1E9104

Roll No. : _____ Total Printed Pages : 4

1E9104

M. Tech. (Sem. I) (Main/Back) Examination, February/March-2011
Computer Science & Engineering
1MCS 4.2 : (Elective - II) Information System Security

Time : 3 Hours] [Total Marks :
[Min. Passing Marks :

Attempt any five questions.
Marks of questions are indicated against each question.
*Draw **neat** and comprehensive **sketches** wherever necessary to **clearly** illustrate your answer.*
*Assume missing **data suitably** if any and **specify** the same.*

Use of following supporting material is permitted during examination.
(Mentioned in form No. 205)

1. Nil 2. Nil

Meaning of Symbols Used :
A = Initiator, B = Responder, KDC = Key Distribution Centre
|| = Concatenation, E(K,M)=Encrypting M with Key=K, ID_i=Identify of B, N = Nonce, R =Random Number.

1 (a) We wish to use the same hardware for AES encryption and decryption . Is it possible ? Justify. 5

(b) Discuss possible defenses against "man-in-the-middle" attack. 5

(c) In DES
(i) Initial permutation and inverse initial permutation on plaintext has no security value.
(ii) Permutation choice-1 for generating the "per round keys" also has no security value.
Accept or reject statement(s) but with reasons. 10

2 (a) Figure shows an authentication protocol similar to that used in Novell Version 3 Security. In the figure, B authenticates the human user A through checking a hash of
A's password as produced by A's workstation. Analyse the strength of this system against (a) eavesdropping and (b) server database disclosure and suggest modifications if required. 10

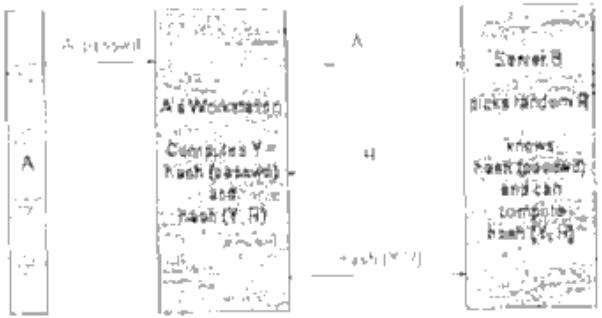

Fig. 1

(b) Figure shows a mutual authentication scheme based on a secret key K_{AB} shared by the communicating parties. Would this protocol be susceptible to a reflection attack ? Justify your answer.

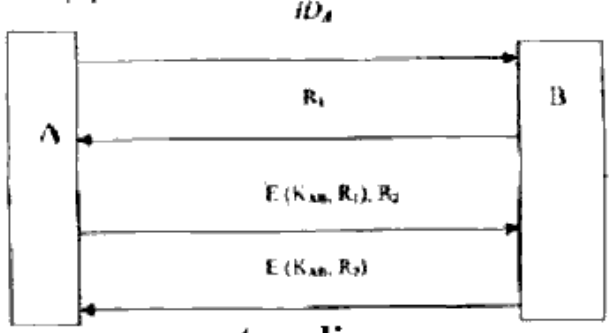

Fig. 2 10

3 (a) Why do many message authentication algorithms such as MD5, SHA-1 pads the input message even if it is integer multiple of the block size? 5

(b) What is birthday paradox ? What is the significance of the paradox in generating message authentication code? 5

(c) Enumerate expressions for generation of signatures and verification of signatures in digital signature standards. Comment on the security of the algorithm. 10

4 (a) What is meant by "Public Key Certificates"? How these certificates are used to distribute public keys? List the messages to be exchanged for distribution of the key. 5

(b) Comment on the security of RSA algorithm against the following attacks :
(i) Brute Force attack
(ii) Mathematical Attack i.e. computing the factors
(iii) Timing Attack
(iv) Chosen Ciphertext Attack
In case of vulnerability against any attack above, what are the countermeasures? 15

5 (a) If there is a revocation mechanism why do certificates need an expiration date? 5

(b) Let two transport mode SAs are bundled to allow both IPSec AH and IPSec ESP protocol on the same end-to-end flow. Which sequence is appropriate: AH before ESP or otherwise. Justify your answer. 7

(c) With suitable diagram and example, explain the processing and transmission of data packets when antireplay mechanism is employed in IPSec. 8

6 (a) How and which key is protected using the passphrase in PGP? Explain the complete process. 5

(b) In PGP, a user has multiple private/public key pairs to encrypt the session key. How does it help in better security? How these keys are managed and the key used for encryption is retrieved? 10

(c) In S/MIME, what the term "Cononical Forms" is used for? What are the different canonical forms used in S/MIME? Describe each form. 5

7 (a) Use of timestamps for prevention of replay attacks is unviable for connection oriented applications and use of challenge/response is not acceptable for connectionless applications. Give reasons. 5

(b) What is meant by a dictionary attack against password? How it can be used to guess the password in Encrypted Key Exchange algorithm? 6

(c) How use of salt improves the security of Lamport's hash? Explain. 4

(d) Lamport's hash is less secure than sending the password across a network. Comment on the correctness of the statement with reasoning. 5

8 (a) Explain the trust model used in PGP? What this model is used for? List the key terms used in the trust model. Also explain the procedure for computing fields used in the trust model. 6

(b) In Secure Electronic Transactions, if we use 3-D security, what changes in payment processing will be required? Explain with neat diagrams. 6

(c) Write notes on the following :
(i) SHTTP
(ii) Secure Socket Layer Handshake protocol. 8
