aktuonline.com

Printed Pages : 7

TIT-701

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

PAPER ID : 0150 Roll No.

B. Tech.

(SEM. VII) EXAMINATION, 2007-08

CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours] *[Total Marks : 100*

Note :
(i) Attempt ***all*** *questions.*
(ii) ***All*** *questions carry* ***equal*** *marks.*
(iii) Be precise in your answer.
(iv) No ***second*** *answer book will be provided.*
(v) Symbols and abbreviations used in question paper have ***usual*** *meanings.*

1 Answer any **four** parts :

(a) Distinguish between active and passive security attacks. Give some examples of both types of attacks. 5

(b) A Hill cipher uses the following key for enciphering the message. 5

$$k = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$$

Obtain the decryption key to be used for deciphering the ciphertext.

aktuonline.com

(c) Draw a block diagram depicting the structure of a fiestal cipher. List important features of the structure. 5

(d) Explain the principle of differential cryptanalysis. 5

(e) What is Double DES ? What kind of attack on double DES makes it almost useless ? 5

(f) (i) Suppose key scheduling algorithm of DES is modified in such a way that 16 round keys has following relation : **3+2=5**

$k_9 = k_8$, $k_{10} = k_7$, $k_{11} = k_6$, $k_{12} = k_5$, $k_{13} = k_4$, $k_{14} = k_3$, $k_{15} = k_2$, $k_{16} = k_1$.

How will this modification affect the strength of DES ? Explain your answer.

(ii) List various modes of operation of block ciphers. Which of these modes are suitable for parallel processing.

2 Answer any **four** parts :

(a) Given that 2 is a primitive root of 19. Determine all other primitive roots of 19. 5

aktuonline.com

(b) Use Chinese remainder theorem to solve the simultaneous congruences 5

$x \equiv 1 \bmod p$

for all $p \in \{2, 3, 5, 7\}$.

(c) If every element of a group G is its own inverse then group G is commutative. Prove. 5

(d) Suppose we have a set of message blocks encoded with the RSA algorithm and we don't have the private key. Assume n = pq, e is the public key. Some how we come to know that one of the plain text block has a common factor with n. Does this help us anyway to recover plaintext without knowledge of private key ? Does the RSA scheme still works even if plain-text blocks share common factor with n ? Defend your answer. 5

(e) In RSA cryptosystem, given that 5

n = 187, e = 17

Obtain the value of d. Here n,e,d have usual meanings. Show all the steps of your calculation.

aktuonline.com

(f) State the discrete logarithm problem for elliptic curves. Suggest a protocol for key exchange using elliptic curves analogous to Diffie Hellman protocol for key exchange. 5

3 Answer any **two** parts :

(a) (i) List the security services provided by a digital signature. **3+7=10**

(ii) Write the DSS (digital signature standard) scheme of digital signature generation and verification. Prove the correctness of the verifying process.

(b) (i) In reference to DSS scheme of digital signature answer the following : **5+5=10**

(a) Signatures of same message signed twice on different occassions differ. Why ?

(b) During signature generation, one uses message directly in place of hash of the message. What will be security implication of this modification ?

(ii) Give an example of replay attack. What are the approaches used to deal with replay attacks.

 aktuonline.com

(c) (i) Suppose a cryptographic hash function produces a digest of n bits. Prove that one need to create $\sqrt{2 \log_e 2} \cdot 2^{n/2}$ message digests to find two messages having same digest with probability more than $\frac{1}{2}$. **7+3=10**

(ii) In MD5 algorithm, what is the number of padding bits if the length of original message is 2590 bits ? Do we need padding if the length of the original message is already a multiple of 512 bits.

4 Answer any **two** parts :

(a) What requirements were defined for Kerberos ? Name various servers of Kerberos and explain the duties of each server. Write the sequence of message exchanges that happens when a client attempts to obtain a service granting ticket in reference to Kerberoes 4. Explain the steps clearly. **10**

aktuonline.com

aktuonline.com

(b) (i) Explain the purpose of Owner Trust field, Key Legitimacy field and Signature Trust field maintained in the Public key ring of PGP. Why Owner Trust field is not enough to permit PGP to use the corresponding public key ? **6+4=10**

(ii) In PGP, explain how A and B exchange the session key for encrypting messages.

(c) (i) Show the general formats of a X.509 certificate and Certificate Revocation List (CRL). **4+2+2=10**

(ii) Why must a CRL be issued periodically even when no new certificates have been revoked ?

(iii) If there is a revocation mechanism, why do certificates need an expiration date ?

5 Answer any **two** parts :

(a) (1) Define the following terms in context of IPSec and explain their purpose : **6+4=10**

(i) Security Association (SA)

(ii) Security Association Database (SAD)

(iii) Security Policy Database (SPD)

(2) Describe the two methods of IPSec.

aktuonline.com

aktuonline.com

(b) List and briefly define the principal categories of SET participants. Further briefly define the sequence of events that are required for a transaction in a SET (Secure Electronic Transaction) environment. **10**

(c) Write short notes on the following : **5×2=10**

(i) Intrusion detection

(ii) Firewall.

aktuonline.com