Q.2 a. Find the multiplicative inverse of 7 in Z_{180} using the extended Euclidean algorithm. (6)

Answer:

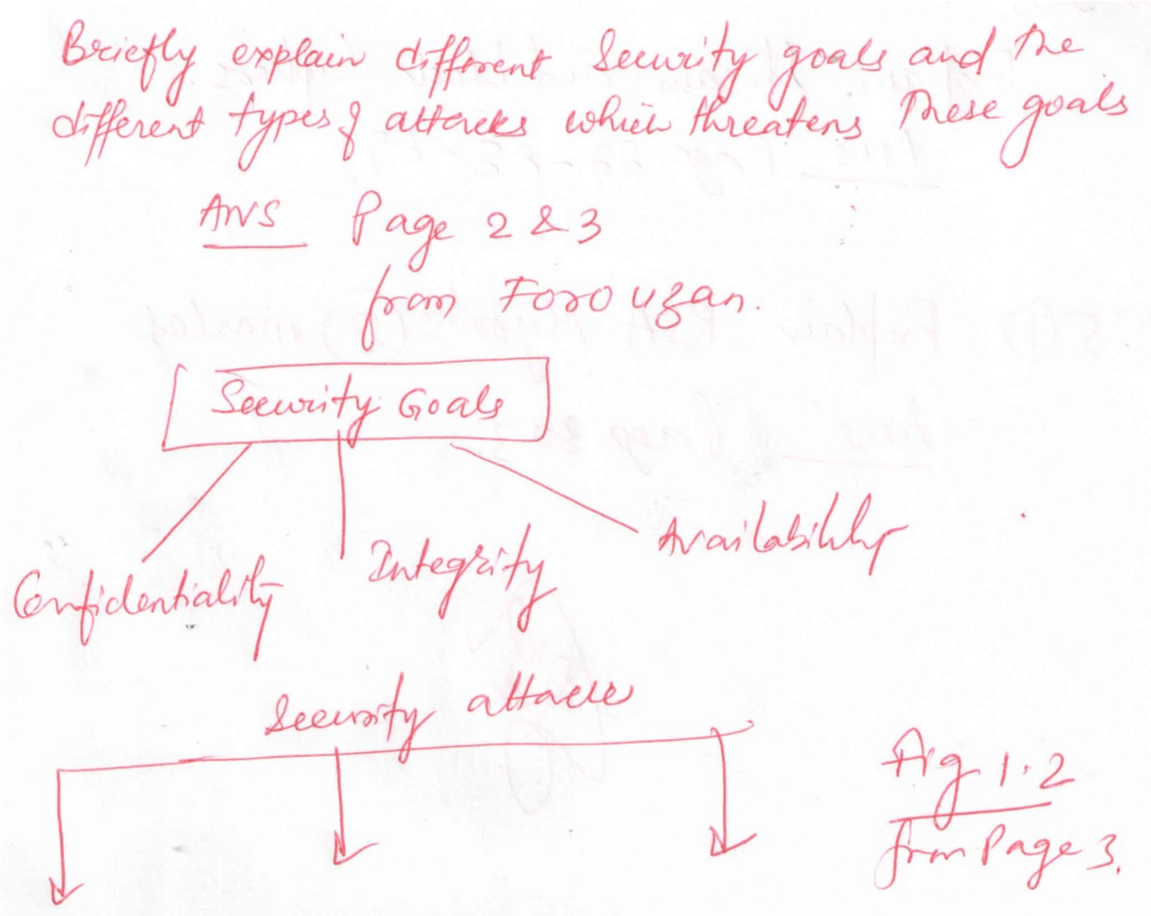
The multiplicative inverse is obtained from the following table.

Q	R1	R2	R	T1	T2	T
2.5	180	7	5	0	1	-25
1	7	5	2	1	-25	26
2	5	2	1	-2.5	26	-77
2	2	1	0	26	-77	180
-	1	0	-	-77	180	-

The gcd of 180 and 7 is 1. The multiplicative inverse is -77 mod 180 = 103.
7 and 103 are multiplicative inverses.

b. Briefly explain different security goals and the different types of attacks which threatens these goals. (10)

Answer:



Briefly explain different Security goals and the different types of attacks which threatens these goals

Ans Page 2 & 3 from Forouzan.

Security Goals

Confidentiality Integrity Availability

Security attacks

Fig 1.2 from Page 3.

Q.3 a. Explain, what do you understand by substitution ciphers? Explain one mono alphabetic cipher with suitable examples. (8)

Answer:

Page 61-63 from Book 1.

For explanation of substitute cipher award 3 marks. For explanation of any mono alphabetic cipher like additive cipher, shift cipher or any other cipher with example award 5 marks.

b. Explain stream and block ciphers. (8)

Answer:

Page 87-88-89

Q.4 a. Draw the general structure of Data Encryption Standard (DES) algorithm and briefly explain its operation. (8)

Answer: Page No. 161-162

Award 3 marks for correctly drawing the block diagram and 5 marks for explanation of each of the boxes. (Detailed explanation is not expected)

b. Explain the principle behind initial and final permutation steps of Data Encryption Standard algorithm. (8)

Answer: Diagram of initial and final permutation, clearly reversing the steps- award 5 marks. Explanation of other details award 3 marks.

Q.5 a. Draw the block diagram of Cipher Block Chaining (CBC) mode to encipher text of any size. Explain the details of the operation. (8)

Answer: Page No.228-230

For drawing the block diagram of encryption and decryption give 6 marks. For explanation of initial value (IV), size in bits, operation of the CBC mode award 10 marks.

b. Explain RSA Algorithm. (8)

Answer:

Page 303

Q.6 a. Distinguish between message integrity and message authentication. (8)

Answer:

Detailed explanation integrity and authentication with about five clear comparisons award 8 marks. For lesser comparisons award proportionately low marks.

b. Define the criteria for cryptographic hash function. (8)

Answer: Page No. 340-342

The characteristics of hash functions are

-- maximum message size
-- block size
-- message digest size
-- number of rounds
-- word size

For explaining the meaning of the above 5 criteria give 8 marks. Reduce marks proportionately for explanation of lesser number of criteria.

Q.7 a. Distinguish between conventional signature and digital signature. (5)

Answer:

Three differences to be given. Give one mark for clearly explaining each difference.

b. What are the attacks on digital signatures? Explain briefly. (5)

Answer: Page No. 389-396

The attacks on digital signatures are:

-- key only attack

--known message attack

-- chosen message attack

Award 5 marks for explaining all the three types of attacks.

c. Describe the possible attacks on Diffiie Hellman key exchange mechanism. (6)

Answer: Page No. 449-450

The attacks on Diffie Hellman exchange mechanisms are:

-- discrete logarithm attack

-- man in the middle attack

Award 3 marks for explaining each of the above attacks.

Q.8 a. Explain the details of private key ring table and public key ring table maintained by each user. (10)

Answer: Page No. 477-479

Private key ring has 5 fields: user ID, key ID, public key, encrypted private key and time stamp. Explaining the details of these five fields award 4 marks. Public key ring table has 8 fields: user ID, key ID, public key, producer trust, certificate(s), certificate trust(s), key legitimacy and time stamp. Brief explanation of these 8 fields award 6 marks.

b. How does information needed for sending and receiving messages is extracted from the set of key rings maintained? (6)

Answer:

Details of extraction of a message from the rings at sender site and receiver site is required to be given. Award 6 marks for these details.

Q.9 a. What are the protocols defined in secure socket layer? (8)

Answer: Page No. 517

The four protocols defined in secure socket layer are:

- Handshake protocol
- Change cipher spec protocol
- Record protocol
- Alert protocol

Award 2 marks for listing the protocols.

b. Compare and contrast the handshake protocols in secure socket layer (SSL) and transport layer security (TLS). (8)

Answer: Page No. 518

Comparing the hand shake protocol and record protocol in the two layers with detailed explanation: award 7 marks each.

TEXT BOOK

Behrouz A. Forouzan, Cryptography & Network Security, Special Indian Edition