E4.44 Network Security Specimen Exam Paper 2 SPRING 2004

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_b= AC46 and k_a= 0000. Explain how the addition and multiplication operations can be reversed in decryption. State what value should be used in place of k_a in decryption and explain (but do not calculate) how the key to replace k_a 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)

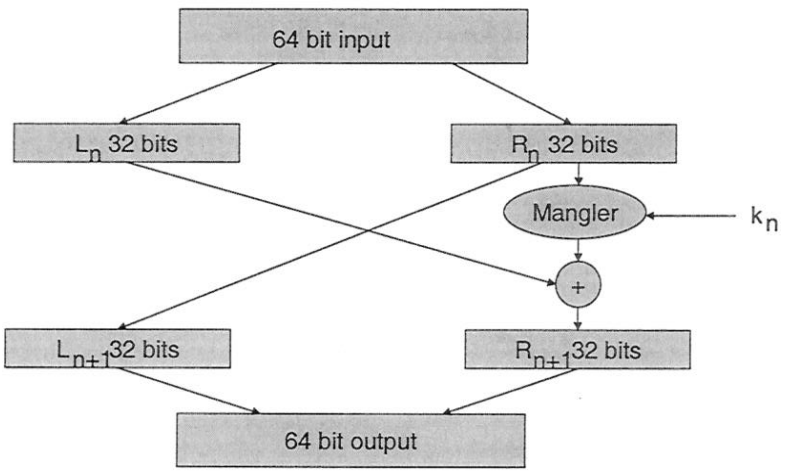


Fig 1.2 IDEA Odd Round

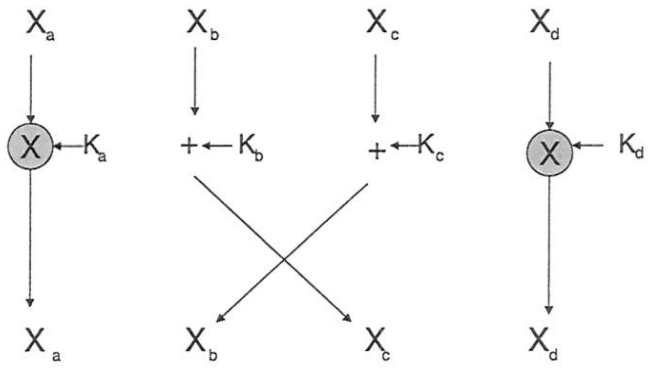


Fig 1.3 IDEA Even Round

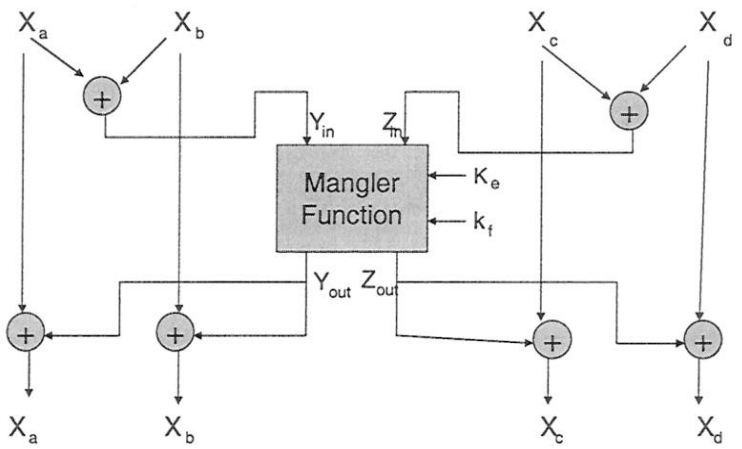


Fig 4.1 LAMPORT'S HASH

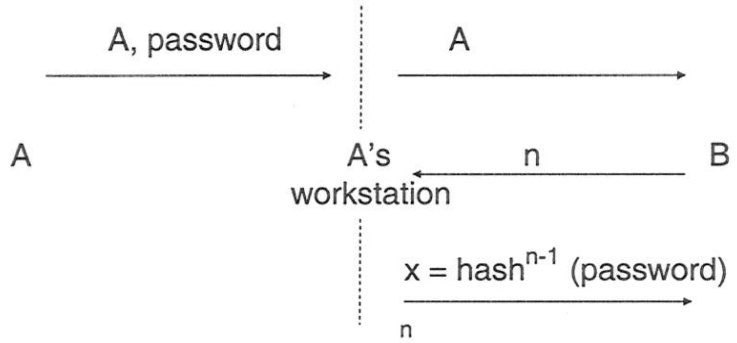


Fig 4.2 Authentication Protocol

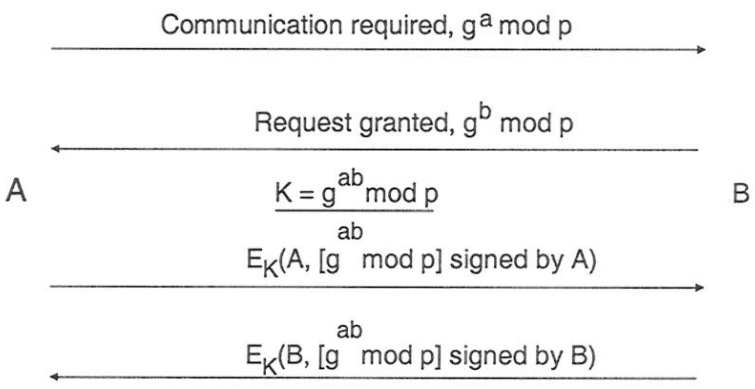


Fig 4.3 Authentication Protocol

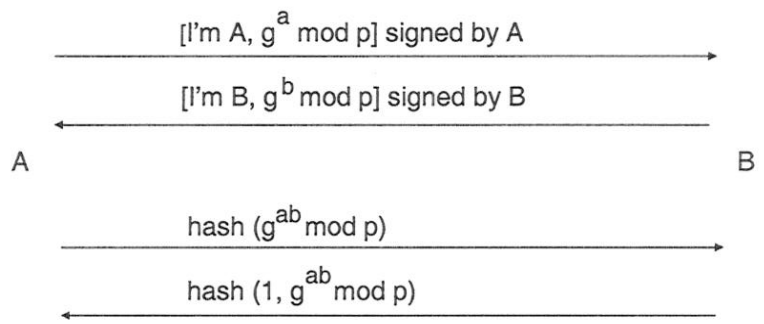
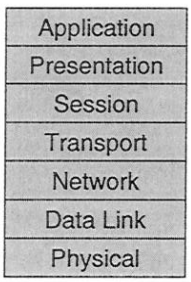


Fig 6.1 OSI Reference Model



E4.44/ISE4.45/SO21 Answers to Sp[pecimen Exam Paper 2

1 (i) From the diagram

L(n+1) = R(n) and R(n+1) = L(n) + Mkn(R(n)) where + denotes bitwise exclusive or

Clearly R(n) = L(n+1) and by adding (exclusive or) Mkn(R(n)) to both sides of the second equation gives L(n) = R(n+1) + Mkn(R(n))
Refer to lecture handout to check your diagram for decryption.

(ii) 3DES is EDE with keys k1, k2 and k1 respectively. Effective key length is 112bits. The second operation is decryption rather than encryption to prevent the final permutation of encryption being reversed by the initial permutation of a second encryption. Two encryptions using k1 and k2 could be attacked by forming tables for a known plaintext/ciphertext pair of 64-bit blocks. The first table would contain the ciphertext for all possible keys used fro encrypting the plaintext. The second table would contain the results of deciphering the known ciphertext with all possible keys. By comparing the results for matches the attacker will find a number of possible matches. These are tried with other known plaintext/ciphertext blocks until a consistent set of matches is obtained. This attack requires considerable storage but is much less computationally intensive than an exhaustive key search.

(iii) Decryption requires the same operations with the additive inverse of kb and the multiplicative inverse of ka. The additive inverse of AC46 is 53BA. 0000 does not have a multiplicative inverse. In order to obtain a multiplicative inverse for this key it is interpreted as 2 raised to the power of 16.

(iv) In the following take + as bitwise exclusive or. In the left hand side of the diagram the output or new Xa = old Xa + Yout and new Xb = old Xb + Yout. Adding (exclusive or) the new Xa and Xb together gives the same result od adding the old Xa and Xb togther as Yout + Yout =0. Therefore if the new Xa nad Xb are introduced to the input they will yield the same Yin which with the same Zin (by a similar argument for the right hand side) must give the same Yout. When this is added to the new Xa it will yield the old Xa. The same applies to Xb, Xc and Xd.

2 (i) Euler's Totient function measures the number of elements in Zn* which is a set of all positive integers less than n which are relatively prime to n. 101 is prime so thast all numbers between 1 and 100 are relatively prime to 101. The totient function is therefore 100.

(ii) 3 is popular because only 3 exponentiations are required for encryption. The private key will be the multiplicative inverse of the public key mod totient function. Therefore for the multiplicative inverse to exist 3 must be relatively prime to the totient function on n. Thus the totient function should not be divisible by 3.

(iii) Refer to lecture handout

(iv) RSA is computationally intensive. Using a message digest to compress the message prior to signature reduces the workload. In respect of this application it should not be computationally feasible to find two messages with the same message digest and given one message and message digest it should not be computationally feasible to find another message with the same digest.

3. The main points about the proposed system are as follows.

The checksum on the magnetic stripe which is used to check the PIN is not a keyed hash. Therefore fake cards could be produced with PINs that check if the hash function is known. Since the hash function was the result of university research it would be difficult to keep secret. Improve by including a secret store key in the hash. The use of a special hash is questionable. It would be preferable to use a standard hash known to have passed the test of time.

The communications through the internet has not been secured. It would be vulnerable to interception in which transactions could be deleted or altered and the attacker would only need to recomputed the TCP checksums and final file checksum. Improve by using IPSec with ESP providing both authentication and privacy. This could be achieved by IPSec outboard devices included within the body of the ATM and in the FM centre.

Processing of the information is conducted at an FM centre. Checks should be made on the security practice at this centre including its personnel policy. The stored data can be used to make replica cards. If an FM centre must be used it would be preferable to use one which has a good record for processing financial data in a secure manner.

4(i) Refer to lecture handouts

(ii) Endpoint Identifier Hiding

(iii) The first exchange is a Diffie Hellman key exchange. An attacker cannot calculate the resulting key by observing the messages. As the messages are signed this gives protection against a bucket brigade attack. In summary it is secure against passive and active attacks.. The protocol exhibits perfect forward secrecy so that if the key and the Diffie Hellman secrets a and b are destroyed a later compromise of either end's database will not yield information by which the communication can be deciphered.

5. (i)

(a) PGP and S/MIME both employ standard algorithms – refer to lecture handouts for details
(b) PGP uses an anarchic system for key distribution and certification. Public keys may be exchanged informally and PGP users are invited to add their own contacts

to directories. A PGP user must make his own decisions in respect to the degree of trust placed in a chain of certificates. S/MIME uses a form of certificate hierarchy which although not as rigid as PEM (e.g. cross links are allowed) is normally based on organizational structure. Refer to lecture handouts for details

(c) S/MIME would be much more suitable for high value e-commerce than PGP. Non-repudiation could ve very important for many high value transactions and therefore there must be trust in public keys.

(ii) Source authentication confirms the name of the originator of the message. Non-repudiation provides the recipient with proof that the message was sent by the originator. Message integrity ensures that the message is received unaltered. Using SHA-1 to form a digest of the message followed by creating a signature of the digest using the private key of RSA could be used to provide all three functions.

(iii) Refer to lecture handouts. The "delegation of rights" feature could be used by a machine organizing an overnight production run in which another machine requires access to data in some part of the process.

6 (i)

Level 1 security can be provided by simple line encryptors
Level 2 security can be provided by protocol sensitive line encryptors
Level 3 security can be provided by IPSec
Level 4 (or more correctly interfacing on top of level 4) security can be provided by SSL
Level 7 security is provided at the application level (e.g. interfacing directly with a payment application)

(ii) Refer to lecture handouts. Transport mode is appropriate for end to end secure communications.

(iii) Refer to lecture handouts