Assignment

1. Find generator of Schnorr group for following prime $p = 11$. Also find other elements of the Schnorr group.
   (i) $p = 11 = 2 * 5 + 1$
2. How will create field of size (3^2). Write all the elements of field of size (3^2). Assume that prime(irreducible) polynomial exist in every degree.
3. Find the additive and the multiplicative inverse of $x^3 + x + 1$ in GF(2^4), with prime polynomial $= x^4 + x + 1$.
4. Find the multiplicative inverse of the following in GF(3^3) with respect to the prime polynomial $= x^3 + x + 1$.
   (i) $x^2 + 2x + 1$ (ii) $2x + 2$
5. Find the multiplicative inverse of the following in GF(7^4) with respect to the prime polynomial $= x^3 + 5$ (if exist else give reason for).
   (i) $5x^2 + 2x + 3$
6. What is one-way function? what is trapdoor one-way function?
7. State and prove the correctness of RSA Cryptosystem.
8. Find the computational cost (in terms of bit operation) of key generation in RSA algorithm.
9. For RSA with parameters: $e = 7$ and $n = 17 * 31$.
   (a) Encrypt the message block $M = 2$.
   (b) Compute a private key corresponding to the given above public key.
   (c) Perform the decryption of the obtained ciphertext using the method which is four times faster than usual method(Using CRT).
10. Alice and Bob have the same modulus n for RSA, and encryption exponents e_A and e_B with $gcd(e_A, e_B) = 1$. Charles sends them the same message m encrypted with these keys, resulting in the ciphertexts c_A and c_B. Adversary intercepts both c_A and c_B. How can she find m?
11. Solve the equation $x^2 + 4x + 1 = 0$ in Z_{23}.
12. What is the 11th root of 2 in Z_{19}? (i.e. what is $2^{1/11} in Z_{19}$)
13. Solve the following system of congruences:
    $x \equiv 12 (mod\ 25)$
    $x \equiv 9 (mod\ 26)$
    $x \equiv 23 (mod\ 27)$

14. Let g is the generator of the cyclic group Z_p. Show that g is quadratic non residue mod p.

15. Solve following quadratic congruent equation.
(i)$b^2 \equiv\ 44(mod\ 83)$-
(ii)$b^2 \equiv\ 11(mod\ 29)$
(iii)$b^2 \equiv\ 15(mod\ 59)$

16. Using only CRT show that if $x \cong y\ mod\ p\ \ and\ \ x \cong y\ mod\ q\ \ then\ \ x \cong y\ mod\ N$.

17. Let sender A sends the same message M to three different receivers using their respective public keys that have same $e = 3$ but different value of n. Let's assume you can intercept all three transmission. Can you find plaintext M in feasible time. If yes explain the method.

18. Show that text-RSA is vulnerable under following security notions.
(i) IND-CPA(semantic security) (ii) IND-CCA

19. Let (Gen,E,D) be a chosen ciphertext secure public-key encryption system with message space $\{0,1\}^{128}$. Which of the following is also chosen ciphertext secure?
(i)(Gen, E', D') where $E'(pk, m) = E(pk, m \oplus 1^{128})$ and $D'(sk, c) = D(sk, c) \oplus 1^{128}$
(ii)(Gen, E', D') where $E'(pk, m) = (E(pk, m), E(pk, 0^{128}))$ and $D'(sk, (c1, c2)) = D(sk, c1)$.
(iii)(Gen, E', D') where $E'(pk, m) = (E(pk, m), E(pk, m))$ and $D'(sk, (c1, c2)) = D(sk, c1)$.

20. Consider the elliptic curve $E_{11}(1, 6)$; that is, the curve defined by $y^2 = x^3 + x + 6$ with modulus of $p = 11$.
(i) Find all points.(ii) If public key assuming private key is 2.
(ii) Assume $k = 3$, find ciphertext. (iv) Decrypt ciphertext.

21. Find the sum of three points on an elliptic curve that lie on straight line?.

22. In the elliptic curve E(a,b) over the GF(2^n). Show that slope of tangent at point P(x_p, y_q) is equal to $(x_p + \frac{y_p}{x_p})$. Also find the expression $P + Q$.

23. Prove that text-ElGamal is not semantically secure (IND-CPA).

24. Prove that modified ElGamal is semantically secure (IND-CPA) if the DDH assumption holds. Show that modified ElGamal is not IND-CCA secure.

25. Prove that $NM - CPA \rightleftharpoons IND - CPA$.

26. Prove that $NM - CCAIND - CCA$.

27. Suppose RSA is (t', ϵ')-secure. Assume that challenge to the adversary is to make forgery on message M_c(Declared Message) in Full Domain Hash signature scheme. Then the Full Domain Hash signature scheme is (t, ϵ)-secure where
$t = t' - (q_{hash} + q_{sig} + 1)O(k^3)$
$\epsilon = \epsilon'$.

28. Suppose Alice wants to sign a message x. She first constructs the message digest z = h(x), and then computes the signature on z,namely, $y = sig_K(z)$. Then she transmits the ordered pair(x,y) over the channel.Suppose hash function is not secondary image resistant.Then show that Adversary can make selective forgery using chosen message attack.

29. Suppose Alice wants to sign a message x. She first constructs the message digest z = h(x),and then computes the signature on z,namely, $y = sig_K(z)$. Then she transmits the ordered pair(x,y) over the channel. Suppose hash function is not secondary image resistant. Then show that Adversary can make existential forgery using known message attack.

30. Suppose Alice wants to sign a message x. She first constructs the message digest z = h(x), and then computes the signature on z,namely, $y = sig_K(z)$. Then she transmits the ordered pair(x,y) over the channel. Suppose hash function is not collision resistant. Then show that Adversary can make existential forgery using chosen message attack.

31. Show that Schnore Signature Algorithm is existentially unforgeable under known message attack.

32. In a Shamire secret sharing (t,n), suppose that $p = 29, t = 3$ and $n = 5$. Find the shares of three participants P_1, P_3, P_5 with their x-coordinates {1,3,5}. You can assume the secret as last digit of your roll number if it is not zero. If last digit is zero then you can assume the secret as last two digit number. Given the shares of these three participants P_1, P_3, P_5 find the secret (Using Lagrange polynomial) for verification