1.

$X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$

$E_{k_j}(x_i) = y_{(i+j) \bmod 3}$

Шифр совершенен, если выполняются два условия:

- для каждой пары входных данных (x и y) существует единственный ключ, который может использоваться для шифрования и дешифрования сообщений;

- должно обеспечиваться равномерное распределение вероятности на ключах, т.е. статистически одинаковая вероятность использования одного ключа.

Выпишем все возможные комбинации:

$E_{k_0}(x_0) = y_{(i+j) \bmod 3} = y_0$
$E_{k_0}(x_1) = y_{(i+j) \bmod 3} = y_1$
$E_{k_1}(x_0) = y_{(i+j) \bmod 3} = y_1$
$E_{k_1}(x_1) = y_{(i+j) \bmod 3} = y_2$
$E_{k_2}(x_0) = y_{(i+j) \bmod 3} = y_2$
$E_{k_2}(x_1) = y_{(i+j) \bmod 3} = y_0$

Рассмотрим пары x_i и y_j и сопоставим их с k_t:

$(x_0, y_0) \rightarrow k_0$
$(x_0, y_1) \rightarrow k_1$
$(x_0, y_2) \rightarrow k_2$
$(x_1, y_0) \rightarrow k_2$
$(x_1, y_1) \rightarrow k_0$
$(x_1, y_2) \rightarrow k_1$

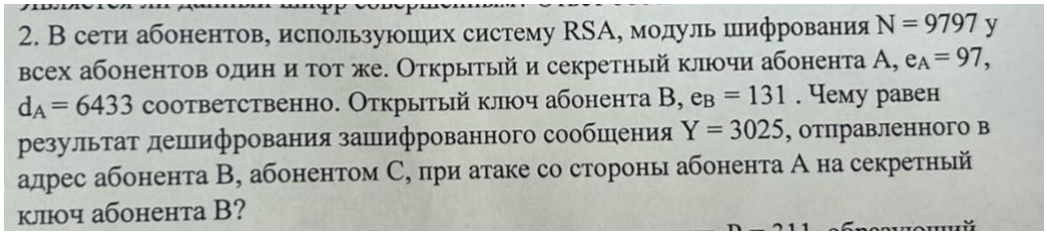
Как можно видеть, каждой паре xi и yj соответствует единственный ключ, т.е. первое условие выполняется.

Второе условие выполняется, исходя из условия, что ключи выбираются равновероятно.

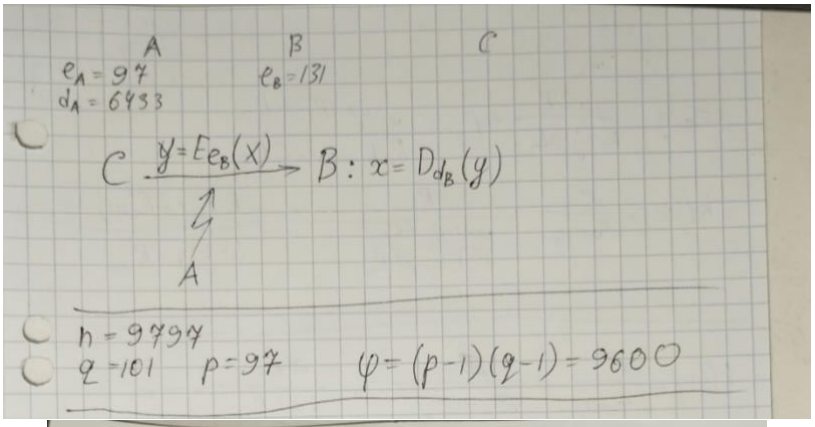
Значит, данный шифр является совершенным

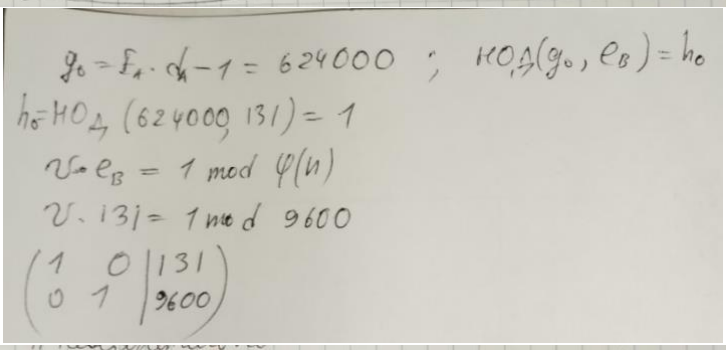
2.

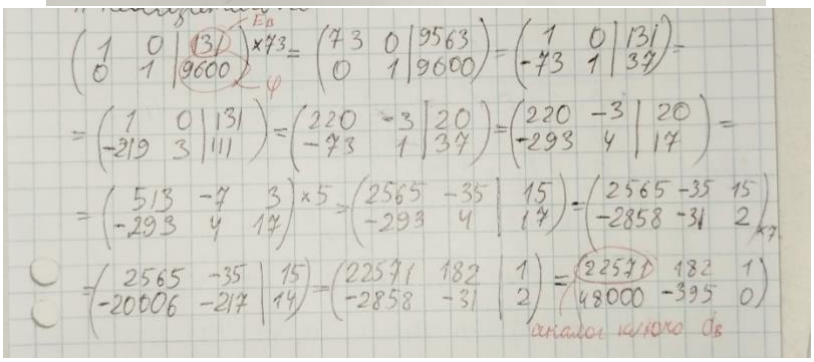
Вариант 1



2. В сети абонентов, использующих систему RSA, модуль шифрования N = 9797 у всех абонентов один и тот же. Открытый и секретный ключи абонента A, $e_A = 97$, $d_A = 6433$ соответственно. Открытый ключ абонента B, $e_B = 131$. Чему равен результат дешифрования зашифрованного сообщения Y = 3025, отправленного в адрес абонента B, абонентом C, при атаке со стороны абонента A на секретный ключ абонента B?


A
B
C
$e_A = 97$
$d_A = 6433$
$e_B = 131$
$C \xrightarrow{y = Ee_B(x)} B : x = D_{d_B}(y)$
A
$n = 9797$
$q = 101$
$p = 97$
$\varphi = (p-1)(q-1) = 9600$


$g_0 = E_A \cdot d_A - 1 = 624000$; $НОД(g_0, e_B) = h_0$
$h_0 = НОД(624000, 131) = 1$
$v \cdot e_B = 1 \bmod \varphi(n)$
$v \cdot 131 = 1 \bmod 9600$
$\left(\begin{array}{cc|c} 1 & 0 & 131 \\ 0 & 1 & 9600 \end{array}\right)$


$\left(\begin{array}{cc|c} 1 & 0 & 131 \\ 0 & 1 & 9600 \end{array}\right) \times 73 = \left(\begin{array}{cc|c} 73 & 0 & 9563 \\ 0 & 1 & 9600 \end{array}\right) = \left(\begin{array}{cc|c} 1 & 0 & 131 \\ -73 & 1 & 37 \end{array}\right) =$
$= \left(\begin{array}{cc|c} 1 & 0 & 131 \\ -219 & 3 & 111 \end{array}\right) = \left(\begin{array}{cc|c} 220 & -3 & 20 \\ -73 & 1 & 37 \end{array}\right) = \left(\begin{array}{cc|c} 220 & -3 & 20 \\ -293 & 4 & 17 \end{array}\right) =$
$= \left(\begin{array}{ccc} 513 & -7 & 3 \\ -293 & 4 & 17 \end{array}\right) \times 5 = \left(\begin{array}{cc|c} 2565 & -35 & 15 \\ -293 & 4 & 17 \end{array}\right) = \left(\begin{array}{ccc} 2565 & -35 & 15 \\ -2858 & -31 & 2 \end{array}\right) \times 7$
$= \left(\begin{array}{cc|c} 2565 & -35 & 15 \\ -20006 & -217 & 14 \end{array}\right) = \left(\begin{array}{cc|c} 22571 & 182 & 1 \\ -2858 & -31 & 2 \end{array}\right) = \left(\begin{array}{ccc} 22571 & 182 & 1 \\ 48000 & -395 & 0 \end{array}\right)$
каноническое d_B

3.

4.

(4). Вариант 2.

(0,7) $p(x) = x^8 \oplus x^4 \oplus x^3 \oplus x \oplus 1$

$00000111 = x^2 \oplus x \oplus 1$

$$\left(\begin{array}{cc|c} 1 & 0 & x^2 \oplus x \oplus 1 \\ 0 & 1 & x^8 \oplus x^4 \oplus x^3 \oplus x \oplus 1 \end{array}\right)$$

$$\left(\begin{array}{cc|c} 1 & 0 & x^2 \oplus x \oplus 1 \\ x^6 \oplus x^5 \oplus x^3 & 1 & x \oplus 1 \end{array}\right)$$

$$\left(\begin{array}{cc|c} x^7 \oplus x^6 \oplus x^4 \oplus 1 & x \oplus 1 & 1 \\ x^6 \oplus x^5 \oplus x^3 & 1 & x \oplus 1 \end{array}\right)$$

$$x^8 \oplus x^4 \oplus x^3 \oplus x \oplus 1 \;\big|\; x^2 \oplus x \oplus 1$$
$$x^8 \oplus x^7 \oplus x^6 \qquad\qquad x^6 \oplus x^5 \oplus x^3$$
$$x^7 \oplus x^6 \oplus x^4 \oplus x^3 \oplus x \oplus 1$$
$$x^7 \oplus x^6 \oplus x^5$$
$$x^5 \oplus x^4 \oplus x^3 \oplus x \oplus 1$$
$$x^5 \oplus x^4 \oplus x^3$$
$$x \oplus 1$$

$$x^7 \oplus x^6 \oplus x^4 \oplus 1 \cdot x^2 \oplus x \oplus 1 = x^9 \oplus x^8 \oplus x^6 \oplus x^2 \oplus x^8 \oplus x^7 \oplus x^5 \oplus x \oplus$$
$$\oplus x^7 \oplus x^6 \oplus x^4 \oplus 1 = x^9 \oplus x^5 \oplus x^4 \oplus x^2 \oplus x \oplus 1$$

$$x^9 \oplus x^5 \oplus x^4 \oplus x^2 \oplus x \oplus 1 \;\big|\; x^8 \oplus x^4 \oplus x^3 \oplus x \oplus 1$$
$$x^9 \oplus x^5 \oplus x^4 \oplus x^2 \oplus x \qquad\qquad x$$
$$1$$

(0,7) $p(x) = x^8 + x^4 + x^3 + x + 1$

$(0,7) = (00000111) = x^2 + x + 1$

$$\left(\begin{array}{cc|c} 1 & 0 & x^2+x+1 \\ 0 & 1 & x^8+x^4+x^3+x+1 \end{array}\right)$$

$x^8 + x^4 + x^3 + x + 1 \;\big|\; x^2 + x + 1$

$+ x^8 + x^7 + x^6 \qquad\qquad x^6 + x^5 + x^3$

$x^7 + x^6 + x^4 + x^3 + x + 1$

$+ x^7 + x^6 + x^5$

$x^6 + x^5 + x^4 + x^3 + x + 1$

$+ x^5 \; x^4 + x^3$

$x + 1$

(ищем множитель)

$\Rightarrow x^8 + x^4 + x^3 + x + 1 = (x^2 + x + 1)(x^6 + x^5 + x^3) + x + 1$

$$\left(\begin{array}{cc|c} 1 & 0 & x^2+x+1 \\ 0 & 1 & x^8+x^4+x^3+x+1 \end{array}\right) \overset{x^6+x^5+x^3}{=} \left(\begin{array}{cc|c} x^6+x^5+x^3 & 0 & (x^6+x^5+x^3)(x^2+x+1) \\ 0 & 1 & x^8+x^4+x^3+x+1 \end{array}\right) / (x^6+x^5+x^3) =$$

$$= \left(\begin{array}{cc|c} 1 & 0 & [illegible] \\ x^6+x^5+x^3 & 1 & [illegible] \end{array}\right) \begin{matrix} x^2+x+1 \\ x+1 \end{matrix} \times \left(\begin{array}{cc|c} [illegible] & 0 & x^2+x+1 \\ [illegible]\times(x^6+x^5+x^3) & 1 & (x+1)x \end{array}\right) =$$

$$= \left(\begin{array}{cc|c} x^7+x^6+x^4+1 & 0 & x^2+x+1 \\ x^6+x^5+x^3 & 1 & x^2+x+0 \end{array}\right) \Rightarrow \quad x^7 + x^6 + x^4 + 1$$

$(11010001) = (1101, 0001) = (D, 1)$

Проверка:

$(x^2 + x + 1) \cdot (x^7 + x^6 + x^4 + 1) \bmod p(x) = 1$

проверяется с помощью кода в online

$x^9 + x^5 + x^4 + x^3 + x^2 + x \;\big|\; x^8 + x^4 + x^3 + x + 1$

$x^9 + x^5 + x^4 + x^2 + x + 1 \;\big|\; x$

1

5.

(0,6) = 0000 1011 – $x^3 + x + 1$

$P(x) = x^8 + x^4 + x^3 + x + 1$

RSA:
1) потоковый – де бит, блочный – де байт
2) ассиметричный
3) шифр замены
4) однозначный
5) однократный

Вариант 1

№5

1) шифр замены
2) симметричный
3) потоковый – бит, блочный – байт
4) однозначный
5) многократный

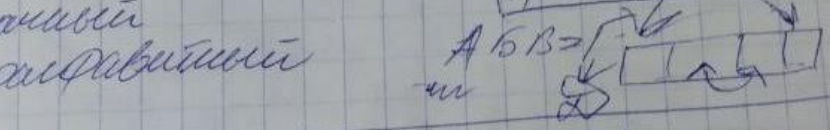
	X_0	X_1
K_0	Y_0	Y_1
K_1	Y_1	Y_2
K_2	Y_2	Y_0

Вариант 2

Шифр Вижинера:
1) замены
2) симметричный
3) потоковый/блочный
4) однозначный
5) многократный

0 → (1, 2)

Эль-Гамаль:
1) замены
2) ассиметричный
3) потоковый/блочный
4) многозначный
5) многократный



Вариант 3

Шифр Вернама:
1) Замены
2) симметричный
3) потоковый
4) однозначный
5) однократный

DES/МАГМА:
1) Замена
2) симметричный
3) блочный
4) однозначный
5) однократный

18.10.2023 18:09

RSA	блочный ассиметричный шифр замены однозначный одноалфавитный
Цезарь	замены симметричный поточный однозначный одноалфавитный
Вижинер	замены симметричный потоковый однозначный многоалфавитный
Эль-гамаль	замены асимметричный блочный многозначный многоалфавитный
Магма **DES**	замены симметричный блочный однозначный одноалфавитный
Из задачи №1	замены симметричный потоковый однозначный многоалфавитный

Гост 28147 89

Режим простой замены

Режим гаммирования

Режим гаммирования с простой связью

Режим выработки имитосвязи