

1. Module 1

7 варіант

1.1. 1

1. Схema RSA. Повідомлення: m = 17; параметри: p = 3 , q = 7, e = 17.

Знайти d, зашифрувати m (тобто знайти c), розшифрувати c.

$$\begin{cases} p = 3 \\ q = 7 \\ e = 17 \\ m = 17 \end{cases}$$
$$n = 21$$
$$\text{mod } \varphi(n) = 12$$
$$17d \equiv 1 \pmod{12}$$

Need to calculate **modular multiplicative inverse**

$$d \equiv 17^{-1} \pmod{12}$$

Using extended Euclidean algorithm. Let’s set: $x_0 = 1, x_1 = 0$

While a>1:

$$q = 1; (a, n) = (12, 5); (x_0, x_1) = (1, -1)$$
$$q = 2; (a, n) = (5, 2); (x_0, x_1) = (-1, 3)$$
$$q = 2; (a, n) = (2, 1); (x_0, x_1) = (3, 5)$$
$$q = 2; (a, n) = (1, 1); (x_0, x_1) = (5, \dots)$$
$$a = 1, \text{ stop}$$
$$x_0 = 5 \rightarrow x = 5$$

Let's verify: $17 * 5 \pmod{12} = 85 \pmod{12} = 1$

$$d = 5$$

Public key = (n, e) = (21, 17)

The encrypted message is $y = 17^{17} \pmod{21}$

The decrypted message is

$$m = 17^{17 * d} \pmod{21}$$
$$m = 17^{17 * 5} \pmod{21}$$

as we know $(17 * 5) = k12 + 1 = 84 + 1 = 85$

$$m = 17^{7 * \varphi(21)} 17 \pmod{21} = 17 \pmod{21}$$

1.2. 2

2. Розв’язати порівняння за модулем:

Need to calculate **modular multiplicative inverse**

$$610x \equiv 1 \pmod{987}$$
$$x \equiv 610^{-1} \pmod{987}$$
$$610x - 987y = 1$$

Using extended Euclidean algorithm. Let’s set: $x_0 = 1, x_1 = 0$

$q =$	$\frac{r_{i-1}-r_{i-1}}{r_i}$	$r_i = r_{i-2} - qr_{i-1}$	$t_{i+1} = t_{i-1} - q_it_i$
0		610	0
1		987	1
1		377	-1
1		233	2
1		144	-3
1		89	5
1		55	-8
1		34	13
1		21	-21
1		13	34
1		8	-55
1		5	89
1		3	-144
1		1	233
1		0	-377

$$x \equiv -377 \pmod{987} = 610$$

1.3. 3

$$15^{3^{1000}} \pmod{17} =$$
$$3^{1000} \pmod{16} = 16^x + y$$
$$15^{16x+y} \pmod{17} = 15^y * 15^{16x} \pmod{17}$$

За малою теоремою Ферма

$$15^{16x} \pmod{17} = (15^{16})^x \pmod{17}$$
$$(15^{p-1})^x \pmod{p} = 1^x \pmod{p} \longrightarrow (15^{16})^x \pmod{17} = 1 \pmod{17}$$

Залишилось знайти y.

$$15^y \pmod{17} = 15^{3^{1000}} \pmod{17}$$

16 is not prime. 3^1000 is not prime, but 3 and 16 is coprime -> we can apply Euler’s theorem.

$$\varphi(n) = 8$$
$$3^{1000} \pmod{16} = (3^8)^{125} \pmod{16}$$

By Euler’s theorem:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$
$$3^8 \equiv 1 \pmod{16}$$
$$(3^8)^{125} \equiv 1 \pmod{16}$$
$$3^{1000} \pmod{16} = 1 \pmod{16}$$
$$3^{1000} = 16^z + 1$$

Finally:

$$15^{16z} * 15 \pmod{17}$$
$$15^{16z} \pmod{17} = 1 \pmod{17}$$
$$1 * 1 * 15 \pmod{17} = 15 \pmod{17}$$