Course: "Fundamentals of Cryptography".

Laboratory work No. 5.

Exercise 1.

1.1. Calculate a common secret key in an asymmetric encryption algorithm for a chosen functions:

a) $2^x \pmod 4$;

b) $78^x \pmod{33}$.

The secret keys for the transmitter and receiver: 6 and 3.

1.2. Answer the question: is it possible to use the function $2^{-1} \pmod 6$ as a common functions and justify your answer.

Exercise 2.

Find prime roots modulo for the function **$y = a^x \bmod n$**:

n = 8;

n = 11.

Justify the answer by constructing a complete table of reflections **(a,x) → (y).**

Exercise 3.

Construct a table of mappings (a,x) → (y) for the function y= a x mod 7 and determine the value of x corresponding to the combinations

a = 1, y = 1;

a = 3, y = 4;

a = 4, y = 2;

a = 5, y = 6;

a = 6, y = 6.

Indicate which of these values of a,x are suitable for use in coding algorithms.

Exercise 4.

Calculate multiplicative inverse number of 34 (mod 27). $34^{-1} \pmod{27}$ and describe the calculation procedure step by step.