VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

Winter Semester 2023-24

Continuous Assessment Test – II

Course Name & code: Cryptography and Network Security & BCSE309L

Class Number: Common to all batches **Slot: E1 + TE1**

Exam Duration: 90 mins **Maximum Marks: 50**

Answer all the Questions.

1. Alice and Bob want to exchange public keys using the Diffie Hellman approach. They both agree on the prime number p = 17 and the generator g = 7. Alice and Bob choose their private key as Xa = 5 and X_b = 4. Meanwhile, an attacker named Darth intercepts their communication with the private keys X_{DA} = 4 and X_{DB} = 8 to break the communication between Alice and Bob. Calculate and analyze the procedure by which the attacker generates the identical key to gather the information from Alice and Bob. **10**

2. Consider that two communicating parties, UserA and B, agreed to use the Elgamal cryptosystem to secure their conversation. The values used are as follows: A prime number q = 17 and the generator value α = 11. Suppose that User A chose his private key X_A as 6, and User B chose the random integer k as 5. Show the steps involved in key generation, encryption, and decryption for the message M=7. **10**

3. Apply the ECC algorithm to secure the communication for the plain text point P_m= (9, 7). The global public elements used by the user are as follows: Elliptic curve E_{23}(1,1), G= (3,10), and the private key n_A =2, and the secret integer k = 2. Compute the ciphers C1 and C2. (Show the complete calculation.) **10**

4. a. Determine the number of padding bits, total length and number of blocks used in HMAC for the hash functions SHA 512 and MD5 if the input message to be sent is M= 1011011100011110 and the key K = 10111011. **(5 Marks)** **10**

   b. Evaluate the value of Ch (e, f, g), Maj (a, b, c), of SHA512 algorithm for the buffers 'a', 'b', 'c', 'e', 'f', and 'g' that contain the hexa-decimal values as follows: 1111777700001111, FFFF222222221111, BBBB999911112222, CCCC222222220000, 1111DDDD22221111, and 33331111AAAAFFFF, respectively. **(5 Marks)**

5. Person A wants to send a message to Person B. Both agreed to use SHA1 for obtaining the message digest. Let the generated message digest for the message be 4. Both agree on the public key components {p, q, h} as {23, 11, 7}. Person A selects his private key as 3. Let the pseudorandom integer k be 5. Demonstrate the step-by-step calculation for the following: **10**
   - Generate the digital signature using DSS.
   - Signature Verification

Scanned with OKEN Scanner