E4.44
SO21
ISE4.45

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2007

MSc and EEE/ISE PART IV: MEng and ACGI

NETWORK SECURITY

Monday, 14 May 10:00 am

Time allowed: 3:00 hours

Corrected Copy

There are SIX questions on this paper.

Answer FOUR questions.

All questions carry equal marks

Any special instructions for invigilators and information for candidates are on page 1.

Examiners responsible First Marker(s) : P.J. Beevor
Second Marker(s) : E. Gelenbe

Special instructions for invigilators

None

Special instructions for students

None

The Questions

1. a) Figures 1.1 and 1.2 show respectively the odd and even encryption rounds of the IDEA algorithm. Explain how decryption can be achieved in each case, justifying your answer with appropriate supporting analysis. [5]

b) If the keys K_a, K_b, K_e and K_f in Figures 1.1 and 1.2 are respectively *0A24, B2C7, 5C89* and *289D* determine the relative keys required for decryption. [7]

c) Figure 1.3 shows the *MixColumn* operation of an AES encryption round. Explain the process shown in Figure 1.3, stating whether the operation should be considered a permutation or substitution in the block cipher. Explain further how the relative decryption operation can be achieved, justifying your explanation with appropriate analysis. [6]

d) In an operation with the AES cipher it is required to find the inverse polynomial of $x^4 + 1$ modulo $x^8 + x^4 + x^3 + x + 1$, both polynomials being over Z_2. Explain how Euclid's algorithm can be used to find the inverse polynomial of $x^4 + 1$, illustrating your answer by completing the first two calculated rows of Euclid's algorithm (you are not required to find the inverse polynomial). How would this operation be achieved in a practical implementation of AES? [7]

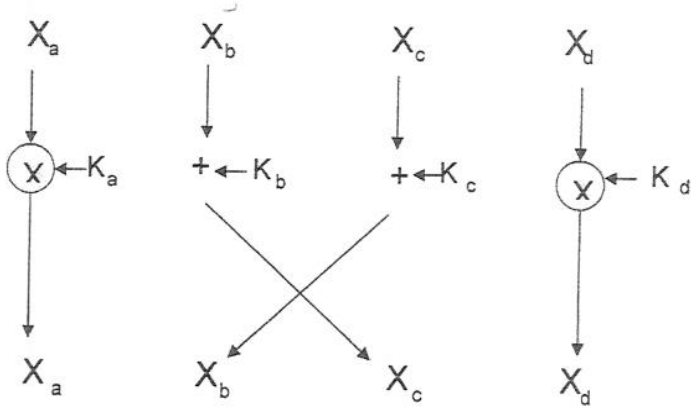

Figure 1.1 IDEA Odd Round

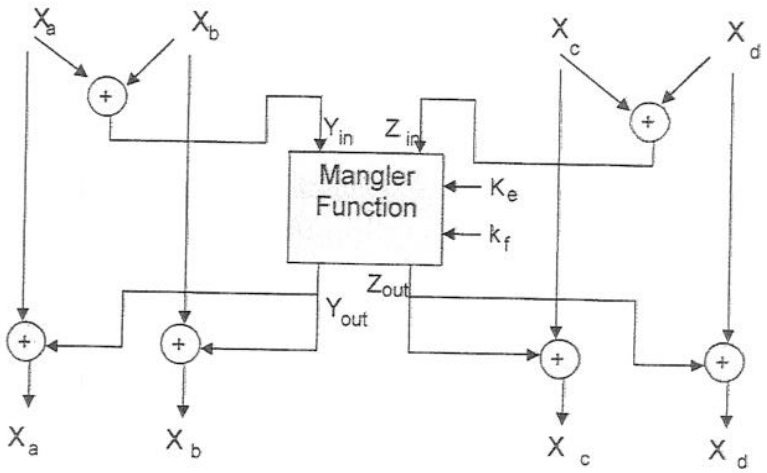

Figure 1.2 IDEA Even Round

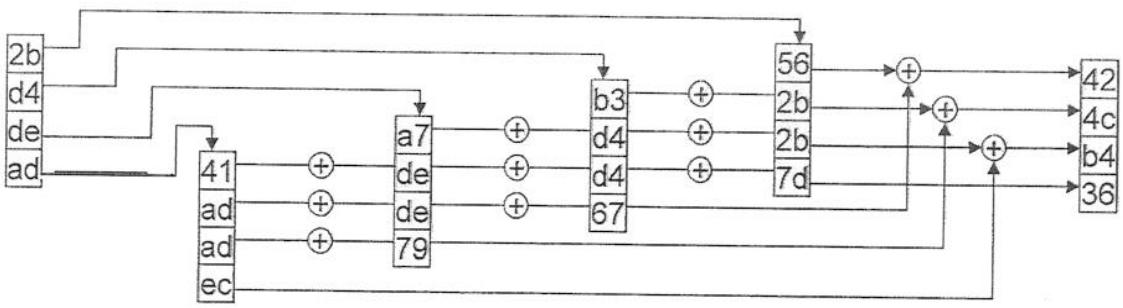

Figure 1.3 Mix Column Operation in AES

2. a) In the RSA system of public key cryptography, a principal with another's public key pair (e, n) encrypts a plaintext message m to form the ciphertext $c = m^e \bmod n$.

i) Explain in detail how the intended recipient of the message may use his private key to recreate the message m. [4]

ii) Explain how an attacker provided with unrestricted computing resources could retrieve the plaintext. [4]

iii) What restrictions must be placed on the length of the message m to ensure that it can be unambiguously deciphered? [2]

iv) If the message m is one of a limited number of standard messages that may be sent, what would be the most efficient method for the attacker to decipher the plaintext? [3]

b) The triple DES (3DES) system of cryptography uses 3 standard DES operations (encrypt – decrypt – encrypt or EDE) to convert plaintext into ciphertext.

i) What is the standard message block size used in 3DES? [2]

ii) What is the effective key length of a 3DES system? [2]

iii) What are the advantages of using the DES operations EDE over other possible combinations of 3 standard DES operations? [3]

iv) If only two standard DES encrypt operations (EE) are used to increase the effective key length of DES, what method of attack may be used to ensure that the intended increase in key length is not achieved? [5]

3. a) Discuss what properties should be present in a good message digest function. Suggest two applications of such a function, and explain in each case why these properties are essential. [6]

b) In the context of message digest functions, explain what is meant by the 'birthday paradox'. What are the implications of the 'birthday paradox' for the length of the message digests currently in use? [5]

c) Figure 3.1 shows the outline design of the message authentication code known as HMAC which uses 'Secure Hash Algorith-1' (SHA-1). Explain why the design uses two separate paths to form the final message authentication code. [7]

d) In order to reduce the complexity of HMAC a simpler design is proposed. In this design the message is divided into 160-bit blocks and each block forms one input into a stage of the digest for which the other input is the 160-bit output of the previous stage. In each stage of the digest the current 160-bit message block is rotated 32 bits to the left and added modulo-2 to the output of the previous stage. The result is the output of that stage.

Discuss whether this design would exhibit the properties of a good message digest function, and, if not, propose a method by which such a system could be attacked. [7]

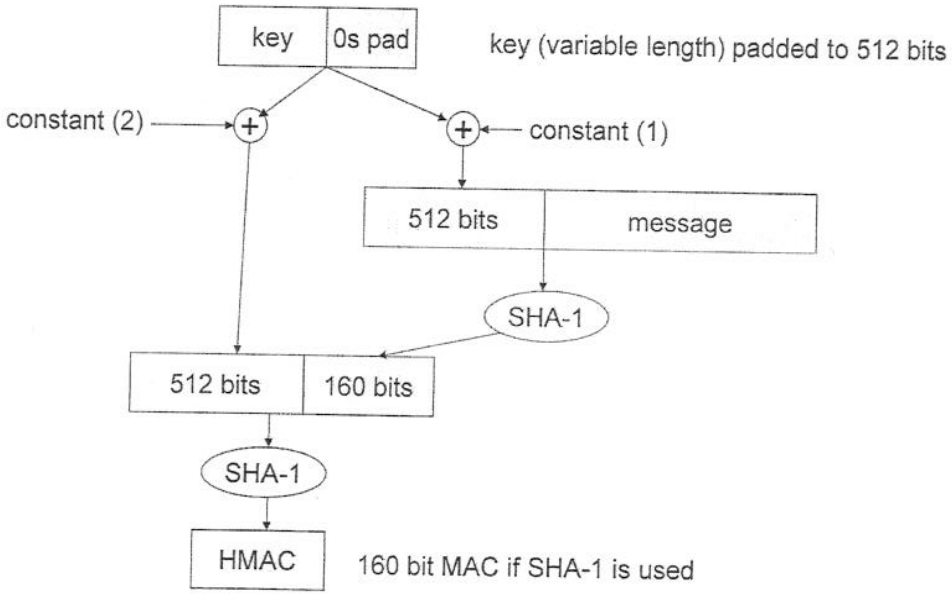

Figure 3.1 Outline Design of HMAC

4. a) What is the function of the Key Distribution Centre (KDC) in the Kerberos system of network security? What feature of the design of the KDC is intended to ensure high availability? How is secure communication achieved between two principals which are not connected to the same KDC? [5]

b) Describe three differences between Kerberos V4 and Kerberos V5. What features of V5 not present in V4 should be of interest to an IT manager of a major business? [5]

c) Explain what is meant by 'Perfect Forward Secrecy' (PFS) and describe one method by which it may be achieved. Does Kerberos (V4 or V5) exhibit PFS? [5]

d) In the context of the 7-layer OSI Reference Model of communications describe how security may be established at layers 1, 2, 3, 4 and 7 and describe briefly the issues involved with layers 1, 2, and 7. [5]

e) If secure communication is required between two principals connected to the same IP network, and the security systems available are IPSec and TLS, discuss the security requirements that would make IPSec the chosen option. [5]

5. a) Two principals which share a secret one-time pad are connected through an optical fibre link. Explain how quantum cryptography can be used to establish totally secure communication between the principals. Explain further how quantum cryptography can be used to establish the shared secret one-time pad without the use of any techniques from conventional cryptography. [10]

b) A government wishes to issue identify cards to its citizens using smart card technology with the data secured by conventional cryptography. In order to make use of local knowledge to confirm an individual's identity, a large number of reception centres are set up in local government offices. The applicant is interviewed in the reception centre, and biometric and other personal data is collected. This data is sent through the internet to a central government office and is protected through the internet by means of an IPSec VPN. The central office sends the data to a specialist contractor (part of a multi-national group) together with a 512-bit government RSA key which is intended to be used to create a signature on the personal data. The contractor is responsible for producing the identity cards, which may be checked for validity by comparing the biometric data in the card with that exhibited by the cardholder, and by verifying the government signature on the personal data.

The government wishes to recover the cost of developing and manufacturing the identity cards with a high charge to its citizens, and, to aid its introduction, the government guarantees a card lifetime of 20 years.

You are a security consultant invited by the government to audit the proposed scheme. What would be your major concerns about security, and what additional information would you require to undertake an effective audit? [15]

6. a) Explain how a firewall, placed between a corporate LAN and the internet, can be configured to provide the following protection:

i) allow all communications except that using the TELNET protocol;

ii) allow all file transfer communications initiated from within the LAN but block all similar communications initiated from outside the LAN. [5]

b) What is meant by a 'denial of service attack'? What techniques are available to protect vulnerable servers on the internet from such attacks? [5]

c) What features should be exhibited by a good public key infrastructure (PKI)? Describe in outline the PKIs employed by 'Privacy Enhanced Mail' and 'Pretty Good Privacy'. [5]

d) Explain what is meant by a 'replay' attack and provide an example where such an attack would be possible. Explain further how a modification to your example would serve as protection against such an attack. [5]

e) i) In the context of email security explain what is meant by 'non-repudiation'. Explain further why the property of non-repudiation is important in e-commerce applications. [2]

ii) One party on an email system wishes to send securely the same email to 100 recipients on the same email system. All parties to the communication are provided with standard systems of secret (e.g. DES, IDEA, etc.) and public (e.g. RSA) key cryptography. Propose an efficient way for the broadcast email to be sent. [3]