Indian Institute of Technology, Kharagpur
Department of Computer Science and Engineering
End Spring Semester 2023

Subject – Cryptography and Network Security, Subject No. – CS60041
Full Marks – 100, Date – 22th November, 2023, AN, Time – 3 hrs.

Answer all questions

1. Suppose Alice wishes to send a text message M to Bob using the RSA algorithm. Bob's public key is the pair (n, e) = (253, 13). Note that 253 = (23)(11). Alice uses an alphabet set of only 10 letters and encodes them as
   A = 0, B = 1, C = 2, D = 3, E = 4, F = 5, G = 6, H = 7, I = 8, J = 9.
   Alice transmits the message in blocks. Each block corresponds to two letters which are encoded into their numerical equivalents, e.g. BJ becomes [19] and then it is enciphered by using RSA.
   (a) If Bob receives the cipher text "AE", what was the message transmitted by Aliee?
   (b) In the above problem, why can't we put more than 2 letters in a block?
   (c) Are the text messages that are sent in this way secure? Justify your answer.
   (d) Does the above system work if the Alice uses the English alphabet set of 26 letters and encodes them as A = 0, B = 1, ..., Z = 25? If not, why? Suggest some changes so that the system works correctly.

   [5+5+5+5=20]

2. (a) For the elliptic curve $E_{13}(4,4)$, What is the size of the group G? What is the structure of G?
   (b) Suppose that the cubic polynomial $X^3 + AX + B$ factors as
   $$X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3).$$
   Prove that $4A^3 + 27B^2 = 0$ if and only if two (or more of e_1, e_2 and e_3 are same.
   (c) Describe the key exchange algorithm using elliptic curve. Explain clearly the notation used in the algorithm.
   (d) Consider and elliptic curve $E_5(1,1)$, and P (4,2), Q (0,1) be two point on E. Solve the elliptic curve discrete logarithm problem for P and Q (Hint: P = nQ).

   [4+6+4+6=20]

3. Let p = 2p' + 1 and q = 2q' + 1 be two s-bit long primes such that p' and q' are prime numbers. Let n = pq and g be an element of Z_n^* of order p'q'.
   (a) How should p, q, p', q' be generated. Give a sketch of the algorithm.
   (b) How should g be generated?

We now assume that p, q, p', q' are unknown and that only n and g are public. For a message m, which is represented by an integer of arbitrary size, we define the hash function $H(m) = g^m \bmod n$. This defines a hash function.

(c) Show that finding collisions on H is equivalent to factorizing n.
(d) Show that inverting H is at least as hard as solving the discrete logarithm problems with respect to the base g in Zp^* and Zq^*.

[4+4+6+6=20]

4(a) Find all possible values of "e" for N = 55. (e, N, p, q are the same as used in RSA).
(b) Define Euler-Totient function $\varphi(n)$. Suppose an eavesdropper Eve knows N = pq and also knows $\varphi(N) = (p-1)(q-1)$, Show that Eve can then find p and q.
(c) State Chinese Remainder Theorem. Is the requirement that the moduli be pair-wise relatively prime in CRT necessary? What happens if we remove the restriction?
(d) What is the primitive root of a number? Find all the primitive roots of 12.

[5+5+5+5=20]

5(a) What characteristics are needed in a secure hash function?
(b) Assume in an authentication scheme, the hash function used is H and the encryption /decryption function is E/D. Show how the function will be used to provide authentication as well as confidentiality.
(c) Describe the function of "Theta (θ) step" of Keccak-f permutation of NIST standard SHA-3 hash. Mention clearly the structure of input, output.
(d) Describe briefly the stream cipher "Grain" with a proper diagram.

[5+5+5+5=20]