Kolokwium zaliczeniowe ćwiczenia z WKR dla grupy IZ06IO2

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

Zadanie 1.
Niech $x \in \mathbf{Z}_{31}$ odpowiada wartości liczbowej tekstu jawnego i niech $y \in \mathbf{Z}_{31}$ odpowiada wartości liczbowej szyfrogramu. Znajdź wartość liczbową tekstu jawnego wiedząc, że $y = 25$, a do szyfrowania użyto szyfru afinicznego z kluczem $k = (a, b) = (11, 8)$.

Zadanie 2.
Alicja i Bob uzgodnili między sobą grupę multiplikatywną 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 $a = 26$ oraz $b = 22$.

Zadanie 3.
Wykorzystując kryptosystem RSA oraz mając dane:
Alicji: dwie liczby pierwsze $p = 19$ i $q = 11$ oraz liczbę losową $e = 101$,
Boba: dwie liczby pierwsze $p = 17$ i $q = 13$ oraz liczbę losową $e = 61$:

a) Alicja przesłała do Boba szyfrogram $y = 75$. Wyznacz wartość liczbową tekstu jawnego x.
b) Alicja przesłała do Boba 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 Z_{109}^* oraz jej generator $\alpha=6$, liczbę losową będącą elementem klucza prywatnego $t=30$,
Boba: grupę multiplikatywną Z_{101}^* oraz jej generator $\alpha=3$, liczbę losową będącą elementem klucza prywatnego $t=50$,

a) Alicja chce wysłać Bobowi wiadomość $x = 60$ w postaci zaszyfrowanej. Wyznacz wartość liczbową tego szyfrogramu, wiedząc, że do szyfrowania wykorzystano randomizer $r = 25$;
b) Alicja chce podpisać wiadomość, której skrót wynosi $h = 100$. Wyznacz wartość tego podpisu cyfrowego, wiedząc, że do jego wygenerowania wykorzystany został randomizer $r=19$.

Zadanie 5.
Sprawdź, czy $\alpha = 5$ jest generatorem grupy multiplikatywnej Z_{113}^* oraz oblicz liczbę generatorów w Z_{113}^*.

Uwaga: Wszystkie obliczenia wykonać przy użyciu poznanych algorytmów.