Работа 9

КРИПТОСИСТЕМА С ОТКРЫТЫМ КЛЮЧОМ (АЛГОРИТМ RSA)

Пусть абоненты A и B решили организовать для себя возможность секретной переписки. Для этого каждый из них независимо выбирает два больших простых числа (p_{A_1}, p_{A_2} и p_{B_1}, p_{B_2}), находит их произведение (r_A и r_B), функцию Эйлера от этого произведения ($\varphi(r_A)$ и $\varphi(r_B)$) и случайное число (a и b), меньшее вычисленного значения функции Эйлера и взаимно простое с ним. Кроме того, A из уравнения $a\alpha \equiv 1 \pmod{\varphi(r_A)}$ находит α $(0 < \alpha < \varphi(r_A))$, а B из уравнения $b\beta \equiv 1 \pmod{\varphi(r_B)}$ находит β $(0 < \beta < \varphi(r_B))$. Затем A и B печатают доступную всем книгу паролей вида:

$$\boxed{\begin{array}{l} A\colon\ r_A, a \\ B\colon\ r_B, b \end{array}}.$$

Теперь кто-угодно может отправлять конфиденциальные сообщения A или B. Например, если пользователь книги паролей хочет отправить сообщение m для B (m должно быть меньшим r_B, или делиться на куски, меньшие r_B), то он использует ключ b из книги паролей для получения шифрованного сообщения m_1 по формуле $m_1 \equiv m^b \pmod{r_B}$, которое и отправляется B. B для дешифровки m_1 использует ключ β в формуле $m_1^{\beta} \equiv m^{b\beta} \equiv m \pmod{r_B}$, т. к. $b\beta \equiv 1 \pmod{\varphi(r_B)}$, следовательно, $b\beta = k\varphi(r_B) + 1$ для некоторого целого k и $m^{k\varphi(r_B)+1} \equiv (m^{\varphi(r_B)})^k m \equiv m \pmod{r_B}$, т.к. $m^{\varphi(r_B)} \equiv 1 \pmod{r_B}$ по теореме Эйлера-Ферма. Доказано [12], что задача нахождения секретного ключа β по данным из книги паролей имеет ту же сложность, что и задача разложения числа r_B на простые множители.

Пример. Пусть для A $p_{A_1} = 7$ и $p_{A_2} = 23$, тогда $r_A = p_{A_1}p_{A_2} = 161$, $\varphi(161) = 6 * 22 = 132$, $a = 7$, $\alpha = 19$ (из уравнения $7\alpha \equiv 1 \pmod{132}$). Следовательно, запись в книге паролей для A будет иметь вид A: 161, 7. Если кто-то захочет отправить A секретное сообщение $m = 3$, то он должен сначала превратить его в шифровку m_1 по формуле $m_1 \equiv 3^7 \equiv 94 \pmod{161}$. Когда A получит $m_1 = 94$ он дешифрует его по формуле $m \equiv 94^{19} \equiv 3 \pmod{161}$.

Задания

1

Нужно послать секретные сообщения 25 и 2 для JB и 14 для CIA, используя следующие записи открытой книги паролей криптосистемы RSA:

JB: 77,7;
CIA: 667,15.

2

Пользователь системы RSA выбрал $p_1 = 11$ и $p_2 = 47$. Какие из чисел 12, 33, 125, 513 он может выбрать для открытого ключа? Вычислить для них закрытый ключ.

3

Пользователь системы RSA, выбравший $p_1 = 17$, $p_2 = 11$ и $a = 61$, получил шифрованное сообщение $m_1 = 3$. Дешифровать m_1.