное значение из этих величин:

$$\Delta\vartheta = \max(\Delta\theta_1, \Delta\theta_2). \tag{20}$$

Сформируем график применения алгоритмов DES и RSA на интервале времени [0, τ].

При $\Delta\vartheta = \Delta\theta_1$, которая является кратной величине Δt, алгоритм DES включается в моменты времени, определяемые из рекуррентного выражения вида:

$$t_j^{(1)} = t_{j-1}^{(1)} + \Delta\theta_1,\ j = (\overline{1, n_1}), \tag{21}$$

где $t_0^{(1)} = 0$.

Во все оставшиеся моменты времени сетки, которые определяются как:

$$t_0^{(2)} = 0,\ t_j^{(2)} = t_{j-1}^{(2)} + \Delta t,\ t_j^{(2)} \neq t_j^{(1)},\ j = (\overline{1, N}) \tag{22}$$

включается алгоритм RSA.

Формулы, аналогичные выражениям (20), (21), можно записать для случая, когда $\Delta\vartheta = \Delta\theta_2$.

При значении $\Delta\vartheta = \Delta\theta_1 = \Delta\theta_2$, кратном Δt, выражение (20) можно применить к любому из алгоритмов DES или RSA.

Если величина $\Delta\vartheta$ не является кратной шагу сетки Δt, то проводится корректировка периодичности применения соответствующего алгоритма. Для этой цели на сетке рассматриваются интервалы времени $[t_{j-1}, t_j]$, $j = (\overline{1, N})$ и из их состава выделяется интервал $[t_{k-1}, t_k]$, для которого выполняется неравенство:

$$t_{k-1} < \Delta\vartheta < t_k,\ k = (\overline{1, N}). \tag{23}$$

В этом случае в выражении (21) полагаем $\Delta\vartheta = t_{k-1}$.

Рассмотрим примеры, иллюстрирующие применение физической смеси стратегий (10) и (11) использования алгоритмов DES и RSA.

Пример 1.

Пусть на основе сайтов, посвященных вопросам стойкости алгоритмов DES и RSA, получены следующие оценки.

«Взлом» алгоритма DES с помощью компьютерной сети может быть осуществлен за 22 часа. Теоретически «взлом» этого алгоритма возможен за 6 мин на ЭВМ стоимостью 10 млн. дол.

«Взлом» алгоритма RSA при использовании 40-битного кода защиты с помощью офисного компьютера был осуществлен за 13 дней. При использовании процессора P5/100 с интерпретатором be и ОС FreeBSD затраты времени на «взлом» этого алгоритма были равны 20-25 мин. Из приведенных данных выберем их минимальные значения:

$$T_1 = 6 \text{ мин};\quad T_2 = 20 \text{ мин}.$$

Тогда, используя формулы (10)-(12), имеем:

$$p_1^0 = \frac{6}{6+20} = 0,231;\ p_2^0 = \frac{20}{6+20} = 0,769;\ \nu^0 = \frac{6^2 + 6\cdot 20 + 20^2}{6+20} = 21,38 \text{ мин}.$$

Выигрыш от применения предлагаемого подхода, согласно формуле (13), будет равен:

$$\Delta T = \frac{6+20}{\max(6,\ 20)} = 1,3 \text{ раза}.$$

Выберем, согласно условию (14), величину Δt следующим образом:

$$\Delta t = 5 \text{ мин.} < \min(6, 20).$$

Это означает, что в течение 5 минут действующий алгоритм DES не может быть «взломан», а по истечении этого времени осуществляется переключение на алгоритм RSA.

В качестве интервала времени [0, τ], на котором должна производиться смена действующих в системе алгоритмов DES и RSA, выберем условный интервал [0, 60] мин.

Число таких смен (переключений), вычисленное по формуле (15), будет равно:

$$N = \frac{60}{5} = 12.$$

Сетка значений времени, вычисленная по формуле (16), приведена в табл. 2.

Таблица 2

j	1	2	3	4	5	6	7	8	9	10	11	12
t, мин	0	5	10	15	20	25	30	35	40	45	50	55

Используя выражения (17) и вычисленные выше значения вероятностей p_1^0 и p_2^0, имеем:

$$n_1 = [12 \cdot 0{,}231] = [2{,}772] = 3; \quad n_2 = [12 \cdot 0{,}772] = [9{,}264] = 9.$$

Отметим, что для найденных значений условие (18) выполняется.

Периодичности применения в течение часа алгоритмов DES и RSA (см. формулы (19)) будут равны:

$$\Delta\theta_1 = \frac{60}{3} = 20 \text{ мин}; \quad \Delta\theta_2 = \frac{60}{9} = 6{,}666 \text{ мин}.$$

Максимум $\Delta\vartheta$ из этих величин, определенных из выражения (20), соответствует значению $\Delta\theta_1 = 20$ мин, которое является кратным значению $\Delta t = 5$ мин.

Применяя соотношение (21), получаем текущие моменты времени $t_j^{(1)}$, $j = (\overline{1,3})$, в которые начинает действовать алгоритм DES:

$$t_1^{(1)} = 0 + 20 = 20 \text{ мин}; \quad t_2^{(1)} = 20 + 20 = 40 \text{ мин}; \quad t_3^{(1)} = 40 + 20 = 60 \text{ мин}.$$

Оставшиеся моменты времени $t_j^{(2)}$, $j = (\overline{0,9})$, в которые включается алгоритм RSA, с использованием выражения (22) конкретизируются как:

$$t_0^{(2)} = 0 \text{ мин}; \quad t_1^{(2)} = 0 + 5 = 5 \text{ мин}; \quad t_2^{(2)} = 5 + 5 = 10 \text{ мин}; \quad t_3^{(3)} = 10 + 5 = 15 \text{ мин};$$
$$t_4^{(2)} = 20 + 5 = 25 \text{ мин}; \quad t_5^{(2)} = 25 + 5 = 30 \text{ мин}; \quad t_6^{(2)} = 30 + 5 = 35 \text{ мин};$$
$$t_7^{(2)} = 40 + 5 = 45 \text{ мин}; \quad t_8^{(2)} = 45 + 5 = 50 \text{ мин}; \quad t_9^{(2)} = 50 + 5 = 55 \text{ мин}.$$

Здесь учтено, что на интервалах времени [15, 20] мин., [35, 40] мин., [55, 60] мин. действует алгоритм DES.

График включения в работу алгоритмов DES и RSA приведен в табл. 3.

Таблица 3

t, мин	0	5	10	15	20	25	30	35	40	45	50	55
Алгоритм	RSA	RSA	RSA	DES	RSA	RSA	RSA	DES	RSA	RSA	RSA	DES

Из этой таблицы следует, что время применения в системе алгоритма RSA всегда меньше величины $T_2 = 20$ мин. его «взлома».

Сформируем оценку $\overline{\nu}$ величины средних затрат времени на «взлом» действующих в системе алгоритмов при использовании предлагаемого подхода:

$$\overline{\nu} = \frac{n_1}{N} T_1 + \frac{n_2}{N}(T_1 + T_2) = \frac{3}{12} \cdot 6 + \frac{9}{12} \cdot 26 = 21 \text{ мин}.$$

Эта величина отличается от значения ν^0 на 0,38 мин., что говорит о практическом их совпадении.

Пример 2.

Известно, что для повышения стойкости данных осуществляется тройное применение алгоритма DES (**3DES**) [1].

Будем считать, что в этом случае величина $T_1 = 3 \times 6 = 18$ мин.

Применяя для введенного выше условного интервала времени $[0, \tau] = [0, 60]$ мин. отмеченные в Примере 1 формулы, получаем следующие результаты:

$$p_1^0 = \frac{18}{18+20} = 0,474;\ p_2^0 = \frac{20}{18+20} = 0,526;\ \nu = \frac{18^2 + 18 \cdot 20 + 20^2}{18+20} = 28,53 \text{ мин};$$

$$\Delta T = \frac{18+20}{\max(18,\ 20)} = 1,9 \text{ раза};\ \Delta t = 15 < \min(18,\ 20);$$

$$N = \frac{60}{15} = 4;\ n_1 = [4 \cdot 0,474] = [1,88] = 2;\ n_2 = [4 \cdot 0,526] = [2,12] = 2;$$

$$\Delta\theta_1 = \Delta\theta_2 = \frac{60}{2} = 30 \text{ мин.} = \Delta\vartheta.$$

Отметим, что полученное $\Delta\vartheta$ является кратным значению шага сетки Δt = 15 мин.

График включения в течение одного часа алгоритмов 3DES и RSA представлен в табл. 4.

Таблица 4

t, мин.	0	15	30	45
Алгоритм	3DES	RSA	3DES	RSA

Из таблицы видно, что интервалы времени действия алгоритмов 3DES и RSA меньше величин T_1 = 18 мин. и T_2 = 20 мин. их «взлома».

Пусть выбрана величина шага сетки Δt = 12 мин.

В этом случае N = 5 и узлы сетки согласно выражению (16) будут иметь следующие значения:

$$t_1 = 12 \text{ мин.};\ t_2 = 24 \text{ мин.};\ t_3 = 36 \text{ мин.};\ t_4 = 48 \text{ мин.};\ t_5 = 60 \text{ мин.}$$

Значения n_1 и n_2 будут равны:

$$n_1 = [5 \cdot 0,474] = [2,37] = 2;\quad n_2 = [5 \cdot 0,526] = [2,63] = 3.$$

Периодичности применения алгоритмов 3DES и RSA вычисляются как:

$$\Delta\theta_1 = \frac{60}{2} = 30 \text{ мин.} = \Delta\vartheta;\ \Delta\theta_2 = \frac{60}{3} = 20 \text{ мин.}$$

Величина $\Delta\vartheta$ не является кратной величине шага сетки Δt, то есть частное от деления первой на вторую не является целым числом.

Найдем на сетке значения времени $t_j,\ j = \overline{(1,5)}$ интервал, содержащий величину $\Delta\vartheta$ = 30 мин. Границы такого интервала согласно условию (23) определяются значениями t_2 = 24 мин. и t_3 = 36 мин. Тогда при формировании моментов времени применения алгоритма 3DES в выражении (21) величина $\Delta\vartheta$ полагается равной 24 мин. График применения рассматриваемых алгоритмов представлен в табл. 5.

Таблица 5

t, мин.	0	12	24	36	48
Алгоритм	3DES	RSA	3DES	RSA	3DES

Из этой таблицы также следует, что интервалы действия алгоритмов не превышают времени их «взлома».

Рассмотрим *применение метода Монте-Карло*, описанного в работе [3], для реализации оптимальных смешанных стратегий (10), (11). Этот метод позволяет сформировать последовательность случайных (рандомизированных) реализаций алгоритмов шифрования и дешифрования, заданных значениями вероятностей их наступления в любой момент времени функционирования ИС.

В качестве случайных событий будем рассматривать следующие события: A_1^0 – применение алгоритма DES; A_2^0 – применение алгоритма RSA.

Как было отмечено выше, вероятности p_1^0 и p_2^0 их наступления определяются из выражений (10) и (11).

Суть метода Монте-Карло состоит в генерации равномерно распределенного в интервале (0, 1) случайного числа ξ и проверке условия вида:

$$0 < \xi \le p_1^0 . \tag{24}$$

При выполнении этого условия считается, что наступило случайное событие A_1^0.

Если число ξ таково, что выполнятся неравенство:

$$p_1^0 < \xi \le 1, \tag{25}$$

то предполагается наступление события A_2^0.

Для практической реализации этого подхода будем использовать бесконечную временную сетку функционирования ИС с шагом Δt, удовлетворяющим условию (14). Узлы этой сетки t_1, t_2, t_3,…, t_{j-1}, t_j,… при $t_0 = 0$ вычисляются по формуле (16).

На введенной сетке выделим интервалы времени (t_{j-1}, t_j), $j = 1, 2, 3,\ldots$, на которых должны в соответствии с вероятностями p_1^0 и p_2^0 использоваться алгоритмы DES или RSA.

Пусть в момент времени t_{j-1} с помощью датчика случайных чисел (ДСЧ) получено число $\xi_{j-1} \in (0, 1)$, $j = 1, 2, 3,\ldots$

Значения ξ_{j-1} и p_1^0 используются при проверке условий (24) и (25).

Если выполняется условие (24), то на интервале времени (t_{j-1}, t_j) должен функционировать алгоритм DES, в противном случае, когда выполняется условие (25) на этом интервале времени должен функционировать алгоритм RSA.

При этом суммарное время непрерывной работы каждого алгоритма не должно превышать времени его «взлома». Для этого вычисляется максимальное количество k_i следующих подряд интервалов времени Δt, в которых возможно применение одного и того же алгоритма, невзирая на условия (24) и (25):

$$k_i = \begin{cases} \text{entiar}(T_i / \Delta t), & \text{если } (T_i / \Delta t) - \text{entiar}(T_i / \Delta t) > 0; \\ \text{entiar}(T_i / \Delta t) - 1, & \text{если } (T_i / \Delta t) - \text{entiar}(T_i / \Delta t) = 0, \end{cases} \quad i = 1,\ 2. \tag{26}$$

Здесь функция entiar(x) выполняет выделение целой части числа x.

Для фиксирования следующих подряд интервалов времени Δt, в которых осуществлялось применение одного и того же алгоритма, используется счетчик таких интервалов m_i, $i = 1$ или 2.

В каждый момент времени t_{j-1} проверяется условие: $m_i < k_i$, $i = 1$ или 2.

Если это неравенство выполняется, то на интервале (t_{j-1}, t_j) применяется ранее используемый алгоритм, к счетчику m_i прибавляется единица. В противном случае в момент времени t_{j-1} происходит смена алгоритма, и соответствующий счетчик m_i обнуляется.

Применение предложенного подхода проиллюстрируем следующим примером.

Пример 3. В этом примере используются исходные данные и результаты Примеров 1 и 2 при различных вариантах случайных чисел.

Результаты вычисленных экспериментов для различных исходных данных приведены в табл. 6 ($p_1^0 = 0,23$; $p_2^0 = 0,77$; $T_1 = 6$; $T_2 = 20$; $\Delta t = 5$; $k_1 = 1$; $k_2 = 3$), табл. 7 ($p_1^0 = 0,474$; $p_2^0 = 0,526$; $T_1 = 18$; $T_2 = 20$; $\Delta t = 15$; $k_1 = 1$; $k_2 = 1$), табл. 8 ($p_1^0 = 0,474$; $p_2^0 = 0,526$; $T_1 = 18$; $T_2 = 20$; $\Delta t = 12$; $k_1 = 1$; $k_2 = 1$).

Таблица 6

Интервалы времени	Вариант 1		Вариант 2		Вариант 3	
	Случ. число	Алгоритм	Случ. число	Алгоритм	Случ. число	Алгоритм
0-5	0,0029	DES	0,1671	DES	0,3284	RSA
5-10	0,6429	RSA	0,028	RSA	0,4173	RSA
10-15	0,9338	RSA	0,3949	RSA	0,0364	DES
15-20	0,1405	DES	0,9034	RSA	0,3722	RSA
20-25	0,6622	RSA	0,8739	DES	0,9204	RSA
25-30	0,1362	DES	0,6188	RSA	0,6953	RSA
30-35	0,3942	RSA	0,9096	RSA	0,6959	DES
35-40	0,2981	RSA	0,5567	RSA	0,1718	RSA
40-45	0,9204	RSA	0,8998	DES	0,0047	DES

Окончание табл. 6

Интервалы времени	Вариант 1		Вариант 2		Вариант 3	
	Случ. число	Алгоритм	Случ. число	Алгоритм	Случ. число	Алгоритм
45-50	0,3101	DES	0,9185	RSA	0,707	RSA
50-55	0,7419	RSA	0,2381	RSA	0,6574	RSA
55-60	0,0584	DES	0,8348	RSA	0,1148	DES
60-65	0,5207	RSA	0,1898	DES	0,7552	RSA
65-70	0,5858	RSA	0,9353	RSA	0,5414	RSA
70-75	0,5589	RSA	0,071	DES	0,6091	RSA
75-80	0,1796	DES	0,2081	RSA	0,0956	DES
80-85	0,8049	RSA	0,4425	RSA	0,4002	RSA
85-90	0,9445	RSA	0,3555	RSA	0,3443	RSA
90-95	0,1234	DES	0,5159	DES	0,3872	RSA
95-100	0,9489	RSA	0,2824	RSA	0,4874	DES
100-105	0,3313	RSA	0,8596	RSA	0,2049	RSA
105-110	0,312	RSA	0,1833	DES	0,6877	RSA
110-115	0,192	DES	0,7897	RSA	0,6786	RSA
115-120	0,2622	RSA	0,9232	RSA	0,2279	DES

Таблица 7

Интервалы времени	Вариант 1		Вариант 2		Вариант 3	
	Случ. число	Алгоритм	Случ. число	Алгоритм	Случ. число	Алгоритм
0-15	0,5296	RSA	0,517	RSA	0,2085	DES
15-30	0,2771	DES	0,3579	DES	0,1637	RSA
30-45	0,8499	RSA	0,7126	RSA	0,6433	DES
45-60	0,0726	DES	0,5946	DES	0,9608	RSA
60-75	0,6542	RSA	0,4412	RSA	0,1768	DES
75-90	0,3204	DES	0,2781	DES	0,5347	RSA
90-105	0,9154	RSA	0,11	RSA	0,7989	DES
105-120	0,7891	DES	0,5332	DES	0,8646	RSA

Таблица 8

Интервалы времени	Вариант 1		Вариант 2		Вариант 3	
	Случ. число	Алгоритм	Случ. число	Алгоритм	Случ. число	Алгоритм
0-12	0,4667	DES	0,3732	DES	0,7657	RSA
12-24	0,0444	RSA	0,6533	RSA	0,9986	DES
24-36	0,9374	DES	0,6187	DES	0,1421	RSA
36-48	0,6268	RSA	0,5097	RSA	0,1802	DES
48-60	0,4226	DES	0,3887	DES	0,0359	RSA
60-72	0,4292	RSA	0,3391	RSA	0,6578	DES
72-84	0,6556	DES	0,1039	DES	0,8364	RSA
84-96	0,0832	RSA	0,9947	RSA	0,7226	DES
96-108	0,582	DES	0,7994	DES	0,63	RSA
108-120	0,5737	RSA	0,5893	RSA	0,7937	DES

Заключение

При практической реализации предложенного метода в зашифрованных файлах данных должен указываться номер примененного алгоритма. Первым этапом при дешифрации файлов является выделение этого номера и активизация соответствующего программного модуля.

Данный метод при его развитии может быть обобщен на случай применения в защищаемой системе более двух известных в настоящее время алгоритмов шифрования и дешифрования данных [1], что, несомненно, приведет к повышению ее информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. *Шнайдер Б.* Прикладная криптография. Протоколы, алгоритмы и программы на языке С. М.: Триумф, 2012. 611 с.
2. *Гуц А.К., Вахний Т.В.* Теория игр и защита компьютерных систем. Омск: Изд-во ОМГУ, 2013. 160 с.
3. *Вентцель Е.С.* Исследование операций. М.: Сов. радио, 1972. 632 с.
4. *Моисеев В.С.* Основы теории эффективного применения беспилотных летательных аппаратов. Казань: «Школа», 2015. 444 с. (Серия «Современная прикладная математика и информатика»).

Поступила в редколлегию 19. 11. 15

GAME-THEORETIC METHOD OF ENCRYPTING AND DECRYPTING DATA WITH RANDOMIZED APPLICATION OF DES AND RSA ALGORITHMS

V. Moiseev, L. Moiseeva

To improve information security is offered an original approach to randomized application in information systems widely used DES and RSA algorithms of encryption and decryption.

Keywords: a mathematical model of the game, the decision of the game, a physical mixture of strategies, Monte Carlo method.

Моисеев Виктор Сергеевич – д-р техн. наук (КНИТУ-КАИ, Казань)
E-mail: em131@yandex.ru

Моисеева Лия Тагирджановна – канд. техн. наук (КНИТУ-КАИ, Казань)
E-mail: em131@yandex.ru