

## ОЦЕНКА АСИММЕТРИЧНЫХ МЕТОДОВ ШИФРОВАНИЯ В СИСТЕМАХ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

**Цель работы.** Изучить принципы работы асимметричных алгоритмов криптографического преобразования информации и оценить их эффективность.

### Краткие сведения из теории

#### Асимметричные криптосистемы

**Криптосистема шифрования данных RSA.** Алгоритм RSA предложили в 1978 г. три автора: Р. Райвест (Rivest), А. Шамир (Shamir) и А. Адлеман (Adleman). Алгоритм получил свое название по первым буквам фамилий его авторов.

Надежность алгоритма основывается на трудности факторизации больших чисел в произведение простых множителей. В криптосистеме RSA открытый ключ  $K_b$ , секретный ключ  $k_b$ , сообщение  $M$  и криптограмма  $C$  принадлежат множеству целых чисел  $Z_N = \{0, 1, 2, \dots, N-1\}$ , где  $N$  – модуль  $N = PQ$ . Здесь  $P$  и  $Q$  – случайные большие простые числа. Для обеспечения максимальной безопасности выбирают  $P$  и  $Q$  равной длины и хранят в секрете. Множество  $Z_N$  с операциями сложения и умножения по модулю  $N$  образует арифметику по модулю  $N$ . Открытый ключ  $K_b$  выбирают случайным образом так, чтобы выполнялись условия:  $1 < K_b \leq \varphi(N)$ ,  $\text{НОД}(K_b, \varphi(N)) = 1$ ,  $\varphi(N) = (P-1)(Q-1)$ , где  $\varphi(N)$  – функция Эйлера. Второе из указанных выше условий означает, что открытый ключ  $K_b$  и значение функции Эйлера  $\varphi(N)$  должны быть взаимно простыми. Далее, используя расширенный алгоритм Евклида, вычисляют секретный ключ  $k_b$ , такой, что

$$k_b K_b \equiv 1 \pmod{\varphi(N)} \text{ или } k_b = K_b^{-1} \pmod{(P-1)(Q-1)}. \quad (1)$$

Это можно осуществить, так как при известной паре простых чисел  $(P, Q)$  можно легко найти  $\varphi(N)$ . Заметим, что  $k_b$  и  $N$  должны быть взаимно простыми. Открытый ключ  $K_b$  используют для шифрования данных, а секретный ключ  $k_b$  – для расшифрования.

Преобразование шифрования определяет криптограмму  $C$  через пару «открытый ключ  $K_b$ , сообщение  $M$ » в соответствии со следующей формулой:

$$C = E_{K_b}(M) = E_b(M) = M^{K_b} \pmod{N}. \quad (2)$$

В качестве алгоритма быстрого вычисления значения  $C$  используют ряд последовательных возведений в квадрат целого  $M$  и умножений на  $M$  с приведением по модулю  $N$ .

Обращение функции  $C = M^{K_a} \pmod{N}$ , т. е. определение значения  $M$  по известным значениям  $C$ ,  $K_b$  и  $N$ , практически не осуществимо при  $N \approx 2^{512}$ . Однако обратную задачу, т. е. задачу расшифрования криптограммы  $C$ , можно решить, используя пару «секретный ключ  $k_b$ , криптограмма  $C$ » по следующей формуле:

$$M = D_{K_b}(C) = D_b(C) = C^{k_b} \pmod{N}. \quad (3)$$

Подставляя в это уравнение значение  $C$ , получаем

$$\left(M^{K_a}\right)^{k_b} = M \pmod{N} \text{ или } M^{K_a k_b} = M \pmod{N}. \quad (4)$$

Сопоставляя это выражение с формулой расшифрования, получаем  $K_b k_b = n \varphi(N) + 1$  или, что то же самое,  $K_b k_b \equiv 1 \pmod{\varphi(N)}$ .

Следовательно, если криптограмму  $C = M^{K_a} \pmod{N}$  возвести в степень  $k_b$ , то в результате восстанавливается исходный открытый текст  $M$ , так как

$$\left(M^{K_a}\right)^{k_b} = M^{K_a k_b} = M^{n\varphi(N)+1} \equiv M \pmod{N}. \quad (5)$$

Таким образом, получатель, который создает криптосистему, защищает два параметра: 1) секретный ключ  $k_b$  и 2) пару чисел  $(P, Q)$ , произведение которых дает значение модуля  $N$ . С другой стороны, отправителю известны значения модуля  $N$  и открытого ключа  $K_b$ . Противнику известны лишь значения  $K_b$  и  $N$ . Если бы он смог разложить число  $N$  на множители  $P$  и  $Q$ , то он узнал бы тройку чисел  $\{P, Q, K_b\}$ , вычислил бы значение функции Эйлера  $\varphi(N) = (P-1)(Q-1)$  и определил значение секретного ключа  $k_b$ .

Однако, как уже отмечалось, разложение очень большого  $N$  на множители вычислительно не осуществимо (при условии, что длины выбранных  $P$  и  $Q$  составляют не менее 100 десятичных знаков).

Предположим, что пользователь  $A$  хочет передать пользователю  $B$  сообщение в зашифрованном виде, используя криптосистему RSA. В таком случае пользователь  $A$  выступает в роли отправителя сообщения, а пользователь  $B$  – в роли получателя. Криптосистему RSA должен сформировать получатель сообщения, т. е. пользователь  $B$ . Рассмотрим последовательность действий пользователей  $B$  и  $A$  при передаче сообщения «ГБВ» и при использовании небольших чисел для простоты вычислений, хотя на практике применяются очень большие числа.

1 Пользователь  $B$  выбирает два произвольных простых числа  $P$  и  $Q$ :  $P = 3$  и  $Q = 11$ .

2 Пользователь  $B$  вычисляет значение модуля  $N = PQ$ :  $N = 3 \cdot 11 = 33$ .

3 Пользователь  $B$  вычисляет значение функции Эйлера  $\varphi(N) = (P - 1)(Q - 1)$  и выбирает случайным образом значение открытого ключа  $K_B$  с учетом выполнения условий:  $1 < K_B \leq \varphi(N)$ ,  $\text{НОД}(K_B, \varphi(N)) = 1$ .

$$\varphi(N) = \varphi(33) = (P - 1)(Q - 1) = 2 \cdot 10 = 20; K_B = 7.$$

4 Пользователь  $B$  вычисляет значение секретного ключа  $k_B$ , используя расширенный алгоритм Евклида при решении  $k_B \equiv K_B^{-1} \pmod{\varphi(N)}$ .  $k_B \equiv 7^{-1} \pmod{20}$ . Решение дает  $k_B = 3$ .

5 Пользователь  $B$  пересылает пользователю  $A$  пару чисел  $(N, K_B)$  по незащищенному каналу.

6 Пользователь  $A$  разбивает исходный открытый текст  $M$  на блоки, каждый из которых может быть представлен в виде числа  $M_i = 0, 1, 2, \dots, N - 1$ . Для этого он представляет шифруемое сообщение «ГБВ» как последовательность целых чисел в диапазоне от 0 до 32. Например, пусть буква Б представляется как число 1, буква В – как число 2, буква Г – как число 3. Тогда сообщение «ГБВ» можно представить как последовательность чисел 312, т. е.  $M_1 = 3, M_2 = 1, M_3 = 2$ .

7 Пользователь  $A$  шифрует текст, представленный в виде последовательности чисел  $M_i$ , по формуле  $C_i = M_i^{K_B} \pmod{N}$ :

$$\begin{aligned} C_1 &= 3^7 \pmod{33} = 2187 \pmod{33} = 9, \\ C_2 &= 1^7 \pmod{33} = 1 \pmod{33} = 1, \\ C_3 &= 2^7 \pmod{33} = 128 \pmod{33} = 29, \end{aligned}$$

и отправляет криптограмму  $C_1, C_2, C_3, \dots, C_i$  пользователю  $B$ .  $C_1, C_2, C_3 = 9, 1, 29$ .

8 Пользователь  $B$  расшифровывает принятую криптограмму  $C_1, C_2, C_3, \dots, C_i$ , используя секретный ключ  $k_B$ , по формуле  $M_i = C_i^{k_B} \pmod{N}$ :

$$\begin{aligned} M_1 &= 9^3 \pmod{33} = 729 \pmod{33} = 3, \\ M_2 &= 1^3 \pmod{33} = 1 \pmod{33} = 1, \\ M_3 &= 29^3 \pmod{33} = 24389 \pmod{33} = 2. \end{aligned}$$

В результате будет получена последовательность чисел  $M_i$ , которые представляют собой исходное сообщение  $M$ . Таким образом, восстановлено исходное сообщение: «ГБВ».

Чтобы алгоритм RSA имел практическую ценность, необходимо иметь возможность без существенных затрат генерировать большие простые числа, уметь оперативно вычислять значения ключей  $K_B$  и  $k_B$ .

Криптосистемы RSA реализуются как аппаратным, так и программным путем. Для аппаратной реализации операций шифрования и расшифрования

RSA разработаны специальные процессоры. Эти процессоры, реализованные на сверхбольших интегральных схемах (СБИС), позволяют выполнять операции RSA, связанные с возведением больших чисел в колоссально большую степень по модулю  $N$ , за относительно короткое время. Аппаратная реализация RSA примерно в 1000 раз медленнее аппаратной реализации симметричного криптоалгоритма DES. Программная реализация RSA примерно в 100 раз медленнее программной реализации DES. С развитием технологии эти оценки могут несколько изменяться, но асимметричная криптосистема RSA никогда не достигнет быстродействия симметричных криптосистем. Малое быстродействие криптосистем RSA ограничивает область их применения, но не уменьшает их ценность.

**Схема шифрования Эль Гамала.** Схема Эль Гамала, предложенная в 1985 г., может быть использована как для шифрования, так и для цифровых подписей. Безопасность схемы Эль Гамала обусловлена сложностью вычисления дискретных логарифмов в конечном поле.

Для того чтобы генерировать пару ключей (открытый ключ – секретный ключ), сначала выбирают некоторое большое простое число  $P$  и большое целое число  $G$ , причем  $G < P$ . Числа  $P$  и  $G$  могут быть распространены среди группы пользователей. Затем выбирают ключ  $X$  – случайное целое число, причем  $X < P$ . Число  $X$  является секретным ключом и должно храниться в секрете. Далее вычисляют  $Y = G^X \bmod P$ . Число  $Y$  является открытым ключом.

Для того чтобы зашифровать сообщение  $M$ , выбирают случайное целое число  $1 < K < P - 1$ , такое, что числа  $K$  и  $(P - 1)$  являются взаимно простыми. Затем вычисляют числа  $a = G^K \bmod P$ ,  $b = Y^K M \bmod P$ . Пара чисел  $(a, b)$  является шифротекстом. Длина шифротекста вдвое больше длины исходного открытого текста  $M$ .

Для того чтобы расшифровать шифротекст  $(a, b)$ , вычисляют

$$M = b/a^X \bmod P. \quad (6)$$

Для примера выберем  $P = 11$ ,  $G = 2$ , секретный ключ  $X = 8$ .

Вычисляем  $Y = G^X \bmod P = 2^8 \bmod 11 = 256 \bmod 11 = 3$ . Открытый ключ  $Y = 3$ .

Пусть сообщение  $M = 5$ . Выберем некоторое случайное число  $K = 9$ . Убедимся, что  $\text{НОД}(K, P - 1) = 1$ .  $\text{НОД}(9, 10) = 1$ . Вычисляем пару чисел  $a$  и  $b$ :  $a = G^K \bmod P = 2^9 \bmod 11 = 512 \bmod 11 = 6$ ;  $b = Y^K M \bmod P = 3^9 \cdot 5 \bmod 11 = 19683 \cdot 5 \bmod 11 = 9$ . Получим шифротекст  $(a, b) = (6, 9)$ .

Выполним расшифрование этого шифротекста. Вычисляем сообщение  $M$ , используя секретный ключ  $X$ :  $M = b/a^X \bmod P = 9/6^8 \bmod 11$ . Выражение  $M = 9/6^8 \bmod 11$  можно представить в виде  $6^8 \cdot M \equiv 9 \bmod 11$  или  $1679616 \times M \equiv 9 \bmod 11$ . В результате находим  $M = 5$ .

В реальных схемах шифрования необходимо использовать в качестве

модуля  $P$  большое целое простое число, имеющее в двоичном представлении длину от 512 до 1024 бит.

**Комбинированный метод шифрования.** Главным достоинством криптосистем с открытым ключом является их потенциально высокая безопасность: нет необходимости ни передавать, ни сообщать кому бы то ни было значения секретных ключей, ни убеждаться в их подлинности. В симметричных криптосистемах существует опасность раскрытия секретного ключа во время передачи. Однако алгоритмы, лежащие в основе криптосистем с открытым ключом, имеют следующие недостатки:

– генерация новых секретных и открытых ключей основана на генерации новых больших простых чисел, а проверка простоты чисел занимает много процессорного времени;

– процедуры шифрования и расшифрования, связанные с возведением в степень многозначного числа, достаточно громоздки.

Именно поэтому быстродействие криптосистем с открытым ключом обычно в сотни и более раз меньше быстродействия симметричных криптосистем с секретным ключом.

Комбинированный (гибридный) метод шифрования позволяет сочетать преимущества высокой секретности, присущие асимметричным криптосистемам с открытым ключом, с преимуществами высокой скорости работы, присущими симметричным криптосистемам с секретным ключом. При таком подходе криптосистема с открытым ключом применяется для шифрования, передачи и последующего расшифрования только секретного ключа симметричной криптосистемы. А симметричная криптосистема применяется для шифрования и передачи исходного открытого текста. В результате криптосистема с открытым ключом не заменяет симметричную криптосистему с секретным ключом, а лишь дополняет ее, позволяя повысить в целом защищенность передаваемой информации. Такой подход иногда называют схемой электронного цифрового конверта.

Если пользователь  $A$  хочет передать зашифрованное комбинированным методом сообщение  $M$  пользователю  $B$ , то порядок его действий будет таков:

1 Создать (например, сгенерировать случайным образом) симметричный ключ, называемый в этом методе сеансовым ключом  $K_c$ .

2 Зашифровать сообщение  $M$  на сеансовом ключе  $K_c$ .

3 Зашифровать сеансовый ключ  $K_c$  на открытом ключе  $K_a$  пользователя  $B$ .

4 Передать по открытому каналу связи в адрес пользователя  $B$  зашифрованное сообщение вместе с зашифрованным сеансовым ключом.

Действия пользователя  $B$  при получении зашифрованного сообщения и зашифрованного сеансового ключа должны быть обратными:

5 Расшифровать на своем секретном ключе  $k_b$  сеансовый ключ  $K_c$ .

6 С помощью полученного сеансового ключа  $K_c$  расшифровать и прочи-

тат сообщение  $M$ .

При использовании комбинированного метода шифрования можно быть уверенным в том, что только пользователь В сможет правильно расшифровать ключ  $K_c$  и прочитать сообщение  $M$ .

Комбинированный метод шифрования является наиболее рациональным, объединяя в себе высокое быстродействие симметричного шифрования и высокую криптостойкость, гарантируемую системами с открытым ключом.

### Порядок выполнения работы

1 Изучить краткие сведения из теории.

2 По последней цифре шифра из таблицы 1 необходимо выбрать сообщение, которое будут подвергаться шифрованию.

Таблица 1 – Исходные сообщения

Параметр	Последняя цифра шифра				
	1	2	3	4	5
$M_4$	3 0 7 9 11 2	7 12 1 0 3 2	9 1 3 17 2 6	13 3 2 7 1 4	6 2 12 9 1 3
Параметр	Последняя цифра шифра				
	6	7	8	9	0
$M_4$	7 3 8 9 10 2	19 9 8 1 0 6	9 3 0 8 1 12	7 8 9 15 1 5	6 1 0 16 5 9

3 По предпоследней цифре шифра из таблицы 2 необходимо выбрать ключи шифрования.

4 По первой цифре шифра из таблицы 3 необходимо выбрать параметры шифрования.

Таблица 2 – Ключи шифрования

Параметр	Предпоследняя цифра шифра									
	1	2	3	4	5	6	7	8	9	0
$X_1$	9	7	5	12	8	9	7	8	13	7

9 Зашифровать сообщение  $M_4$  с использованием асимметричной схемы шифрования:

- RSA с параметрами  $P_1, Q_1$ .
- Эль Гамалья с параметрами  $P_2, G_1, X_1, K_6$ .

Таблица 3 – Параметры алгоритмов шифрования

Параметр	Первая цифра шифра									
	1	2	3	4	5	6	7	8	9	0
$P_1$	4	5	7	9	11	13	15	16	12	6
$Q_1$	13	16	12	10	8	7	8	3	5	11
$P_2$	14	15	16	17	18	19	20	21	22	23
$G_1$	2	4	6	8	10	12	11	9	7	5
$K_6$	12	9	7	15	10	11	9	11	8	13

## **Содержание отчета**

- 1 Цель работы.
- 2 Исходные данные.
- 3 Результаты расчетов.
- 4 Вывод по работе.

## **Контрольные вопросы**

- 1 Дайте понятие криптографии.
- 2 Что относится к криптографическим методам защиты информации?
- 3 В чем принцип асимметричных методов шифрования?
- 4 Почему асимметричные методы шифрования называются криптосистемами с открытым ключом?
- 5 Алгоритм RSA.
- 6 Алгоритм Эль Гамала.