

1. (a) Figure 1.1 shows the results of applying Euclid's algorithm to find the greatest common divisor of 65,537 and 300. State what is the greatest common divisor. What property does the number 300 exhibit in relation to 65,537? [4]
- (b) For any positive integer n what does Euler's Totient Function define? If $n = 13p$, where p is a prime number, calculate $\Phi(n)$. [4]
- (c) Figures 1.2 and 1.3 illustrate the odd and even rounds of the International Data Encryption Algorithm (IDEA). Explain how these rounds could be reversed in the decryption process. [4]
- (d) In the fifth and sixth rounds of an IDEA encryption the following keys are used in the notation shown in figures 1.2 and 1.3:

$$K_a = 6C60, K_b = 02A1, K_c = 8D4F, K_f = 92BD$$

Find the equivalent keys for the process which decrypts these rounds.

[9]

- (e) Compare the security strengths of DES and IDEA.

[4]

n	q_n	r_n	u_n	v_n
-2		65,537	1	0
-1		300	0	1
0	218	137	1	-218
1	2	26	-2	437
2	5	7	11	-2403
3	3	5	-35	7646
4	1	2	46	-10,049
5	2	1	-127	27,744
6	2	0	300	65,537

Figure 1.1 Euclid's Algorithm

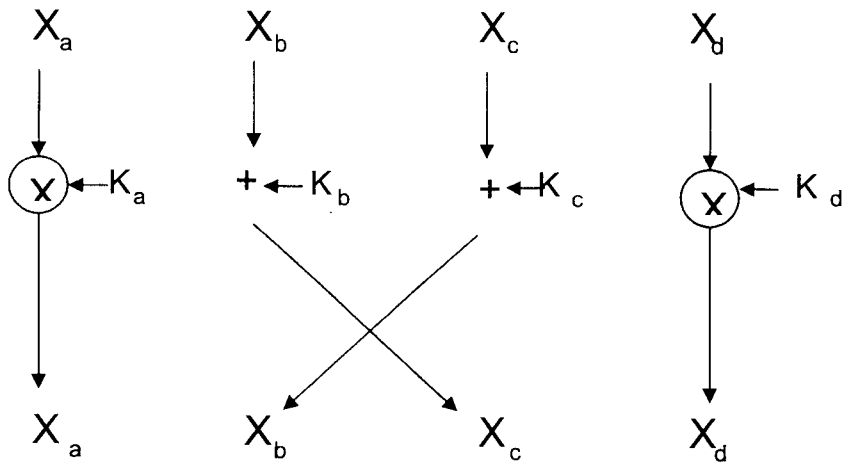


Figure 1.2 IDEA Odd Round

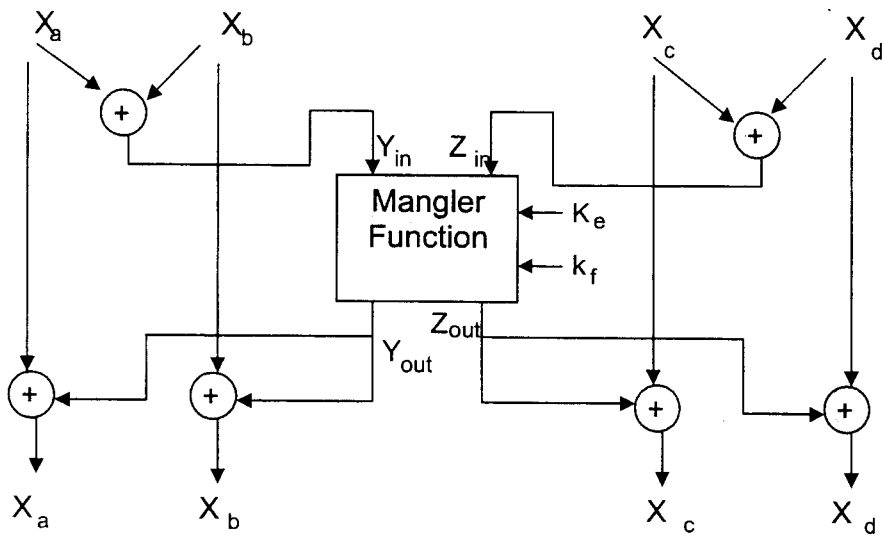


Figure 1.3 IDEA Even Round

2. (a) Explain how the RSA algorithm provides encryption and decryption. Suggest a practical way of finding private/public key pairs. [6]
- (b) Explain why the numbers 3 and 65,537 are popular choices for the public key exponent in the RSA algorithm. Explain how several principals may have the same public key exponent but different private keys. [6]
- (c) What are the benefits of following the Public Key Cryptography Standard (PKCS) when applying RSA encryption? When the RSA algorithm is employed to create a signature for a long message, why is it usual to use a message digest function prior to the application of the RSA algorithm? [5]
- (d) In the following examples the RSA algorithm is used in a straightforward manner (i.e. without reference to PKCS). Explain how each implementation could be attacked, and suggest how protection could be applied in each case.
- (i) The same message, encrypted under the recipient's public key, is sent to three recipients each of which use 3 as their public exponent. [3]
- (ii) A short message, encrypted under the recipient's public key, and less than a third in length of the public key modulus, is sent to a recipient whose public key is 3. [3]
- (iii) A message which could be one of ten known messages is sent to a recipient encrypted under that recipient's public key. [2]

3. (a) State and explain the properties of a good message digest function. [5]
- (b) Describe how a SHA-1 message digest is created (a detailed description of the SHA-1 round structure is not required) [5]
- (c) Explain how the SHA-1 message digest function may be used to calculate a cryptographic Message Authentication Code (MAC). What precautions should be taken to prevent an attacker being able to alter the message to recalculate a valid MAC. [5]
- (d) The following is proposed as a message digest function intended to be used in a process which calculates a MAC for a long message.

Firstly, the message is padded to be a multiple of 160 bits. Each 160-bit sequence is represented by 5 32-bit words. The first words are added together modulo ~~232~~ 2^{32} to form a final 32-bit word as shown in Figure 3.1. The five final 32-bit words are combined bitwise exclusive-or to form a 32-bit MAC. Discuss how the proposed system could be attacked.

- (e) Why would a 32-bit MAC be considered insufficiently secure irrespective of what was used to create it? [2]

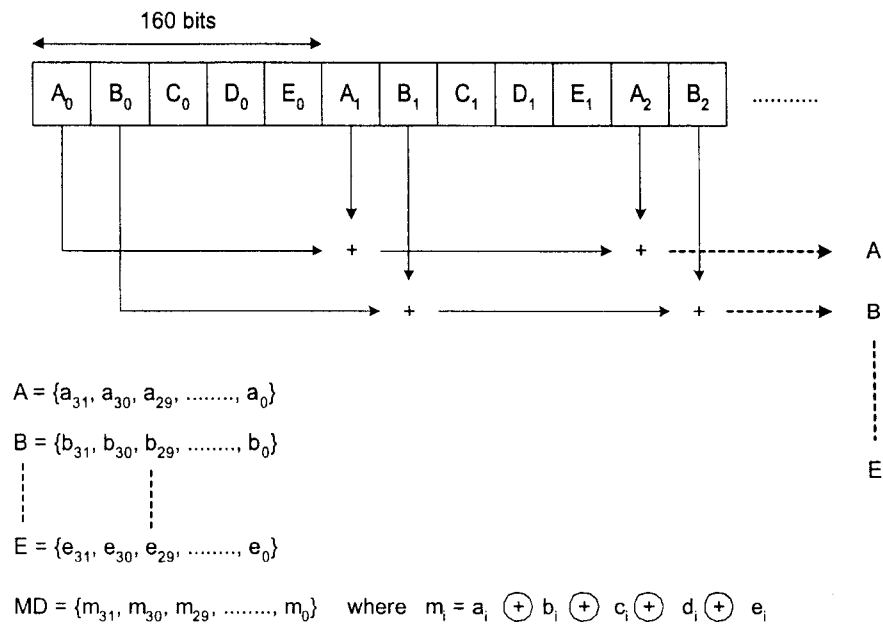


Figure 3.1 Message Digest

4. (a) What function could the Kerberos system provide in a distributed computing application on the Internet? What is the purpose of a session key in Kerberos? [4]
- (b) Explain the function of a ticket, a ticket granting ticket and the KDC master key in Kerberos. [6]
- (c) What additional functionality is provided by Kerberos V5 compared with Kerberos V4? Why is it necessary to store more key versions in V5 than in V4? [10]
- (d) Figure 4.1 shows the remote login procedure in Kerberos in which a workstation A makes an application request to server B. What is the purpose of the encrypted timestamp sent by A to B? Why does B reply with an encrypted version of timestamp + 1? [5]

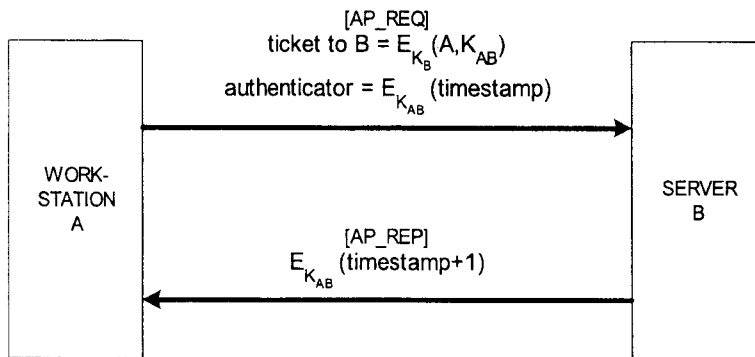


Figure 4.1 Remote Login in Kerberos

5. (a) In the context of electronic mail briefly explain the following terms:
- (i) non-repudiation
 - (ii) proof of submission
 - (iii) message flow confidentiality
 - (iv) message sequence integrity
- [4]
- (b) Discuss the relative merits of the schemes used for key distribution and certification in PEM, S/MIME and PGP.
- [7]
- (c) Explain what is meant by “perfect forward secrecy” and describe any method by which it may be implemented
- [7]
- (d) Explain the term “denial of service/clogging protection” and describe a way in which such protection could be implemented in a real-time communication security system.
- [7]

- 6 (a) In respect of the position of the security function in the OSI Reference Model, discuss the relative methods used by IPSec and SSL in real-time communication security. [6]
- (b) Explain the terms AH and ESP as employed in the IPSec protocol. Discuss whether both implementations are necessary for secure communications on the Internet. [6]
- (c) Figure 6.1 is an illustration of the cipher block chaining (CBC) encryption technique. Explain the following: [6]
- (i) the function of the Initialisation Vector (IV), and
 - (ii) how the resultant ciphertext can be altered to effect a specific change in a known plaintext.
- (d) Assuming the CBC system shown in Figure 6.1, explain how message privacy and integrity can be achieved by using
- (i) a single CBC run with one key, and
 - (ii) two CBC runs each with a separate key.

Compare the security strengths of the two methods.

[7]

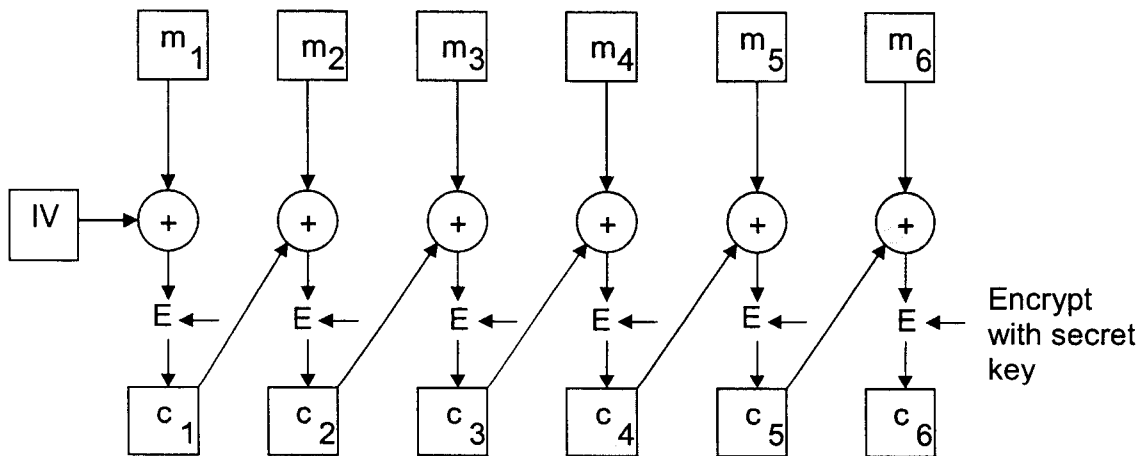


Figure 6.1 CBC Encryption