VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CAT-II, Winter Semester 2018-19 _ KEY

Course Title: Cyber Security (CSE4003)	**Slot : A2**
Duration: 90 Minutes	**Max. Marks : 50**

ANSWER ALL QUESTIONS

1. Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root α=2.

   i).If user A has public key Y_A=9, what is A's private key X_A

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

(ii) We know, $Y_A \equiv \alpha^{X_A} \bmod q$
$\Rightarrow 9 \equiv 2^{X_A} \bmod 11$
$\Rightarrow X_A = 6$ is the required A's private key.

(iii) We have B's public key $Y_B = 3$.
Again, $K_{A,B} = Y_B^{X_A} = Y_A^{X_B} \bmod q$. So, $K_{A,B} = Y_B^{X_A} \bmod q = 3^6 \bmod 11 = 3$ is the required shared secret key between A and B.

b) Alice and Bob wish to share private messages, where each of them of two separate keys generated. What kind of strategy would you suggest to ensure confidentiality, key management and authentication for the conversation between Alice and Bob? Explain the strategy and also highlight the design issues related to the strategy proposed

Dual Encryption (Symmetric and Asymmetric) and MAC

2. (i) What is the padding field for sha-512 if the message is of 1600 bits?
   704 bits padding

(ii) Given the Message= "hai" encode it into message block for SHA 512.

6861698000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000018

(iii) Calculate the value of constant K80 given the 80th prime number is 409.

6C44198C4A475817

3. (a) Suppose Bob uses the RSA cryptosystem with a very large modulus n for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25(A→ 0... Z→ 25), and then encrypting each number separately using RSA with large e

and large n. Is this method secure? If not, describe the most efficient attack against this encryption method.

Consider a set of alphabetic characters {A, B, …, Z}. The corresponding integers, representing the position of each alphabetic character in the alphabet, form a set of message block values SM = {0, 1, 2, …, 25}. The set of corresponding ciphertext block values SC = {0^e mod N, 1^e mod N, …, 25^e mod N}, and can be computed by everybody with the knowledge of the public key of Bob.
Thus, the most efficient attack against the scheme described in the problem is to compute M^e mod N for all possible values of M, then create a look-up table with a ciphertext as an index, and the corresponding plaintext as a value of the appropriate location in the table.

(b) DSA specifies that if the signature generation process results in a value of s = 0, a new value of k should be generated and the signature should be recalculated. Why?

A user who produces a signature with s = 0 is inadvertently revealing his or her private key x via the relationship:

$$s = 0 = k^{-1}[H(m) + xr) \bmod q$$

$$x = \frac{-H(m)}{r} \bmod q$$

4. a. Show that the condition $4a^3+27b^2 \neq 0$ mod p is fulfilled for the curve $y^2 \equiv x^3+2x+2$ mod 17

$$4 \cdot 2^3 + 27 \cdot 2^2 = 4 \cdot 8 + 27 \cdot 4 = 32 + 108 = 140 \equiv 4 \neq 0 \bmod 17$$

b. Is (4, 7) a point on the elliptic curve $y^2 = x^3 + 5x + 5$ over real numbers.

Yes, since the equation holds true for x = 4 and y = 7: $7^2 = 4^3 - 5(4) + 5$

5. a) Alice wants to send a message to Bob. Alice wants Bob to be able to ensure that the message did not change in transit. Briefly outline the cryptographic steps that Alice and Bob must follow to ensure the integrity of the message by creating and verifying a MAC.

Alice i) Generates message M ii) Generates MAC = H(M,K) with M and K as input parameters iii) Sends {M, MAC} to Bob • Bob i) Receives {M', MAC} (message denoted as M' because it's integrity is

uncertain) ii) Generates MAC' from M'. iii) Compares MAC' and MAC iv) If MAC = MAC' then Bob knows message was unchanged in transit

b) Distinguish between HMAC and MAC. How ipad and opad constants used in HMAC? Do they enhance the security of the algorithm?

Message Authentication Code (MAC) is a string of bits that is sent alongside a message. The MAC depends on the message itself and a secret key. No one should be able to compute a MAC without knowing the key. This allows two people who share a secret key to send messages to each without fear that someone else will tamper with the messages

HMAC is a recipe for turning hash functions (such as MD5 or SHA256) into MACs. So HMAC-MD5 and HMAC-SHA256 are specific MAC algorithms. Hash-based message authentication code (HMAC) is a mechanism for calculating a message authentication code involving a hash function in combination with a secret key. This can be used to verify the integrity and authenticity of a message.

Main objective of using distinct constant values for ipad and opad in HMAC while calculating the message digest twice is to avoid cases in which: K+⊕ipad OR K+⊕opad will be a string of zero values.

HMAC more secure because of key and the message are hashed in separate steps.
This ensures the process is not susceptible to extension attacks that add to the message and can cause elements of the key to be leaked as successive MACs are created.

****