AQ – 2926

First Semester M. E. (ENTC) Examination

CRYPTOGRAPHY AND NETWORK SECURITY

Paper – 1 ENTC 5

P. Pages : 4

Time : Three Hours] [Max. Marks : 80

Note : (1) Due credit will be given to neatness and adequate dimensions.
(2) Assume suitable data wherever necessary.
(3) Illustrate your answer wherever necessary with the help of neat sketches.
(4) Use pen of Blue/Black ink/refill only for writing the answer book.

1. (a) Consider a one-time pad version of the vigenere cipher. Solve the following :–

(i) Encrypt the plain text 'sendmore money' with the key stream 9, 0, 1, 7, 23, 15, 21, 14, 11, 11, 2, 8, 9. 8

(ii) Using the cipher text produced in part (i), find a key so that the cipher text decrypts to the plaintext 'Cashnotneeded'.

(b) Prove that $x^i \bmod (x^4+1) = x^{i \bmod 4}$ 6

OR

2. (a) The Merkle-Hellman attack on Triple DES begins by assuming a value of A = 0. Then, for each of the 2^{56} possible values K_1, the plain text P that produces A = 0 is determined. Describe the rest of the algorithm. 7

(b) Suppose the DESF function mapped every 32-bit input R, regardless of the value of the input K, to (a) 32 bit string of one's.
(b) bitwise complement of R. Find.

(i) What function would DES then compute ?

(ii) What would the decryption look like ? Given that.

$(A \oplus B) \oplus C = A \oplus (B \oplus C)$

$A \oplus A = 0; A \oplus 0 = A; A \oplus 1 = \bar{A}.$

Where A, B, and C are n-bit string of bits. 0 is an n-bit string of zeros and 1 is an n-bit string of ones. 7

P.T.O.

3. (a) Suppose Alic and Bob wish to exchange keys, and Darth is the adversary. In man-in-the-middle attack in the Diffie-Hellman key exchange protocol in the adversary generates two public private key pairs for the attack. Could the same attack be accomplished with one pair ? Justify your answer. 6

(b) Develop a suitable elliptic curve encryption / decryption scheme. The cryptosystem parameters are E_{11} (1, 6) and G = (2, 7). B's secret key is $n_B = 7$.

(i) Find B's public key P_B.

(ii) 'A' wishes to encrypt the message $P_m = (10, 9)$ and chooses the random value $k = 3$. Determine the cipher text C_m,

(iii) Show the calculation by which 'B' recovers Pm from C_m. 7

OR

4. (a) Explain the following key control schemes in the key distribution scenario.

(i) Transparent key control.

(ii) Hierarchical key control.

(iii) Decentralized key control. 7

(b) Perform encryption and decrypefrom using RSA algorithm given that p = 11; q = 13; e = 11; M = 7. 6

5. (a) Consider the problem of creating domain parameters for Digital signature algorithm. Suppose we have already found primes p and q such that $q|(p-1)$. Now we need to find $g \in Zp$ with g of order $(q \bmod p)$. Consider the following two algorithms :—

Algorithm 1	Algorithm 2
Repeat	Repeat
Select $g \in Z_p$	Select $h \in Z_p$
$h \leftarrow g^q \bmod p$	$g \leftarrow h^{(p-1)/p}$ mop P
until (h=1 and g≠1)	until (g≠1)
return g	return g

(i) Prove that the value returned by Algorithm 1 has order q

(ii) Prove that the value returned by algorithm 2 has order q

(iii) Suppose p = 40193 and q = 157. How many loop iterations do you expect Algorithm 1 to make before it finds a generator ?

(iv) If p is 1024 bits and q is 160 bits, would you recommend using algorithm 1 to find g. Justify your answer. 6

(b) List the properties of Hash functions. Hence, explain different ways is which a Hash code can be used to provide message authentication. 7

OR

6. (a) Explain the HMAC algorithm using appropriate HMAC structure. Hence suggest changes required in HMAC in order to replace one underlying hash function with another. 7

(b) The high-speed transport protocol XTP (Xpress Transfer Protocol) uses a 32-bit checksum function defined as the concatenation of two 16-bit functions : XOR and RXOR, also defined as "two simple Hash functions."

(i) Will this checksum detect all errors caused by an odd number of error bits.

(ii) Will this checksum detect all errors caused by an even number of error bits. If not, characterize the error pattern that will cause the checksum to fail.

(iii) Comment on the effectiveness of this function for use as a Hash function for authentication. 6

7. (a) Explain the following related to S/MIME.

(i) Functions provided by S/MIME.

(ii) Enhanced security services. 7

(b) Explain the general structure of private and public key ring in case of Pertty Good Privacy (PGP) scheme. 7

OR

8. (a) What is purpose of X.509 standard ? Hence, explain in detail different elements of X.509 certificate. 7

(b) Explain in detail the environmental shortcomings and technical deficiencies of kerberos version G. 7

9. Explain the different phases in lifetime of a typical virus. Hence explain in detail different type of viruses and worms. 13

OR

10. (a) Explain the four techniques used by firewalls to control access and enforce a security policy. 6

(b) What do you mean by guessable passwords ? List and explain in detail the four techniques used to avoid guessable passwords. 7

11. (a) Explain the steps that are involved in the SSL record protocol transmission. 6

(b) In each IPsec implementation, what parameters identify a security association (SA) and what parameters characterize the nature of a partitculare SA ? 7

OR

12. (a) Explain in detail Transport mode and Tunnel mode ESP. 6

(b) Explain the following in respect of web security.

(i) Web security threats.

(ii) Web Traffic security Approaches with their advantages. 7