Лабораторная работа № 3

Вариант 13

Кутреева С. И.
872302

① Найти открытый ключ K_o, используя расширенный алгоритм Евклида.

$p = 11$, $q = 5$, $K_c = 17$

$n = p \cdot q = 55$

$\varphi(r) = (p-1)\cdot(q-1) = 10 \cdot 4 = 40$

$\varphi(40) = 40 \cdot \frac{1}{2} \cdot \frac{4}{5} = 16$

40	2
20	2
10	2
5	5
1	

$17_{y_1} \bmod 40 = 1$

$17 K_o = 1 \bmod 40$

$K_o = 17^{\varphi(40)-1} \bmod 40 = 17^{15} \bmod 40 = \left((17^2)^7 \cdot 17\right) \bmod 40 = \left((9^2)^3 \cdot 17 \cdot 9\right) \bmod 40 =$

$= (1^3 \cdot 33) \bmod 40 = \underline{33}$

Расширенный алгоритм Евклида:

$\begin{cases} y_1 \cdot b \bmod a = 1 & a = \varphi(r), \\ x_1 \cdot a + y_1 \cdot b = d_1, & b = K_c \\ d_1 = НОД(a,b) \end{cases}$

② Выполнить шифрование RSA открытым ключом K_o первых 5 букв своей фамилии (КУПРЕ). Для представления букв в числовой форме исп-ть:

'А' – 2, 'Б' – 3, 'В' – 4, ..., 'Я' – 34. => 'К' – 13, 'У' – 22, 'П' – 18, 'Р' – 19, 'Е' – 7 ← M(i)

$C(1) = 13^{33} \bmod 55 = \left((13^2)^{16} \cdot 13\right) \bmod 55 = (4^{16} \cdot 13) \bmod 55 =$

$= (36 \cdot 13) \bmod 55 = (31^2 \cdot 13) \bmod 55 = (26 \cdot 13) \bmod 55 =$

$= (2 \cdot 13^2) \bmod 55 = (2 \cdot 4) \bmod 55 = 8$

Шифрование RSA:

$C(i) = (M(i)^{K_o}) \bmod n$, где C(i) – шифротекст

К	У	П	Р	Е
13	22	18	19	7
↓	↓	↓	↓	↓
8	22	13	39	2

$C(2) = 22^{33} \bmod 55 = \left((22^2)^{16} \cdot 22\right) \bmod 55 = (44^{16} \cdot 22) \bmod 55 =$

$= (11^8 \cdot 22) \bmod 55 = (11^4 \cdot 22) \bmod 55 = (11 \cdot 22) \bmod 55 = 22$

$C(3) = 18^{33} \bmod 55 = \left((18^2)^{16} \cdot 18\right) \bmod 55 = (49^{16} \cdot 18) \bmod 55 =$

$= (36^8 \cdot 18) \bmod 55 = (31^4 \cdot 18) \bmod 55 = (26^2 \cdot 18) \bmod 55 =$

$= (16 \cdot 18) \bmod 55 = 13$

$C(4) = 19^{33} \bmod 55 = \left((19^2)^{16} \cdot 19\right) \bmod 55 = (31^{16} \cdot 19) \bmod 55 = (26^8 \cdot 19) \bmod 55 =$

$= (16^4 \cdot 19) \bmod 55 = (36^2 \cdot 19) \bmod 55 = (31 \cdot 19) \bmod 55 = 39$

$C(5) = 7^{33} \bmod 55 = \left((7^3)^{11}\right) \bmod 55 = (13^{11}) \bmod 55 = (4^5 \cdot 13) \bmod 55 =$

$= (4^3 \cdot 4^2 \cdot 13) \bmod 55 = (9 \cdot 43) \bmod 55 = 2$

③ Выполнить проверку правильности расшифрования полученных зашифрованных данных при помощи закрытого ключа K_c.

$K_c = 17$, $C(i) = \{8, 22, 13, 39, 2\}$

$M(1) = 8^{17} \bmod 55 = \left((8^{2^8}) \cdot 8\right) \bmod 55 = (9^8 \cdot 8) \bmod 55 =$

Расшифровка RSA:

$M(i) = (C_i)^{K_c} \bmod n$, где

M(i) – множество чисел = исходный текст.

$= \left((9^4)^2 \cdot 8\right) \bmod 55 = \left(16^2 \cdot 8\right) \bmod 55 = \left(36 \cdot 8\right) \bmod 55 = 13$

$M(2) = 22^{17} \bmod 55 = \left(44^8 \cdot 22\right) \bmod 55 = \left(11^4 \cdot 22\right) \bmod 55 =$

$= \left(11^2 \cdot 22\right) \bmod 55 = 22$

$M(3) = 13^{17} \bmod 55 = \left(4^8 \cdot 13\right) \bmod 55 = \left((4^3)^2 \cdot 16 \cdot 13\right) \bmod 55 =$

$= \left(9^2 \cdot 43\right) \bmod 55 = \left(26 \cdot 43\right) \bmod 55 = 18$

$M(4) = 39^{17} \bmod 55 = \left(36^8 \cdot 39\right) \bmod 55 = \left(31^4 \cdot 39\right) \bmod 55 = \left(26^2 \cdot 39\right) \bmod 55 =$

$= \left(16 \cdot 39\right) \bmod 55 = 19$

$M(5) = 2^{17} \bmod 55 = \left(31 \cdot 2\right) \bmod 55 = 7$

8	22	13	39	2
↓	↓	↓	↓	↓
13	22	18	19	7
К	У	П	Р	Е