

## Kolokwium zaliczeniowe ćwiczeń z WKR dla grupy IZ06IO1

Tytuł maila/załącznika: WKRZ\_2022\_Grupa\_Nazwisko\_Imie\_numer

### Zadanie 1.

Niech  $x \in \mathbb{Z}_{29}$  odpowiada wartości liczbowej tekstu jawnego i niech  $y \in \mathbb{Z}_{29}$  odpowiada wartości liczbowej szyfrogramu. Znajdź wartość liczbową tekstu jawnego wiedząc, że  $y = 15$ , a do szyfrowania użyto szyfru afinicznego z kluczem  $k = (a, b) = (7, 6)$ .

### Zadanie 2.

Alicja i Bob uzgodnili między sobą grupę multiplikatywną  $\mathbb{Z}_{107}^*$  oraz jej generator  $\alpha = 2$ .

Wyznacz wartość klucza  $k$  uzgodnionego przez Alicję i Boba za pomocą protokołu Diffie-Hellmana wiedząc, że ich wartości prywatne wynoszą odpowiednio  $a = 23$  oraz  $b = 30$ .

### Zadanie 3.

Wykorzystując kryptosystem RSA oraz mając dane:

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

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

- Bob przesłała do Alicji szyfrogram  $y = 73$ . Wyznacz wartość liczbową tekstu jawnego  $x$ .
- Bob przesłała do Alicji wiadomość, której skrót wynosi  $h=30$  wraz z podpisem cyfrowym  $s=140$ . Zweryfikować poprawność tego podpisu cyfrowego.

### Zadanie 4.

Wykorzystując kryptosystem ElGamala oraz mając dane:

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

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

- Bob chce wysłać Alicji wiadomość  $x=50$  w postaci zaszyfrowanej. Wyznacz wartość liczbową tego szyfrogramu, wiedząc, że do szyfrowania wykorzystano randomizer  $r = 25$ ;
- Bob chce podpisać wiadomość, której skrót wynosi  $h=60$ . Wyznacz wartość tego podpisu cyfrowego, wiedząc, że do jego wygenerowania wykorzystany został randomizer  $r=23$ .

### Zadanie 5.

Sprawdź, czy  $\alpha = 2$  jest generatorem grupy multiplikatywnej  $\mathbb{Z}_{113}^*$  oraz oblicz liczbę generatorów w  $\mathbb{Z}_{113}^*$ .

**Uwaga:** Wszystkie obliczenia wykonać przy użyciu poznanych algorytmów.