Kolokwium zaliczeniowe ćwiczeń z WKR dla grupy IZ06PD1

Tytuł maila/załącznika: WKRZ_2022_Grupa_Nazwisko_Imie_numer

Zadanie 1.
Niech $x \in \mathbf{Z}_{29}$ odpowiada wartości liczbowej tekstu jawnego i niech $y \in \mathbf{Z}_{29}$ odpowiada wartości liczbowej szyfrogramu. Znajdź wartość liczbową tekstu jawnego wiedząc, że y = 20, a do szyfrowania użyto szyfru afinicznego z kluczem $k = (a, b) = (5, 10)$.

Zadanie 2.
Alicja i Bob uzgodnili między sobą grupę multiplikatywną 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 $a = 25$ oraz $b = 29$.

Zadanie 3.
Wykorzystując kryptosystem RSA oraz mając dane:
Alicji: dwie liczby pierwsze p = 11 i q = 19 oraz liczbę losową e = 101,
Boba: dwie liczby pierwsze p = 13 i q = 17 oraz liczbę losową e = 61:
a) Alicja przesłała do Boba szyfrogram y = 50. Wyznacz wartość liczbową tekstu jawnego x.
b) Alicja przesłała do Boba wiadomość, której skrót wynosi $h=40$ wraz z podpisem cyfrowym $s=150$. Zweryfikować poprawność tego podpisu cyfrowego.

Zadanie 4.
Wykorzystując kryptosystem ElGamala oraz mając dane:
Alicji: grupę multiplikatywną Z_{109}^* oraz jej generator α=6, liczbę losową będącą elementem klucza prywatnego t=25,
Boba: grupę multiplikatywną Z_{101}^* oraz jej generator α=3, liczbę losową będącą elementem klucza prywatnego t=35,
a) Alicja chce wysłać Bobowi wiadomość $x = 60$ w postaci zaszyfrowanej. Wyznacz wartość liczbową tego szyfrogramu, wiedząc, że do szyfrowania wykorzystano randomizer $r = 30$;
b) Alicja chce podpisać wiadomość, której skrót wynosi $h=99$. Wyznacz wartość tego podpisu cyfrowego, wiedząc, że do jego wygenerowania wykorzystany został randomizer $r=20$.

Zadanie 5.
Sprawdź, czy α = 3 jest generatorem grupy multiplikatywnej Z_{103}^* oraz oblicz liczbę generatorów w Z_{103}^*.

Uwaga: Wszystkie obliczenia wykonać przy użyciu poznanych algorytmów.