Matveeva Lada Ivanna Lab 12 AIS ID 99198

Task 1

$h(M) = 88$

Choose $p = 17$ and $q = 11$ $\qquad 187 = 17 \cdot 11$

$N = 187$ $\qquad 160 = 2,5$

$F(N) = (p-1)(q-1) = 160$

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

$e(7, 187)$ - public key

Inverse modulo Extended Euclidian

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

$7 \cdot d \pmod{160} = 1$

$160 = 7 \cdot 22 + 6 \rightarrow 6 = 160 - 7 \cdot 22$

$7 = 6 \cdot 1 + 1 \rightarrow 1 = 7 - 6 \cdot 1$

$1 = 7 - (160 - 7 \cdot 22) \cdot 1$

$1 = 7 - 160 + 7 \cdot 22$

$1 = 7 + 7 \cdot 22$

$1 = 7 \cdot 23$

$7^{-1} \bmod 160 = 23$

$2 + 2 \cdot 3 = 8$

$2 \cdot 4 = 8$

$e(7, 187)$ - public key

$d(23, 187)$ - private key

Signir's private key:

$s = h(M)^d \bmod n$

$s = 88^{23} \bmod 187$

$s = 11$

Verify the signature of the message M

$s^e \bmod n$

$11^7 \bmod 187 = 88$

In this case, we will assume that the signature is genuine

Task 2.1

$n = p * q = 851$

$851 \bmod 2 = 1$

$851 \bmod 3 = 2$

$851 \bmod 5 = 1$

$851 \bmod 7 = 4$

$851 \bmod 11 = 4$

$851 \bmod 13 = 6$

$851 \bmod 17 = 1$

$851 \bmod 19 = 15$

$851 \bmod 23 = 0$

$p = 23$

$q = \frac{851}{23} = 37$

$p = 23, q = 37$

Task 2.2.

$p = 3, q = 11, n = 33, e = 7, d = 3$

$c = m^e \bmod n$

$m = 2$

$(7, 33)$ - public key

encrypt:

$2^7 \bmod 33 = 29$

re-encrypt:

$29^7 \bmod 33 = 17$

$17^3 \bmod 33 = 8$

$8^3 \bmod 33 = 2$

Task 3.2

The code for this task is in ex2_3.py

The appropriate key is 19.

The cipher text includes the name of the AES algorithm.