Dept. of Computer Science and Engg.
Indian institute of Technology, Kharagpur

Subject: Cryptography and Network Security, Subject Code: CS60041
Full Marks: 100 Duration: 3 hrs. Date: 22.11.22 (AN)

Instruction: Answer all the questions

1. (a) Define RSA Cryptosystem with (i) key generation, (ii) encryption and (iii) decryption.

(b) Prove that RSA decryption works.

(c) Show that in RSA cryptosystem, one can find the primes p and q where n = pq, if he/she knows n and $\Phi(n)$.

(d) We want to set up the RSA cryptosystem in a network of n users. How many prime numbers do we have to generate?
We want to reduce this number by generating a smaller pool of prime numbers and making combinations of two of these primes: for each user, pick a new pair of two of these primes in order to set up his key. Show how a malicious user can factorize the modulus of some other user.

(e) We assume that two entities Alice and Bob use RSA public keys with same modulus n but with different public exponents, e1 and e2.
Prove that Eve can decrypt a message sent to Alice and Bob provided that gcd (e1, e2) = 1.

(5x5 = 25)

2. (a) What is an elliptic curve? What is the "zero point" of an elliptic curve?
(b) Consider the elliptic curve $E_7(0,2)$; that is the curve is defined by $y^2 = x3 + 2$ with a modulus of p = 7. Determine all the points in $E_7(0,2)$.
(c) Define the group G associated with the curve E, defined in (b)
(d) For $E_7(0,2)$, consider the point P = (3,1). Compute (i) 2P and (ii) 3P.
(e) Determine whether or not G is cyclic.

(5x5 = 25)

3. (a) Briefly explain Diffie-Hellman key exchange.
(b) Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root a = 2.

(i) Show that 2 is a primitive root of 11

(ii) If user A has public key $Y_A = 9$, what is A's private key X_A?

(iii) If user B has public key $Y_B = 3$, what is the shared secret key K?

(c) Write the key exchange using elliptic curves which is analogue of Diffie-Hellman key exchange.

(5x5 = 25)

4. (a) What is a message authentication code? What is the difference between a message authentication code and a one-way hash function?

(b) What characteristics are needed in a secure hash function?

(c) Consider the Davies and Price hash code scheme where DES is used as the encryption algorithm:]

$H_i = E_{Mi}[H_{i-1}] + H_{i-1}$, here + denotes EXOR operation.

Recall the complementarity property of DES:

If $Y = DES_k(X)$ then $Y' = DES_k(X')$; X' is complement of X.

Use this property to show how a message consisting of blocks $M_1, M_2, \ldots, M_n$ can be altered without altering its hash code.

(d) Frame an attack on the hash code defined in (c).

(e) Briefly describe the Keccak, the NIST Standard SHA3 hash function.

(5x5 = 25)