03533

Printed Pages – 5 CS – 023/IT-701

(Following Paper ID and Roll No. to be filled in your Answer Book)

PAPER ID : 1013 Roll No.

B.Tech.

SEVENTH SEMESTER EXAMINATION, 2005-2006

CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours *Total Marks : 100*

Note : *(i) Attempt **ALL** questions.*

(ii) Be precise in your answer.

1. Attempt *any two* parts : **(10x2)**

(a) (i) Differentiate between the following terms.

(A) Authentication and Authorization

(B) Active attack and Passive attack

(C) Known plaintext attack chosen plaintext attack

(D) Cryptography and Steganography

(ii) Briefly describe the Hill Cipher. If a chosen plaintext attack can be mounted, it is easier to solve Hill Cipher. Describe such an attack.

(b) (i) An organization uses one of the following ciphers at different times to encrypt its data.

Substitution cipher, permutation cipher, DES

Suggest an approach to identify the cipher used to produce the given ciphertext of the organization.

(ii) Justify whether following statement are true or false in context of DES cipher.

(A) It is possible that a plaintext P encrypted with key K_1 can be decrypted with a different key K_2, $(K_2 \neq K_1)$

(B) If key K_1 is complement of key K_2 then ciphertext produced with K_1 will be complement of ciphertext produced with K_2.

(iii) What is avalanche effect ?

(c) (i) Describe Cipher Block chaining mode and cipher feedback mode of operation in reference to DES.

(ii) Briefly explain the principle of differential cryptanalysis.

Attempt *any two* parts of the following : **(10x2)**

(a) (i) Solve the following simultaneous congruence using chinese remainder theorem.

$x \equiv 1 \mod 2$, $x \equiv 1 \mod 3$, $x \equiv 1 \mod 5$, $x \equiv 1 \mod 7$

(ii) Describe RSA public key cipher.

(b) (i) A plaintext m is encrypted twice with the RSA system using two public RSA keys (n,e) and (n,f) and produce ciphertext C_e and C_f respectivley. i.e.

$$C_e = m^e \mod n \text{ and}$$

$$C_f = m^f \mod n$$

Given that gcd (e,f) = 1. Whether an attacker can recover plaintext m ? If yes than how ?

(ii) If G is a finite cyclic group then G has exactly $\phi(|G|)$ generators where is Euler Phi function and $|G|$ is the order of the group G. Prove.

(c) (i) State whether following statement are true or false. Give reasons also.

(A) A commutative ring with unity and without zero divisor is a field.

(B) a and p are relatively prime if and only if $a^{p-1} \equiv 1 \bmod p$.

(ii) Describe Diffie - Hellman algorithm used to exchange secret key between two communicating parties. Explain the algorithm. Show how it is vulnerable to man-in-the middle attack.

(iii) State discrete logarithm problem.

3. Attempt *any two* parts of the following : **(10x2)**

(a) (i) Differentiate between following.

(A) Hash code and Message authentication code (MAC).

(B) Weak collision resistance and strong collision resistance.

(ii) Describe the birthday attack against any hash function. Give the mathematical basis of the attack.

(b) What is digital signature ? What are the requirements for a digital signature ? Describe the digital signature algorithm proposed as part of the digital signature standards (DSS). Give proof of the algorithm. Why each signature requires a new value of K (secret number generated per message in the DSA) ?

(c) (i) Construct an element of order 103 in the multiplicative group of residue mod 1237.

(ii) Compare the MD 5 algorithm with SHA-1 algorithm used for hashing.

(iii) Consider a digital document submission centre (DSC) where students of computer science has been asked to submit their assignment electronically before certain deadline. When an assignment is submitted, DSC puts a timestamp on the document and issues a digital receipt to the student. Earlier is the submission, higher is the grade awarded. Suggest a mechanism that can be implemented for the above purpose. Assume the DSC is not fully trusted by the students.

4. Attempt *any two* parts of the following : (10x2)

(a) What is Kerberos ? Discuss Kerberos version 4 in detail.

(b) What is digital certificate ? Give the format of X. 509 certificate showing the important elements of the certificate. Explain the format.

(c) List the various services supported by PGP. Explain how PGP supports these services. What is the purpose of owner trust field and key legitimacy field in Public Key Ring. How the value of these fields decided ?

5. Attempt *any two* parts of the following : (10x2)

(a) (i) Explain the concept of security association (SA) in IP Sec.

(ii) Describe how authentication header (AH) is used in transport and tunnel modes in IPsec protocol.

(iii) What are the important features of Oakley algorithm used for key determination in context of IP sec.

(b) (i) What is dual signature ? What is the purpose of dual signature ? Explain how a dual signature is constructed.

(ii) Who are the participants in SET (Secure Electronic Transaction) system. Describe in brief the sequence of events that are required for a transaction.

(c) Write short notes on any two of the following.

(i) Firewalls

(ii) Web security threats and SSL

(iii) Viruses and related threats.

- o O o -