# Tutorial 2

(Last date to submit: 30th October 2021)

1. Let $G$ be a cyclic group of order $n$ with generator $\alpha$. Prove that order of order of $\alpha^k \in G$ is
$$\frac{n}{\gcd(n,k)}$$

2. In El-Gamal public key cryptosystem, the public key used is $(p, \alpha, \beta)$. Why is it important that $\alpha$ is primitive root modulo $p$? Is (97, 8, 33) a suitable El-Gamal public key? Justify your answer.

3. **Man-in-the-middle** (**MITM**) attack is a cyberattack where the attacker secretly transmits and possibly alters the communications between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two parties.
Suppose there are two parties A and B agreed to use Diffie Hellman key exchange using a cyclic group $Z_{13}$ with 2 as generator. A uses exponent 5 and B uses 4.
Suppose attacker can intercept as well as inject his own messages.
Let attacker uses exponent 7. Discuss how the attacker can use MITM attack on the key exchange between A and B.

4. G is a non-commutative group of order 10. Show that G must have a subgroup of order 5.

5. Let $G$ be a finite group of order $n$. prove that if $n$ is coprime to 3 and $(ab)^3 = a^3 b^3$ for all $a$, $b \in G$ then $G$ is abelian.

6. Prove that

   (a) $x^2 + 1$ is irreducible over $Z_7$.

   (b) $x^3 - 9$ is irreducible over $Z_{31}$.

   (c) $x^3 - 9$ is reducible over $Z_{11}$.

7. Gaussian integer is a complex number such that its real and imaginary parts are both integers. $Z[i] = \{a + bi \mid a, b \in Z\}$ is a ring of Gaussian integers. Prove that the ring of Gaussian integers modulo 3 is a field. Also find its characteristic.

8. Find a polynomial of degree 3 irreducible over the ring of integers, $Z_3$, mod 3. Use it to construct a field having 27 elements.

9. If F is a field, and $f \in F[x]$ with gcd $(f, D(f)) = 1$, then $f$ is square-free.

10. Prove that any homomorphism of a field is either a monomorphism or takes each element into 0.

11. Construct the Galois field of 16 elements, GF $(2^4)$, using a primitive polynomial

    $f(x) = x^4 + x + 1$. Compute the powers $x^i$, $0 \leq i \leq 14$ and represent these powers (multiplicative group) as polynomials of the form $a_0 + a_1 x + a_2 x^2 + a_3 x^3$.

12. Suppose there be two hash functions $h$ and $h'$. $h$ is $n$-bit hash function, which is pre-image, second pre-image and collision resistant.

    Function $h'$ is defined as

$$h'(x) = \begin{cases} 0||x & x \in \{0,1\}^n \\ 1||x & \text{otherwise} \end{cases}$$

    Prove that $h'$ is also second preimage and collision resistant, but it is not preimage resistant.

13. What is the minimum size of the linear feedback shift register, which can generate first nine bits 100000001?