

Kolokwium zaliczeniowe ćwiczeń z WKR – I termin

Imię i nazwisko:.....Grupa:.....Nr albumu:.....

Zadanie 1

Niech $x \in \mathbb{Z}_{31}$ odpowiada wartości liczbowej tekstu jawnego i niech $y \in \mathbb{Z}_{31}$ odpowiada wartości liczbowej szyfrogramu. Znajdź wartość liczbową tekstu jawnego wiedząc, że $y = 20$, a do szyfrowania użyto szyfru afinicznego z kluczem $k = (a, b) = (11, 8)$.

Zadanie 2.

Alicja i Bob uzgodnili między sobą grupę multiplikatywną \mathbb{Z}_{113}^* oraz jej generator $\alpha = 3$. Wyznacz wartość klucza k uzgodnionego przez Alicję i Boba za pomocą protokołu Diffie-Hellmana wiedząc, że ich wartości prywatne wynoszą odpowiednio $a = 20$ oraz $b = 24$.

Zadanie 3.

Wykorzystując kryptosystem RSA oraz mając dane:

Alicji: dwie liczby pierwsze $p = 19$ i $q = 11$ oraz liczbę losową $e = 101$,

Bob: dwie liczby pierwsze $p = 17$ i $q = 13$ oraz liczbę losową $e = 61$:

- Alicja przesłała do Boba szyfrogram $y = 65$. Wyznacz wartość liczbową tekstu jawnego x .
- Alicja przesłała do Boba wiadomość, której skrót wynosi $h = 35$ wraz z podpisem cyfrowym $s = 140$. Zweryfikować poprawność tego podpisu cyfrowego.

Zadanie 4

Wykorzystując kryptosystem ElGamala oraz mając dane:

Alicji: grupę multiplikatywną \mathbb{Z}_{109}^* oraz jej generator $\alpha = 6$, liczbę losową będącą elementem klucza prywatnego $t = 30$,

Bob: grupę multiplikatywną \mathbb{Z}_{101}^* oraz jej generator $\alpha = 3$, liczbę losową będącą elementem klucza prywatnego $t = 50$,

- Alicja chce wysłać Bobowi wiadomość $x = 40$ w postaci zaszyfrowanej. Wyznacz wartość liczbową tego szyfrogramu, wiedząc, że do szyfrowania wykorzystano randomizer $r = 25$;
- Alicja chce podpisać wiadomość, której skrót wynosi $h = 60$. Wyznacz wartość tego podpisu cyfrowego, wiedząc, że do jego wygenerowania wykorzystany został randomizer $r = 19$.

Zadanie 5

Sprawdź, czy $\alpha = 3$ jest generatorem grupy multiplikatywnej \mathbb{Z}_{107}^* oraz oblicz liczbę generatorów w \mathbb{Z}_{107}^* .

Uwaga: Wszystkie obliczenia wykonać przy użyciu poznanych algorytmów.