E4.44 Network Security Specimen Exam Paper 2

Answer 4 questions

Time allowed: 3 hours

1

(i) Fig1.1 shows the round structure for encryption in DES. Express the function of the round by equations relating R_{n+1} and L_{n+1} in terms of R_n and L_n and the Mangler function with key k_n. By manipulating these equations show how L_n and R_n can be obtained from L_{n+1} and R_{n+1} in the decryption process. Finally draw the round structure for decryption.

(ii) Explain how the DES algorithm can be strengthened by 3 DES. What is the effective key length of 3 DES. Explain why a decryption operation is used in 3 DES and why the same effective key length cannot be obtained by the use of just two encryption operations using separate keys.

(iii) Fig 1.2 shows the structure for an odd round in IDEA in which k_6= AC46 and k_{52}= 0000. Explain how the addition and multiplication operations can be reversed in decryption. State what value should be used in place of k_8 in decryption and explain (but do not calculate) how the key to replace k_{52} could be calculated.

(iv) Fig 1.3 shows an even round in IDEA. By analyzing the structure show that the round structure for decryption is the same as that for encryption using the same keys.

2

(i) For any positive integer n what does Euler's Totient function $\phi(n)$ measure? If n = 101 what is $\phi(n)$?

(ii) Explain why the number 3 is a popular choice of public key exponent in the RSA algorithm. If n is the public key modulus and 3 is chosen as the public key exponent, explain why $\phi(n)$ should not be divisible by 3.

(iii) For a message m explain with full mathematical detail how the RSA algorithm can be used to create and verify a signature to the message.

(iv) Explain why in using the RSA algorithm to create signatures it is normal to sign a message digest of the message and not the full message itself. In respect of this application of message digests state the properties of a good message digest function.

3. A small chain of retail outlets wishes to install its own Automated Teller Machines (cash machines) for the exclusive use of its own store cash cards. The cards are of the conventional magnetic stripe variety in which personal information such as account number and credit limit are encoded into the magnetic stripe. The magnetic stripe also contains the result of hashing the personal information with the Personal Identification

Number (PIN) of the card holder so that the PIN can be checked off line. The details of transactions (account, cash withdrawn, time of transaction) are stored in the cash machine until retrieved by the processing centre through a TCP session on the Internet. In addition to the checks provided by TCP, a checksum is computed for the entire file of transactions and sent to the processing centre to ensure total message integrity.

Other details are as follows. The hash function used in the cards was designed by a university mathematics department as part of research sponsored by the store. The processing of data collected from the machines has been outsourced to the same facilities management group that runs the store's stock control and office automation systems.

You have been asked to conduct a security audit of the above operation. State what you perceive as the main potential vulnerabilities of the system described above and the nature of any actions that could be taken to improve confidence in overall security.

4.
(i) Fig 4.1 is a representation of Lamport's Hash. Explain the purpose of this protocol and how it works. Explain what is meant by a "small n attack"

(ii) Fig 4.2 shows a protocol which provide authentication of two endpoints in a communication session. Aside from authentication,what other security feature is exhibited by this protocol?

(iii) Fig 4.3 shows an authentication session which additionally generates a session key. Given that the first two messages are in clear, discuss whether this protocol would be vulnerable to an active or passive attack. If the session key and its component parts are destroyed after the session, discuss whether a later compromise of A's and/or B's database would enable an attacker to decipher a record of all communications.

5
(i) Compare the relative merits of the S/MIME and PGP in respect of
- (a) strength of algorithms employed,
- (b) key distribution and certification, and
- (c) suitability for high value e-commerce

(ii) Explain the terms source authentication, non-repudiation and message integrity in the context of electronic mail security. Explain how you might arrange for all these security features to be included in an electronic mail message using the SHA-1 message digest function and the RSA algorithm.

(iii) Explain how Kerberos V5 provides for "delegation of rights". In what circumstances would it be appropriate to use this feature of V5?

6.
(i) Fig 6.1 is a representation of the OSI Reference Model. Briefly describe how security could be applied at levels 1, 2, 3, 4, and 7.

(ii) Explain what is meant by tunnel mode and transport mode in IPSec. In what circumstances would it be appropriate to use transport mode?

(iii) Explain what security services are provided by AH and ESP in the IPSec protocol.

Specimen 02 Diagrams

Fig 1.1 A DES Round (encryption)

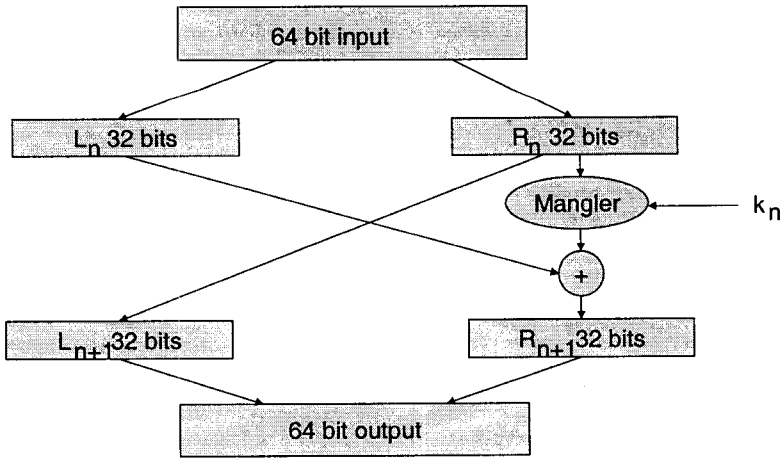

Fig 1.2 IDEA Odd Round

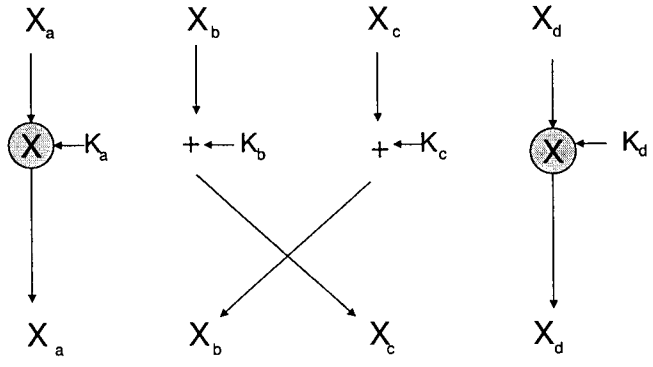

Fig 1.3 IDEA Even Round

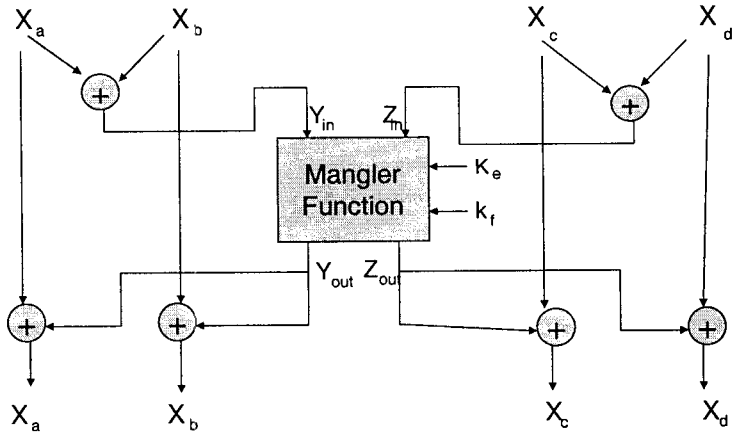

Fig 4.1 LAMPORT'S HASH

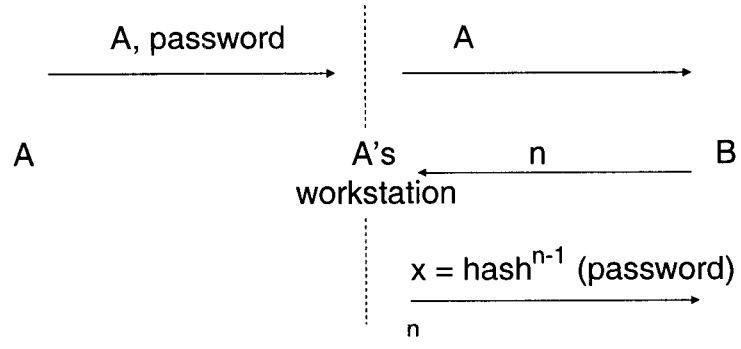

Fig 4.2 Authentication Protocol

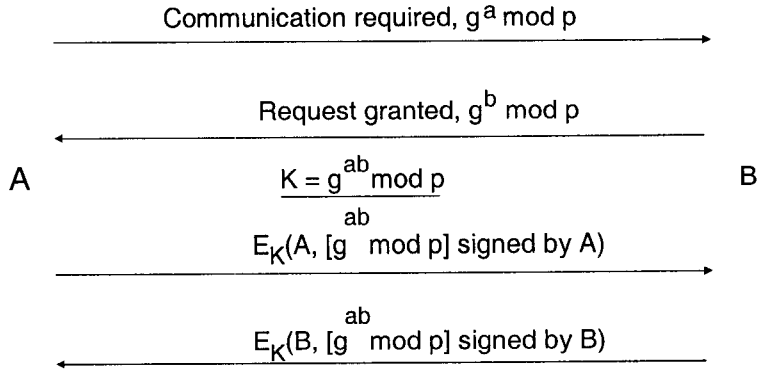

Fig 4.3 Authentication Protocol

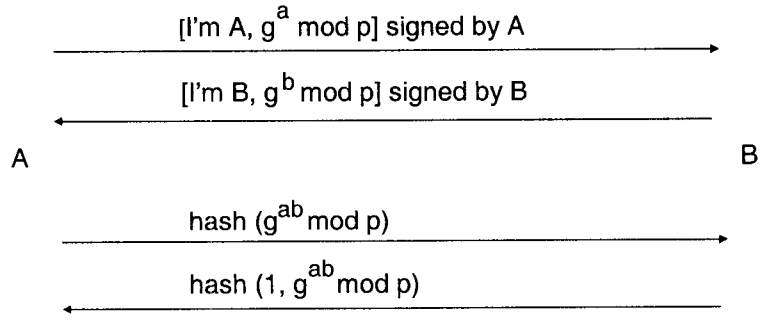

Fig 6.1 OSI Reference Model