1. Consider a binary stream cipher where the key stream $z_1, z_2, \ldots$ is formed by repeating a randomly generated bit string $K = (k_1, k_2, \ldots, k_m)$. Hence $z_j = k_i$ if and only if $j \equiv i \pmod{m}$.

   a) (3 points) The redundancy of the plaintext is $R$. Determine the unicity distance, that is, how many bits of ciphertext is required on the average to determine the key $K$?

   b) (3 points) Assume that $m = 5$ and the plaintext bit string is formed by repeating the following procedure (a finite number of times): two bits are generated at random, and a third bit is computed as an xor sum of these two bits. The first fifteen bits of the ciphertext are: 0 1 0 1 0 1 1 1 0 0 0 1. Attempt to find the key $K = (k_1, k_2, k_3, k_4, k_5)$.

2. (6 points) Consider the finite field $\mathbb{F} = \mathbb{Z}_2[x]/(x^3 + x + 1)$ and let $f : \mathbb{F} \to \mathbb{F}$ be a function defined as

   $f(z) = z^{-1}$, for $z \neq 0$,

   $f(0) = 0$.

   Let a Feistel cipher be defined as follows

   $L_i = R_{i-1}$

   $R_i = L_{i-1} + f(R_{i-1} + K_i)$,

   where $L_i \in \mathbb{F}$, $R_i \in \mathbb{F}$ and the round keys are defined as $K_i = K^i$, for $i = 1, 2, 3$, where $K \in \mathbb{F}$ is the key. Assume that one known plaintext-ciphertext pair is given as follows: $L_0 = 100$, $R_0 = 001$, $L_3 = 110$ and $R_3 = 100$. Attempt to find the key $K$.

3. (6 points) Solve the following system of congruences

   $15x \equiv 12 \pmod{2003}$

   $12 \equiv x \pmod{2004}$

4. (6 points) It is given that

   $2^{41} \equiv 1655213 \pmod{15122003}$.

   Use the Pollard $p-1$ algorithm to find a nontrivial divisor of 15122003.

5. (6 points) The parameters in El Gamal Signature Scheme are $p = 31$, $\alpha = 3$. Alice sees two messages $x_1$ and $x_2$ and their signatures $(\gamma_1, \delta_1)$ and $(\gamma_2, \delta_2)$ generated by the same signer with the following values:

   $x_1 = 25$, $\gamma_1 = 24$, $\delta_1 = 7$

   $x_2 = 5$, $\gamma_2 = 24$, $\delta_2 = 17$

   Attempt to find the signer’s private key.