Task 1 Lada Ivanna Matveeva AIS ID: 99198 LAB 8.

1.1 $p = 5$, $q = 7$

1.2 $N = 35$

$F(N) = (p-1)(q-1) = 24$

$24 - 2, 3 \quad 35 = 5, 7$

$11 \neq 2, 3, 5, 7$

$e \begin{cases} 1 < e < f(N) \\ \text{coprime with } N, F(N) \end{cases}$

$e(11, 35)$ - public key

Inverse modulo
Extended Euclidian

$d \cdot e \pmod{f(N)} = 1$

$11 \cdot d \pmod{24} = 1$

$24 = 11 \cdot 2 + 2 \quad \rightarrow 2 = 24 - 11 \cdot 2$

$11 = 2 \cdot 5 + 1 \quad \rightarrow 1 = 11 - 2 \cdot 5$

$1 = 11 - 2 \cdot 5$

$1 = 11 - (24 - 11 \cdot 2) \cdot 5$

$1 = 11 - 5 \cdot (24 - 11 \cdot 2)$

$1 = 11 - 5 \cdot 24 + 11 \cdot 2 \cdot 5$

$1 = 11 + 11 \cdot 10$

$1 = 11 \cdot 11$

$11^{-1} \bmod 24 = 11$ $\quad 11 \cdot 11 \bmod 24 = 1$

a - z → 1 - 26
A - Z → 27 - 52

$d(11, 35)$ - private key

word : B r a t i s l a v a
dec : 28 18 1 20 9 19 12 1 22 1

encrypt:

B : 28 → $28^{11} \bmod 35 = 7$

r : 18 → $18^{11} \bmod 35 = 2$

a : 1 → $1^{11} \bmod 35 = 1$

decrypt

$7 \rightarrow 7^{11} \bmod 35 = 28$: B

$2 \rightarrow 2^{11} \bmod 35 = 18$: r

$1 \rightarrow 1^{11} \bmod 35 = 1$: a

t: 20 → $20^{11} \bmod 35 = 20$ | $20 \to 20^{11} \bmod 35 = 20$: t

i: 9 → $9^{11} \bmod 35 = 4$ | $4 \to 4^{11} \bmod 35 = 9$: i

s: 19 → $19^{11} \bmod 35 = 24$ | $24 \to 24^{11} \bmod 35 = 19$: s

l: 12 → $12^{11} \bmod 35 = 3$ | $3 \to 3^{11} \bmod 35 = 12$: l

a: 1 → $1^{11} \bmod 35 = 1$ | $1 \to 1^{11} \bmod 35 = 1$: a

v: 22 → $22^{11} \bmod 35 = 8$ | $8 \to 8^{11} \bmod 35 = 22$: v

a: 1 → $1^{11} \bmod 35 = 1$ | $1 \to 1^{11} \bmod 35 = 1$: a

Task 2

2.1 $p = 9$ $N = 99$

2.2 $q = 11$

$99 = 11 \cdot 3$

$80 = 2 \cdot 5$

$13 \neq 2, 3, 5, 11$

$$F(N) = (p-1)(q-1) = 8 \cdot 10 = 80$$

$$e\{\ 1 < e < F(N)$$
$$\text{coprime with } N, F(N)$$

$e(13, 99)$

$d \cdot e \pmod{f(N)} = 1$

$13d \pmod{80} = 1$

Extended Euclidian

$80 = 13 \cdot 6 + 2$ | $2 = 80 - 13 \cdot 6$

$13 = 2 \cdot 6 + 1$ | $1 = 13 - 2 \cdot 6$

$1 = 13 - (80 - 13 \cdot 6) \cdot 6$

$1 = 13 - 6(80 - 13 \cdot 6)$

$1 = 13 - 6 \cdot 80 + 13 \cdot 6 \cdot 6$

$1 = 13 + 13 \cdot 36$

$1 = 13 \cdot 37$

$13^{-1} \bmod 80 = 37$

$13 \cdot 37 \mod 80 = 1$

$e(13, 99)$ – public key
$d(37, 99)$ – private key

A – Z – 1 – 26

encrypt			decrypt		
B – 2	→	$2^{13} \mod 99 = 74$	$74^{37} \mod 99 = 2$	:	B
A – 1	→	$1^{13} \mod 99 = 1$	$1^{37} \mod 99 = 1$	:	A
N – 14	→	$14^{13} \mod 99 = 5$	$5^{37} \mod 99 = 14$	:	N
K – 11	→	$11^{13} \mod 99 = 11$	$11^{37} \mod 99 = 11$	:	K

Task 3

3.1 $p = 7$

3.2 $q = 11$

e { $1 < e < f(N)$
coprime with N, $F(N)$

$F(N) = (p-1) \cdot (q-1) = 60$

$N = 77$

$77 - 7, 11$
$60 - 2, 3, 5$

~~2~~, ~~3~~, ~~5~~, ~~7~~, ~~11~~, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, ~~61~~

$e \in \{13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59\}$

2. $p = 9 \quad q = 11$

$N = 99$

$F(N) = (p-1)(q-1) = 8 \cdot 10 = 80$

e { $1 < e < F(N)$ coprime with $N, F(N)$

$99 = 3 \cdot 11$

$80 = 2 \cdot 5$

~~2~~, ~~3~~, ~~5~~, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, ~~83~~, ~~89~~

$e \in$ { 7, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79 }