Biyani's Think Tank

Concept based notes

Network Security and Cryptology

(BCA Part-III)

Priyamvada Pareek
Revised By: Ms Rashmi Sharma
Lecturer
Deptt. of Information Technology
Biyani Girls College, Jaipur

Biyani's
Group of Girls' Colleges

Published by :

Think Tanks
Biyani Group of Colleges

Concept & Copyright :

©Biyani Shikshan Samiti
Sector-3, Vidhyadhar Nagar,
Jaipur-302 023 (Rajasthan)
Ph : 0141-2338371, 2338591-95 • Fax : 0141-2338007
E-mail : acad@biyanicolleges.org
Website :www.gurukpo.com; www.biyanicolleges.org

ISBN: 978-93-82801-81-8

First Edition : 2009
Second Edition: 2010
Price:

While every effort is taken to avoid errors or omissions in this Publication, any mistake or omission that may have crept in is not intentional. It may be taken note of that neither the publisher nor the author will be responsible for any damage or loss of any kind arising to anyone in any manner on account of such errors and omissions.

Leaser Type Setted by :

Biyani College Printing Department

Preface

I am glad to present this book, especially designed to serve the needs of the students. The book has been written keeping in mind the general weakness in understanding the fundamental concepts of the topics. The book is self-explanatory and adopts the “Teach Yourself” style. It is based on question-answer pattern. The language of book is quite easy and understandable based on scientific approach.

Any further improvement in the contents of the book by making corrections, omission and inclusion is keen to be achieved based on suggestions from the readers for which the author shall be obliged.

I acknowledge special thanks to Mr. Rajeev Biyani, *Chairman* & Dr. Sanjay Biyani, *Director* (*Acad.*) Biyani Group of Colleges, who are the backbones and main concept provider and also have been constant source of motivation throughout this Endeavour. They played an active role in coordinating the various stages of this Endeavour and spearheaded the publishing work.

I look forward to receiving valuable suggestions from professors of various educational institutions, other faculty members and students for improvement of the quality of the book. The reader may feel free to send in their comments and suggestions to the under mentioned address.

Note: **A feedback form is enclosed along with think tank. Kindly fill the feedback form and submit it at the time of submitting to books of library, else NOC from Library will not be given.**

Author

Syllabus

B.C.A. Part-III

Network Security And Cryptology

Introduction : Goals and settings, The symmetric setting, The asymmetric setting. Other goals Pseudorandom Number Generation, Authenticated key exchange, Coin flipping, What cryptography is about, Protocols, parties and adversaries, Cryptanaly and computer security the rules of the game, Approaches to the study of cryptography, Phases in the cryptography's Development, Cryptanalysis-driven design, Shannon security of symmetric encryption, Computertational complexity theory, Atomic primitives, what background do I need? , Historical notes, problems.

Block Ciphers : What is a block cipher? Data Encryption Standard (DES) Key recovery attacks on block ciphers, Iterated DES and DESX, Advanced encryption Standard (AES), Limitations of recovery key based security, Problems.

Pseudorandom Functions : Function families, Random functions and permutations, Pseudorandom Functions, Pseudorandom permutations, Modeling block ciphers, Example attacks, Security against key recovery, The birthday attack, The PRP/PRF switching lemma. Historical notes.

Symmetric Encryption : Some Symmetric Encryption schemes, Issues Iqn privacy, Indistinguishability under chosen-plaintext attack, Example chosen-plaintext attacks, INF-CPA implies PR-CPA, Security of CTR modes, Security of CBC with a random IV, Historical notes.

Hash Functions : The hash function SHAI, Collision resistant hash functions, Collision, attacks. One-way ness of collision resistant hash functions, Polynomial evolution is an almost universal hash, function, The CBC MAC function, Collision-resistance under hidden-key attack.

Message Authentication : The setting, Privacy does not imply authenticity, Syntax of message-authentication schemes a definition of security for MACs , The PRF-as-a MAC paradigm, The CBC MACs.

Number-Theoretic Primitives : Introduction to discrete algorithm related problems, The choice of group; The RSA system, Historical notes.

Asymmetric Encryption : Asymmetric encryption schemes, Notions of security, one encryption query or many? Hybrid encryption, El Gamal scheme and its variants.

Digital signatures : Digital signature schemes, A notion of security, RSA based signatures.

□ □ □

Content

□ □ □

Chapter-1

Introduction

Q.1. What do you understand by Network Security?

Ans.: The use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer. Network Security measures needed to protect data during their transmission. In fact, the term network security is defined as :

1) The authorization of access to files and directories in a network. Users are assigned an ID number and password that allows them access to information and programs within their authority. Network security is controlled by the network administrator.

2) Protecting a network from unwanted intruders.

The **goals** of network security are :

- Privacy
- **Authentication :** Authentication mechanisms are used to establish trust between online entities
- Availability
- **Integrity :** integrity mechanisms are used to verify correctness of online exchanges and/or data.

Q.2. Define Cryptography. Define approaches and phases in Cryptography Development.

Ans.: An original message is known as the plaintext, while the coded message is called ciphertext. The process of converting plaintext to cyphertext is known as enciphering or encryption: restoring the plaintext from the ciphertext is deciphering or decryption. The many schemes used for enciphering constitute the area of study known as cryptography.

Cryptographic key recovery system that operates in two phases.

In the **first phase**, the sender establishes a secret value with the receiver. For each key recovery agent, the sender generates a key-generating value as a one-way function of the secret value and encrypts the key-generating value with a public key of the key recovery agent.

In the **second phase**, performed for a particular cryptographic session, the sender generates for each key recovery agent a key-encrypting key as a one-way function of the corresponding key-generating value and multiply encrypts the session key with the key-encrypting keys of the key recovery agents. The encrypted key-generating values and the multiply encrypted session key are transmitted together with other recovery information in a manner permitting their interception by a party seeking to recover the secret value. To recover the secret value, the party seeking recovery presents the encrypted key-generating values and public recovery information to the key recovery agents, who decrypt the key-generating values, regenerate the key-encrypting keys from the corresponding key-generating values, and provide the regenerated key-encrypting keys to the recovering party. The recovering party uses the key-encrypting keys to recover the secret value. Since the key-generating values cannot be derived from the key-encrypting keys, they may be used over a period spanning multiple cryptographic sessions without requiring new values or new public key encryptions.

□ □ □

Chapter-2

Block Cipher

Q.1. Write Short notes on -

(1) Iterated DES

(2) Data Encryption Standard

(3) DESX

(4) Advanced Encryption Standard

Ans.: (1) Iterated DES : A block cipher that "iterates a fixed number of times of another block cipher, called round function, with a different key, called round key, for each iteration".

Most block ciphers are constructed by repeatedly applying a simpler function. This approach is known as *iterated block cipher*. Each iteration is termed a *round*, and the repeated function is termed the *round function*; anywhere between 4 to 32 rounds are typical.

(2) Data Encryption Standard :A16-round Feistel cipher with block size of 64 bits. DES stands for Data Encryption Standard.

DES was developed by IBM in 1974 in response to a federal government public invitation for data encryption algorithms. In 977, DES was published as a federal standard, FIPS PUB 46.

DES Algorithm :

Input :

T: 64 bits of clear text

k1, k2, ..., k16: 16 round keys

IP: Initial permutation

FP: Final permutation

f(): Round function

Output :

C: 64 bits of cipher text

Algorithm :

T' = IP(T), applying initial permutation

(L0, R0) = T', dividing T' into two 32-bit parts

(L1, R1) = (R0, L0 ^ f(R0, k1))

(L2, R2) = (R1, L1 ^ f(R1, k2))

......

C' = (R16, L16), swapping the two parts

C = FP(C'), applying final permutation

where ^ is the XOR operation.

The **round function f(R,k)** is defined as :

Input :

R: 32-bit input data

k: 48-bit round key

E: Expansion permutation

P: Round permutation

s(): S boxes function

Output :

R' = f(R,k): 32-bit output data

Algorithm :

X = E(R), applying expansion permutation and returning 48-bit data

X' = X ^ k, XOR with the round key

X" = s(X'), applying S boxes function and returning 32-bit data

R' = P(X"), applying the round permutation

The **S boxes function s(X)** is defined as :

Input :

X: 48-bit input data

S1, S2, ..., S8: 8 S boxes - 4 x 16 tables

Output :

X' = s(X): 32-bit output data

Algorithm :

(X1, X2, ..., X8) = X, dividing X into 8 6-bit parts

X' = (S1(X1), S2(X2), ..., S8(X8))

where Si(Xi) is the value at row r and column c of S box i with

r = 2*b1 + b6

c = 8*b2 + 4*b3 + 2*b3 + b4

b1, b2, b3, b4, b5, b6 are the 6 bits of the Xi

DES Cipher Algorithm Supporting Tables :

- **Initial Permutation – IP :**

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

- **Final Permutation – FP :**

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31

38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

- **Expansion Permutation – E :**

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

- **Round permutation – P :**

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

S boxes - S1, S2, ..., S8 :

S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

DES Key Schedule (Round Keys Generation) Algorithm :

Key Schedule Algorithm :

Input :

K: 64-bit key

PC1: Permuted choice 1

PC2: Permuted choice 2

r1, r2, …, r16: left shifts (rotations)

Output :

k1, k2, …, k16: 16 48-bit round keys

Algorithm :

K' = PC1(K), applying permuted choice 1 and returning 56 bits

(C0, D0) = K', dividing K' into two 28-bit parts

(C1, D1) = (r1(C0), r1(D0)), shifting to the left

k1 = PC2(C1,D1), applying permuted choice 2 and returning 48 bits

(C2, D2) = (r2(C1), r2(D1)), shifting to the left

k2 = PC2(C2,D2), applying permuted choice 2 and returning 48 bits

......

k16 = PC2(C16,D16)

DES Key Schedule Supporting Tables :

- **Permuted Choice 1 - PC1 :**

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

S boxes - S1, S2, ..., S8 :

S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

DES Key Schedule (Round Keys Generation) Algorithm :

Key schedule algorithm :

Input :

K: 64-bit key

PC1: Permuted choice 1

PC2: Permuted choice 2

r1, r2, ..., r16: left shifts (rotations)

Output :

k1, k2, ..., k16: 16 48-bit round keys

Algorithm :

K' = PC1(K), applying permuted choice 1 and returning 56 bits

(C0, D0) = K', dividing K' into two 28-bit parts

(C1, D1) = (r1(C0), r1(D0)), shifting to the left

k1 = PC2(C1,D1), applying permuted choice 2 and returning 48 bits

(C2, D2) = (r2(C1), r2(D1)), shifting to the left k2 = PC2(C2,D2), applying permuted choice 2 and returning 48 bits

......

k16 = PC2(C16,D16)

DES Key Schedule Supporting Tables :

- **Permuted Choice 1 - PC1 :**

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

- **Permuted Choice 2 - PC2 :**

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Left shifts (number of bits to rotate) - r1, r2, ..., r16:

r1	r2	r3	r4	r5	r6	r7	r8	r9	r10	r11	r12	r13	r14	r15	r16
1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Conclusions :

- DES is a 64-bit block cipher.
- 16 round keys are derived from a single 64-bit key.
- Decryption algorithm is identical to the encryption algorithm except for the order of the round keys.

(3) **DES-X :** In cryptography, **DES-X** (or **DESX**) is a variant on the DES (Data Encryption Standard) block cipher intended to increase the complexity of a brute force attack using a technique called *key whitening*.

The algorithm was included in RSA Security's BSAFE cryptographic library since the late 1980s.DES-X augments DES by XORing an extra 64 bits of key (K_1) to the plaintext *before* applying DES, and then XORing another 64 bits of key (K_2) *after* the encryption :

The key size is thereby increased to 56 + 2 × 64 = 184 bits.

However, the effective key size (security) is only increased to 56+64-1-lg(M) =119 - lg(M) = ~119 bits, where M is the number of known plaintext/ciphertext pairs the adversary can obtain,and lg() denotes the binary logarithm. (Because of this, some implementations actually make K_2 a strong one way function of K_1 and K.)

DES-X also increases the strength of DES against differential cryptanalysis and linear cryptanalysis, although the improvement is much smaller than in the case of brute force attacks. It is estimated that differential cryptanalysis would require 2^{61} chosen plaintexts (vs. 2^{47} for DES), while linear cryptanalysis would require 2^{60} known plaintexts (vs. 2^{43} for DES.) Note that with 2^{64} plaintexts (known or chosen being the same in this case), DES (or indeed any other block cipher with a 64 bit block size) is totally broken via the elementary codebook attack.

(4) **Advanced Encryption Standard** (**AES**) : In cryptography, the **Advanced Encryption Standard** (**AES**), also known as **Rijndael**, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor,[3] the Data Encryption Standard (DES).

AES is one of the most popular algorithms used in symmetric key cryptography. It is available by choice in many different encryption packages. This marks the first time that the public has had access to a cipher approved by NSA for top secret information.

AES is fast in both software and hardware, is relatively easy to implement, and requires little memory. As a new encryption standard, it is currently being deployed on a large scale.

Q.2. What is Block Cipher?

Ans.: In cryptography, a **block cipher** is a symmetric key cipher which operates on fixed-length groups of bits, termed *blocks*, with an unvarying transformation. When encrypting, a block cipher might take (for example) a 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext. The exact transformation is controlled using a second input — the secret key. Decryption is similar: the decryption algorithm takes, in this example, a 128-bit block of ciphertext together with the secret key, and yields the original 128-bit block of plaintext.

To encrypt messages longer than the block size (128 bits in the above example), a mode of operation is used.

Block ciphers can be contrasted with stream ciphers; a stream cipher operates on individual digits one at a time, and the transformation varies during the encryption. The distinction between the two types is not always clear-cut: a block cipher, when used in certain modes of operation, acts effectively as a stream cipher.

□ □ □

Chapter-3

Pseudorandom Function

Q.1. What are Pseudorandom Function?

Ans.: In cryptography, a **pseudorandom function family**, abbreviated **PRF**, is a collection of efficiently-computable functions which emulate a random oracle in the following way: No efficient algorithm can distinguish (with significant advantage) between a function chosen randomly from the PRF family and a random oracle (a function whose outputs are fixed completely at random). Pseudorandom functions are vital tools in the construction of cryptographic primitives, especially secure encryption schemes.

A pseudorandom function family can be constructed from any pseudorandom generator, using, for example, the construction given by Goldreich, Goldwasser, and Micali.

Q.2. Explain Birthday Attack?

Ans.: A **birthday attack** is a type of cryptographic attack, so named because it exploits the mathematics behind the birthday problem in probability theory. Given a function *f*, the goal of the attack is to find two inputs x_1,x_2 such that $f(x_1) = f(x_2)$. Such a pair x_1,x_2 is called a collision. The method used to find a collision is to simply evaluate the function *f* for different input values that may be chosen randomly or pseudorandomly until the same result is found more than once. Because of the birthday paradox this method can be rather efficient. Specifically, if a function $f(x)$ yields any of *H* different outputs with equal probability and *H* is sufficiently large, then we expect to obtain a pair of different arguments x_1 and x_2 with $f(x_1) = f(x_2)$ after evaluating the function for about $1.25 \cdot \sqrt{H}$ different arguments on average.

Q.3. What are Psedorandom Permutations?

Ans.: In cryptography, a **pseudorandom permutation**, abbreviated **PRP**, is an idealized block cipher. It means the cipher that cannot be distinguished from a random permutation (that is, a permutation selected at random with uniform probability, from the family of all permutations on blocks of that size) with less computational effort than specified by the cipher's security parameters (this usually means the effort required should be about the same as a brute force search through the cipher's key space). If a distinguishing algorithm exists that achieves significant advantage with less effort than the security parameter specifies, the cipher is considered broken at least in a certificational sense, even if such a break doesn't immediately lead to a practical security failure.

□ □ □

Chapter-4

Symmetric Encryption

Q.1. What is Symmetric Encryption?

Ans.: Symmetric Encryption is an Encryption algorithm where the same key is used for both Encryption and Decryption. The key must be kept secret, and is shared by the message sender and recipient.

Symmetric encryption, also known as single-key and/or private-key encryption, uses a secret key (could be a number, a word, a random string of characters) as a means to modify or mask the content of a given message. A "key" in cryptography simply refers to a piece of information used in completing the operation of a cryptographic algorithm. The key is a necessary tool for encrypting messages and decrypting cipher text. It should be noted, private-key encryption schemes are generally more efficient and less computationally expensive.

Symmetric encryption is the oldest form of encryption and has been used for thousands of years. Former Roman emperor, Julius Caesar, often used various symmetric encryption methods to conceal messages from his enemies. One such method, the rotation cipher, is now commonly referred to as the "Caesar Cipher". The rotation cipher simply substitutes letters from the alphabet with other letters based on a certain key length.

Symmetric Encryption Example: Rotation Cipher – **Key - 2**

A	B	C	D	E	F	G	H	I	J	K	L	M
C	D	E	F	G	H	I	J	K	L	M	N	O
N P	O Q	P R	Q S	R T	S U	T V	U W	V X	W Y	X Z	Y A	Z B

What is most important to understand with symmetric encryption is simply that the same key is used for both the purpose of encrypting and decrypting messages. The use of one key can often make the encryption/decryption process far less complicated. However, there is potential danger in using only one key. If an attacker or man in the middle is able to intercept a symmetrically encrypted message and determine the key, he/she now has the ability to both encrypt and decrypt messages. With this knowledge, an attacker can deceive both the original sender and receiver.

Q.2. What is Chosen Plaintext Attack?

Ans.: A chosen plaintext attack is an attack where the cryptanalyst is able to define his own plaintext, feed it into the cipher, and analyze the resulting ciphertext.

Mounting a chosen plaintext attack requires the cryptanalyst to be able to send data of his choice into the device which is doing the encryption, and it requires the cryptanalyst to be able to view the output from the device. Because of these requirements, a chosen plaintext attack is in some cases impossible to attempt.

A **Chosen-Plaintext Attack (CPA)** is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key.

This appears, at first glance, to be an unrealistic model; it would certainly be unlikely that an attacker could persuade a human cryptographer to encrypt large amounts of plaintexts of the attacker's choosing. Modern cryptography, on the other hand, is implemented in software or hardware and is used for a diverse range of applications; for many cases, a chosen-plaintext attack is often very feasible. Chosen-plaintext attacks become extremely important in the context of public key cryptography, where the encryption key is public and attackers can encrypt any plaintext they choose.

Any cipher that can prevent chosen-plaintext attacks is then also guaranteed to be secure against known-plaintext and ciphertext-only attacks; this is a conservative approach to security.

Two forms of chosen-plaintext attack can be distinguished :

- **Batch Chosen-Plaintext Attack**, where the cryptanalyst chooses all plaintexts before any of them are encrypted. This is often the meaning of an unqualified use of "chosen-plaintext attack".
- **Adaptive Chosen-Plaintext Attack**, where the cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.

□ □ □

Chapter-5

Hash Function

Q.1. What are Hash Functions?

Ans.: A **hash function** is any well-defined procedure or mathematical function for turning some kind of data into a relatively small integer, that may serve as an index into an array. The values returned by a hash function are called **hash values**, **hash codes**, **hash sums**, or simply **hashes**.

Hash functions are mostly used to speed up table lookup or data comparison tasks — such as finding items in a database, detecting duplicated or similar records in a large file, finding similar stretches in DNA sequences, and so on.

Hash functions are related to (and often confused with) checksums, check digits, fingerprints, randomizing functions, error correcting codes, and cryptographic hash functions. Although these concepts overlap to some extent, each has its own uses and requirements. The HashKeeper database maintained by the National Drug Intelligence Center, for instance, is more aptly described as a catalog of file fingerprints than of hash values.

Q.2. What is Universal Hashing?

Ans.: **Universal hashing** is a randomized algorithm for selecting a hash function *F* with the following property: for any two distinct inputs *x* and *y*, the probability that *F(x)*=*F(y)* (i.e., that there is a hash collision between *x* and *y*) is the same as if *F* was a random function. Thus, if *F* has function values in a range of size *r*, the probability of any particular hash collision should be **at most** *1/r*. There are universal hashing methods that give a function *F* that can be evaluated in a handful of computer instructions.

Q.3. What is CBC MAC Function?

Ans.: In cryptography, a **Cipher Block Chaining Message Authentication Code**, abbreviated **CBC-MAC**, is a technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the block before it. This interdependence ensures that a change to any of the plaintext bits will cause the final encrypted block to change in a way that cannot be predicted or counteracted without knowing the key to the block cipher.

To calculate the CBC-MAC of message *m* one encrypts *m* in CBC mode with zero initialization vector. The following figure sketches the computation of the CBC-MAC of a message comprising blocks using a secret key *k* and a block cipher *E*:

□ □ □

Chapter-6

Message Authentication

Q.1. What is Message Authentication?

Ans.: A cryptographic **message authentication code (MAC)** is a short piece of information used to authenticate a message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a *tag*). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content, and so should be called Message Authentication and Integrity Code: (MAIC).

□ □ □

Chapter-7

Asymmetric Encryption

Q.1. What is Asymmetric Encryption?

Ans.: Asymmetric Encryption is a form of Encryption where keys come in pairs. What one key encrypts, only the other can decrypt.

Frequently (but not necessarily), the keys are interchangeable, in the sense that if key A encrypts a message, then B can decrypt it, and if key B encrypts a message, then key A can decrypt it. While common, this property is not essential to asymmetric encryption.

Asymmetric Encryption is also known as Public Key Cryptography, since users typically create a matching key pair, and make one public while keeping the other secret.

Users can "sign" messages by encrypting them with their private keys. This is effective since any message recipient can verify that the user's public key can decrypt the message, and thus prove that the user's secret key was used to encrypt it. If the user's secret key is, in fact, secret, then it follows that the user, and not some impostor, really sent the message.

Users can send secret messages by encrypting a message with the recipient's public key. In this case, only the intended recipient can decrypt the message, since only that user should have access to the required secret key.

The key to successful use of Asymmetric Encryption is a Key Management system, which implements a Public Key Infrastructure. Without this, it is difficult to establish the reliability of public keys, or even to conveniently find suitable ones.

Q.2. What is Hybrid Encryption?

Ans.: Hybrid cryptosystems incorporate aspects from both symmetric and asymmetric encryption schemes. These hybrid systems amalgamate the convenience of public-key with the efficiency of private-key.

A hybrid system is basically broken down into two separate cryptosystems; the key encapsulation system and the data encapsulation system. The data encapsulation system which holds the message data is encrypted and decrypted by means of private-key encryption, meaning that both the sender and receiver have the same key. The key encapsulation system on the other hand uses public-key encryption as a means to encrypt/decrypt the key data. This key data, obtained through public-key encryption, is used as the private-key for the data encapsulation system.

For long, complex messages, the majority of the encrypting/decrypting work is done by the more efficient private-key scheme, while the lesser efficient, public-key method, is used to encrypt/decrypt the short key value.

Q.3. What are the differences in Symmetric, Asymmetric and Hybrid Encryption Methods?

Ans.: Differences in Symmetric, Asymmetric, and Hybrid Encryption Methods.

The differences between the three systems are quite apparent and easily distinguishable. Firstly, symmetric encryption methods use just one key. Both the sender and receiver have the same private key which is used for both encrypting and decrypting messages.

Asymmetric encryption on the other hand uses two different keys. One key is public and accessible to all. This public key allows senders to encrypt their messages. The other key used is a receiver's private key. This private key is used to decrypt a sender's corresponding publicly encrypted message.

Lastly, hybrid encryption, being its own entity, uses characteristics from both symmetric and asymmetric encryption schemes. Hybrid uses public-key (asymmetric) encryption for key encapsulation and private-key (symmetric) encryption for data encapsulation

□ □ □

Chapter-8

Digital Signatures

Q.1. What are Digital Signatures? Give it's benefits and drawbacks.

Ans.: A **digital signature** or **digital signature scheme** is a type of asymmetric cryptography used to simulate the security properties of a handwritten signature on paper. Digital signature schemes consist of at least three algorithms: a key generation algorithm, a signature algorithm, and a verification algorithm. A digital signature mainly provides authentication of a "message". In theory it can also provide non-repudiation, meaning that the authenticity of signed messages can be publicly verified, not only by the intended recipient. Messages may be anything, from electronic mail to a contract, or even a message sent in a more complicated cryptographic protocol.

A digital signature scheme typically consists of three algorithms :

- A *key generation* algorithm that selects a *private key* uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding *public key*.
- A *signing* algorithm which, given a message and a private key, produces a signature.
- A *signature verifying* algorithm which given a message, public key and a signature, either accepts or rejects.

Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify on that message and the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Benefits of Digital Signatures : Below are some common reasons for applying a digital signature to communications :

- **Authentication :** Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

- **Integrity :** In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to *change* an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

Drawbacks of Digital Signatures : Despite their usefulness, digital signatures alone do not solve the following problems :

Association of Digital Signatures and Trusted Time Stamping : Digital signature algorithms and protocols do not inherently provide certainty about the date and time at which the underlying document was signed. The signer might have included a time stamp with the signature, or the document itself might have a date mentioned on it. Regardless of the document's contents, a reader cannot be certain the signer did not, for example, backdate the date or time of the signature. Such misuse can be made impracticable by using trusted time stamping in addition to digital signatures.

Non-repudiation : In a cryptographic context, the word *repudiation* refers to any act of disclaiming responsibility for a message. A message's recipient may insist the sender attach a signature in order to make later repudiation more difficult, since the recipient can show the signed message to a third party (*e.g.*, a court) to reinforce a claim as to its signatories and integrity.

However, loss of control over a user's private key will mean that all digital signatures using that key, and so ostensibly 'from' that user, are suspect. Nonetheless, a user cannot repudiate a signed message without repudiating their signature key. This is aggravated by the fact there is no trusted time stamp, so new documents (after the key compromise) cannot be separated from old ones, further complicating signature key invalidation. A non-repudiation service requires the existence of a PKI which is complex to establish and operate. The Certificate authorities in a PKI usually maintain a public repository of public keys so the associated private key is certified and signatures cannot be repudiated. Expired certificates are normally removed from the repository. It is a matter for the security policy and the responsibility of the authority to keep old certificates for a period of time if non-repudiation of data service is provided.

□ □ □

BACHELOR OF COMPUTER APPLICATIONS
(Part III) EXAMINATION
(Faculty of Science)

(Three – Year Scheme of 10+2+3 Pattern)

PAPER 316

NETWORK SECURITY AND CRYPTOLOGY

OBJECTIVE PART- I

Year - 2011

Time allowed : One Hour *Maximum Marks : 20*

The question paper contains 40 multiple choice questions with four choices and students will have to pick the correct one (each carrying ½ marks.).

1. DES stands for:
   (a) Digital Encryption System
   (b) Data Encryption System
   (c) Dynamic Encryption System
   (d) None of the above ( )

2. In cryptography, the encryption/decryption key are__________
   (a) Public (b) Secret
   (c) Private (d) Both (a) and (b) ( )

3. Digital signatures does not provide:
   (a) Non-repudiation
   (b) Privacy
   (c) Authentication
   (d) Sockets ( )

4. After a message is decrypted, it is called:
   (a) Plain text
   (b) Cipher text
   (c) Cryptotext
   (d) Cryptonite ( )

5. In Which type of cryptography the same key is used in both direction?
(a) Symmetric key (b) asymmetric key
(c) Public key (d) None of the above ( )

6. RSA stands for:
(a) Rivest, Shamir Amozen
(b) Rock Shane and Amozen
(c) Rivest, Shamir and Adleman
(d) None of the above ( )

7. Which protocol provides message authentication integrity and privacy?
(a) AH (b) ESP
(c) Both (a) and (b) (d) None of the above ( )

8. The RSA algorithm uses which cryptography method:
(a) an asymmetric key (b) a private key
(c) a symmetric key (d) none of the above ( )

9. 3 DES (Triple Data Encryption Standard) is based on which of the following?
(a) Hashing Algorithm
(b) Symmetric key based Algorithm
(c) Asymmetric key based Algorithm
(d) None of the above ( )

10. Which of the following creates a message digest out of a message?
(a) Encryption
(b) Decryption
(c) Hash function
(d) None of the above ( )

11. A secure encryption key is:
(a) easy to remember (b) long and random
(c) long and predictable (d) short ( )

12. Which of the following is often used for short messages?
(a) Symmetric key
(b) Asymmetric key
(c) Secret key
(d) None of the above ( )

13. A digital signature requires what type of encryption?
(a) Hashing and asymmetric
(b) Asymmetric and symmetric
(c) Hashing and symmetric
(d) ECC and asymmetric ( )

14. What is shift cipher?
(a) A cipher with public and private keys
(b) A cipher that cannot be broken except by hand calculations
(c) One that uses the geometry of elliptical curves
(d) A cipher that shifts the letters in the alphabet by a numeric amount ( )

15. How many bits are there in a block of the SHA Algorithm?
(a) 128 (b) 2048
(c) 512 (d) 56 ( )

16. What is DES being replaced with?
(a) Diffie-Hellman (b) AES
(c) RC6 (d) MD5 ( )

17. What makes symmetric encryption superior to asymmetric for larger data sets?
(a) It's more secure
(b) speed
(c) Any one with the public key could decrypt the data
(d) It user a hash ( )

18. What is typically necessary to perform cryptanalysis?
(a) The key
(b) Large amounts of plaintext and ciphertextt
(c) A hash of the message
(d) None of the above ( )

19. What cioher was chosen to be the new AES standard?
(a) IDEA
(b) RC6
(c) ECC
(d) Rijndael ( )

20. Which of the following would be a valid MAC address?
(a) 00:07:e9 (b) 00:07:e9:7c:c8
(c) 00:07:e9:7c:c8:aa (d) 00:07:e9:7c:c8:aa:ba ( )

21. Encryption under the WPA-2 personal security model is accomplished by________
(a) DES-CCMP (b) AES-CCMP
(c) 3 DES (d) RC5 ( )

22. The PRNG in WEP is based on the __________ cipher algorithm.
(a) RC2
(b) RC4
(c) Dts
(d) AES ( )

23. A process for creating a unique "signature" for a set of data:
(a) Digital signing
(b) Decrypting
(c) Hashing
(d) Encryption ( )

24. The act of deliberately accessing computer systems and networks without authorization is generally known as:
(a) Computer Intrusions (b) Hacking
(c) Cracking (d) Probing ( )

25. What is Diffie-Hellman most commonly used for?
(a) Symmetric Encryption Key Exchange
(b) Signing Digital Contracts
(c) Securing e-mail
(d) Storing Encrypted Passwords ( )

26. The length of time a private key needs to remain secure is:
(a) The length of time a certificate offers validity
(b) Until a certificate has been revoked
(c) As long as the material that has been encrypted needs to remain secure
(d) Not applicable; once used, it is time invariant ( )

27. Which of the following is not part of a public key infrastructure?
(a) A substitution cipher
(b) The certificate revocation list
(c) The certificate authority
(d) Certificates ( )

28. The entity requesting an SA sets what?
(a) The Session Number (b) The Session ID
(c) The Initiator Cookie (d) The Process ID ( )

29. Which of the following provides connection security by using common encryption methods?
(a) The TLS Certificate Protocol
(b) The TLS Handshake Protocol
(c) The TLS Key Protocol
(d) The TLS Record Protocol and TLS Handshake Protocol ( )

30. Which of the following is a detailed standard for creating and implementing security policies?
(a) PKIX
(b) ISO 17799
(c) FIPS

(d) X509 ( )

31. Which of the following is a secure e-mail standard?
(a) POP3
(b) IMAP
(c) SMTP
(d) S/MIME ( )

32. A one way hash provides which of the following?
(a) Confidentiality (b) Availability
(c) Integrity (d) Authentication ( )

33. Which of the following is a public key cipher?
(a) Eigamal (b) ESDSA
(c) XTR (d) All of the above ( )

34. Which of the following is Asymmetric Encryption Algorithm?
(a) Diffie-Hellman
(b) XTR
(c) ECDSA
(d) All of the above ( )

35. IDEA stands for what?
(a) Indian Data Encryption Algorithm
(b) International Data Encryption Algorithm
(c) Initial Digital Encoding Algorithm
(d) International Digital Encoding Algorithm ( )

36. RC4 is:
(a) Stream cipher (b) Length cipher
(c) Block cripher (d) All of the above ( )

37. Which of the following is Symmetric Encryption Algorithim?
(a) DES
(b) IDEA
(c) Digital Signature Algorithim
(d) Both (a) and (b) ( )

38. Which of the following would be BEST to use to apply corporate security settings to a device?
(a) A security patch
(b) A security hotfix
(c) An OS service pack
(d) A security template ( )

39. Which of the following improves security in a wireless system?
(a) IP-spooling
(b) MAC filtering
(c) SSID spooling
(d) Closed network ( )

40. Which of the following logs might reveal the IP address and MAC address of a rogue device within the local network?
(a) Security logs (b) DHCP logs
(c) DNS logs (d) Antivirus logs ( )

Answer Key

1. ()	2. ()	3. ()	4. ()	5. ()	6. ()	7. ()	8. ()	9. ()	10. ()
11. ()	12. ()	13. ()	14. ()	15. ()	16. ()	17. ()	18. ()	19. ()	20. ()
21. ()	22. ()	23. ()	24. ()	25. ()	26. ()	27. ()	28. ()	29. ()	30. ()
31. ()	32. ()	33. ()	34. ()	35. ()	36. ()	37. ()	38. ()	39. ()	40. ()

DESCRIPTIVE PART-II

Year- 2011

Time allowed : 2 Hours ***Maximum Marks : 30***

Attempt any four descriptive types of questions out of the six. All questions carry 7½ marks each.

Q.1 (a) Explain the RSA Crypto System. Also explain how decryption be made fast.
(b) What are the different types of attacks on double DES and triple DES?.

Q.2 (a) Explain about block cripher principles and modes of operations..
(b) What are the uses of authentication protocols?.

Q.3 (a) What is the use of digital signature? What are the requirements of the digital signature scheme?
(b) What is MAC ? Explain its use?

Q.4 (a) Explain the Diffie-Hellman Key Exchange Algorithim with an example.
(b) Describe the data encryption algorithm.

Q.5 (a) What is a hash function? What are the requirements for a hash function? Also list the basic uses of a hash function.
(b) Explain about Kerberos.

Q.6 Write short notes on :

(a) Traffic Padding
(b) Triple Encryption
(c) Message Authentication
(d) Coin Flipping

BACHELOR OF COMPUTER APPLICATIONS
(Part III) EXAMINATION

(Faculty of Science)

(Three – Year Scheme of 10+2+3 Pattern)

PAPER 316

NETWORK SECURITY AND CRYPTOLOGY

OBJECTIVE PART- I

Year - 2010

Time allowed : One Hour *Maximum Marks : 20*

The question paper contains 40 multiple choice questions with four choices and students will have to pick the correct one (each carrying ½ marks.).

1. Input message in Cryptography is called;
(a) Plain text (b) Cipher Text
(c) Plain and cipher (d) None of the above ( )

2. Asymmetric key is also called:
(a) Secret key (b) Public key
(c) Private key (d) None of the above ( )

3. RSA stands for:
(a) Rivest shamir and Adleman
(b) Rock Shane and Amozen
(c) Rivest Shane and Amozen
(d) Rock Shamir and Adleman ( )

4. A digital signature need a :
(a) Public key system
(b) Private key system
(c) Public and private key system
(d) None of the above ( )

5. Which layer filter the proxy firewall:
(a) Application (b) Transport layer
(c) Network Layer (d) None of the above ( )

6. Secure Hash function or algorithm developed by:
(a) NIST (b) IEEE
(c) ANSI (d) None of the above ( )

7. ....is an encryption method used to offer secure communication by e-mail:
(a) Mail server (b) PGP
(c) SSL (d) None of the above ( )

8. Network security ensures:
(a) Detecting attacks (b) Preventing attacks
(c) Recovering attacks (d) All of the above ( )

9. The process to discover plain text or key is known as:
(a) Cryptanalysis (b) Crypto design
(c) Crypto processing (d) Crypto graphic ( )

10. Hacking refers to:
(a) Data access without permission
(b) Data updation without permission
(c) Data deletion without permission
(d) All of the above ( )

11. Encryption protects against:
(a) Attacks (b) Viruses
(c) Manipulation of data (d) All of the above ( )

12. Hash function is used to produce:
(a) Finger print of a file
(b) Useful for message authentication
(c) Both a and b
(d) None of the above ( )

13. Block cipher processes:
(a) 1000 bits at a time
(b) One bit block of data at a time
(c) Both a and b
(d) None of the above ( )

14. Decryption algorithm:
(a) Encrypts input data
(b) Decrypts the encrypted data
(c) Both a and b
(d) None of the above ( )

15. What is the name of the network attack that floods it with useless traffic?
(a) Virus (b) Trojan horse
(c) DOS attach (d) Spoofing ( )

16. RSA algorithm uses variable sized key that is usually between........and bits.
(a) 256,1048 (b) 256, 2048
(c) 512, 1048 (d) 512, 2048 ( )

17. What is an advantage of RSA over DSS?
(a) It can provide digital signature and encryption functionality
(b) It uses fewer resources and encrypts quicker because it uses symmetric keys
(c) It is a block cipher versus a stream cipher
(d) It employs a one time encryption pad ( )

18. The codified language can be termed as:
(a) Cleartext (b) Uncleartext
(c) Codetext (d) Ciphertext ( )

19. Cryptology means:
(a) Cryptoogy+ Cryptodesign
(b) Cryptology+Cryptanalysis
(c) Cryptograph itself known as cryptology also
(d) None of the above ( )

20. The input block length in AES is:
(a) 56 bits (b) 64 bits
(c) 112 bits (d) 128 bits ( )

21. An attack on a ciphertext message where the attacker attempts to use all possible permutations and combinations is called:
(a) Brute-Plaintext attack (b) Birthday attack
(c) Known-Planitext attack (d) Chosen-plaintext attack ( )

22. Hash collision means:
(a) Two keys for one message
(b) One key for two message
(c) Two different keys for different message
(d) Always the same key ( )

23. Encryption strength is based on:
(a) Strength of algorithm
(b) Secrecy of key
(c) Length of key
(d) All of the above ( )

24. In an authentication using symmetric keys, if 10 people need to communicate, we need.................keys.
(a) 10 (b) 20
(c) 30 (d) 40 ( )

25. In an efficient algorithm for factoring large number is discovered, which of the following schemes will be known to be not secure ?
(a) Diffle-Hellman (b) RSA
(c) AES (d) None of the above ( )

26. Session Key establishes:
(a) Logical connection (b) Physical Connection
(c) Both a and b (d) None of the above ( )

27. In the digital signature technique, the sender of the message uses.................to create ciphertext:
(a) Own symmetric key
(b) Own private key
(c) The receiver's private key
(d) Receiver's public key ( )

28. The symmetric (Shared) key in the Diffle-Hellman protocol is:
(a) $k = g^{xy}$ and p (b) $K = g^{xy}$ mod q
(c) $K = (R_2)^x$ (d) All of the above ( )

29. Secure socket layer is designed to provide, security and compression services to data granted from................
(a) Application Layer (b) Transport Layer
(c) Both (a) and (b) (d) None of the above ( )

30. Which of the following is not type of permutation in P-boxes?
(a) Plain permutation
(b) Straight permutation
(c) Expansion permutation
(d) Compression permutation ( )

31. Which of the following is not type of permutation in P-boxes?
(a) Plain permutation
(b) Straight permutation
(c) Expansion permutation
(d) Compression permutation ( )

32. SHA-1 is similar to:
(a) RSA (b) DES
(c) MDS (d) Rijndael ( )

33. Kerberos is an authentication scheme that can used to implement:
(a) Public key cryptography (b) Digital signature
(c) Hash function (d) Single sign on ( )

34. Transposition cipher involves:
(a) Replacement of blocks of text with other blocks
(b) Replacement of characters of text with other character
(c) Strict row to column replacement
(d) Some permutation on the input text to produce cipher text ( )

35. Which of the following is not a block cipher operating mode?
(a) ECB (b) CBF
(c) OFB (d) CBC ( )

36. If an efficient algorithm for factoring large number is discovered which of this following schemes will be known to be not secure?
(a) AES (b) Diffle-Hellman
(c) RSA (d) EI Gammal ( )

37. What are MD4 and MD5
(a) Symmetric Encryption Algorithms
(b) Asymmetric encryption Algorithms
(c) Hashing algorithms
(d) Digital certificates ( )

38. TDES means:
(a) Triple digital encryption standard
(b) Triangular data encryption standard
(c) Triple data encryption standard
(d) Triangular digital encryption standard ( )

39. If an attakcer stole a password file that contained one way encrypted passwords, what type of an attack would he/she perform to find the encrypted password?
(a) Man-in-the middle attack
(b) Birthday attack
(c) Denial of service attack
(d) Dictionary attack ( )

40. Masquerade attack is another name of:
(a) Virus attack (b) Spoofing
(c) DOS attack (d) Trojan Horse ( )

Answer Key

1. (a)	2. (a)	3. (a)	4. (a)	5. (c)	6. (a)	7. (c)	8. (d)	9. (a)	10. (a)
11. (d)	12. (c)	13. (b)	14. (b)	15. (d)	16. (a)	17. (a)	18. (a)	19. (b)	20. (b)
21. (a)	22. (b)	23. (d)	24. (a)	25. (c)	26. (a)	27. (d)	28. (a)	29. (b)	30. (a)
31. (a)	32. (c)	33. (b)	34. (b)	35. (c)	36. (a)	37. (c)	38. (c)	39. (b)	40. (b)

DESCRIPTIVE PART-II

Year- 2010

Time allowed : 2 Hours ***Maximum Marks : 30***

Attempt any four descriptive types of questions out of the six. All questions carry 7½ marks each.

Q.1 (a) Explain the operation of DES algorithm using diagram. What is the strength of a DES algorithm?

(b) Write down AES parameter and explain AES key expansin.

Q.2 (a) Explain collision resistant has functions by taking suitable example.

(b) What do you mean by 'Birthday Attack"? Explain.

Q.3 (a) What do you mean by pseudo random number generation? Expain

(b) What is MAC ? What is its use?

Q.4 (a) Describe various block cipher operating modes in brief.

(b) Differentiate symmetric and asymmetric encryption scheme.

Q.5 (a) What is the use of digital signature? What are the requirement of a digital signature scheme?

(b) What is coin flipping ?Explain briefly.

Q.6 Explain short notes on any three of the following :

(a) Proxy firewall

(b) One time pad scheme

(c) Triple DES

(d) SHA-1

OBJECTIVE PART- I

Year - 2009

Time allowed : One Hour *Maximum Marks : 20*

The question paper contains 40 multiple choice questions with four choices and student will have to pick the correct one. (Each carrying ½ marks.).

1. Secrecy, authentication and non-repudiation and integrity control are the area of:
(a) Network Security
(b) Cryptology
(c) Hashing
(d) None of these ( )

2. DES stands for:
(a) Data Encryption System
(b) Data Encryption Standard
(c) Digital Electronic Standard
(d) Digital Encryption Standard ( )

3. The protocols used to determine who goes next on a multiaccess channel belong to a sub layer of the data link called the:
(a) MAC
(b) DES
(c) ESP
(d) PKI ( )

4. Any public key algorithm can be used be:
(a) Data Encryption
(b) Pseudorandom Function
(c) Digital Signatures
(d) Pseudorandom Permutation ( )

5. Goals of network security are:
(a) Privacy (b) Authentication and availability
(c) Integrity (d) All of the above ( )

6. A function that maps a message of any length into a fixed length hash value is called:
(a) Pseudorandom function
(b) Message encryption
(c) Hash function
(d) Birthday attack ( )

7. X, 509 include which of the following authentication procedure:
(a) One way authentication
(b) Two way authentication
(c) Three way authentication
(d) None of the above ( )

8. The packet filter firewall is based on the information available in the :
(a) Application Layer and Transport Layer
(b) Network Layer and Transport Layer
(c) Application Layer and Network Layer
(d) None of the above ( )

9. Asymmetric key is also called:
(a) Secret key
(b) Public key
(c) Private key
(d) None of the above ( )

10. A block cipher which operates on fixed length groups of bits is called:
(a) Symmetric key
(b) Asymmetric Key
(c) Private key
(d) None of the above ( )

11. Security mechanism is ensured is:
(a) Detect attack
(b) Prevent Attack
(c) Recover From attack
(d) All of the above ( )

12. Which of the following is a monoalphabetic cipher:
(a) Casesar cipher
(b) Lucifer cipher
(c) Contradictory cipher
(d) Playfair cipher ( )

13. What is the size of data block in AES configuration?
(a) 128
(b) 64
(c) 256
(d) None of the above ( )

14. What type of firewall architecture employs two network cards and a single screening route:
(a) A screened host firewall

(b) A dual homed host firewall
(c) A screened subnet firewall
(d) An application level proxy server ( )

15. Cryptography means:

(a) Secret writing
(b) Word processing
(c) Parallel Processing
(d) All of the above ( )

16. Two way authentication is:

(a) Single transfer of information
(b) Duplex transfer of information
(c) Half duplex transfer of information
(d) None of the above ( )

17. IDEA stands for:

(a) International Data Encryption Algorithm
(b) International Digital Encryption Algorithm
(c) International Data Entity Authentication
(d) None of the above ( )

18. Triple DEA (TDEA) was first proposed by:

(a) Tuchman
(b) Rivest
(c) Both a and b
(d) None of the above ( )

19. Message authentication code:

(a) Generates small block of data
(b) Generates large block of data
(c) Does not generate data
(d) None of the above ( )

20. Which of the following algorithm is not based on block cipher?

(a) DES
(b) TDES
(c) RSA
(d) AES ( )

21. Hacking refers to:

(a) Data access without permission
(b) Data updation without permission
(c) Data deletion without permission
(d) All of the above ( )

22. Difie Hellman key exchange is vulnerable to:
    (a) Discrete logarithm method
    (b) Elliptic curve cryptography
    (c) Man in the middle attach
    (d) None of the above ( )

23. In stream ciphers;
    (a) One character is read at a time
    (b) Two characters are read at a time
    (c) Eight characters are read at a time
    (d) 32 characters are read at a time ( )

24. Which of the following is not a type of permutation in P-boxes?
    (a) Plain Permutation (b) Straight permutation
    (c) Expansion Permutation (d) Compression Permutation ( )

25. Blowfish was developed by Bruce Schneir. The block size is:
    (a) 64
    (b) 32
    (c) 48
    (d) None of the above ( )

26. What is an advantage of RSA over DSS?
    (a) It can provide digital signature and encryption functionality
    (b) It uses fewer resources and encrypts quicker because it uses symmetric keys
    (c) It is a block cipher versus a stream cipher
    (d) It employs a one time encryption pad ( )

27. In most secruity protocols that support authentication, integrity and confidentially:
    (a) DES is used to create digital signatures
    (b) Private key cryptography is used to create digital signatures
    (c) Public key cryptography is used to create digital signatures
    (d) Digital signatures are not implemented ( )

28. Kerberos is an authentication scheme that can used to implement :
    (a) Public key cryptography
    (b) Digital signature
    (c) Hash function
    (d) Single Sign On (SSO) ( )

29. Which of the following is not a property of a packet Filtering firewall?
    (a) Considered a first generation firewall
    (b) Uses ACLs

(c) Operates at the Application Layer
(d) Examines the source and destination address of the incoming packet ( )

30. SHA-a is similar to:
(a) RSA
(b) DES
(c) MD5
(d) Rijndeal ( )

31. KDC stands for:
(a) Karnaugh Display Cycle
(b) Key Distribution Center
(c) Key Display Cycle
(d) None of the above ( )

32. TDEA stands for:
(a) Triple Data Encryption Standard
(b) Third Data Entity System
(c) Third Data Entry System
(d) All of the above ( )

33. A technique used to gain unauthorized access to computers, where the intruder sends messages to a computer with a trusted IP address is called:
(a) Spoofing
(b) Smurfing
(c) Sniffing
(d) None of the above ( )

34. If an attacker stole a password file that contained one way encrypted passwords, what type of an attack would he/she perform to find the encrypted password?
(a) Man in the Middle Attack
(b) Birthday Attack
(c) Denial of Service Attack
(d) Dictionary Attack ( )

35. An attack of a cipher text message where the attacker attempt to us all possible permutation and combination is called:
(a) Brute- force attack
(b) Birthday attack
(c) Known plain text attack
(d) chosen plain text attack ( )

36. Which choice most accurately describes SSL?
(a) It's a widely used standard for securing e-mail at the application level

(b) It gives a user remote access to a command prompt across a secure encrypted session

(c) It uses two protocol, the authentication header and the encapsulating security

(d) It allows an application to have authenticated encrypted communication a cross a network ( )

37. The secure Hash algorithm (SHA) is specified in the :

(a) Data Encryption Standard

(b) Digital Signature Standard

(c) Digital Encryption Standard

(d) Advanced Encryption Standard ( )

38. When two different keys encrypt a plain text message into the same cipher text, this situation is known as:

(a) Public key cryptography

(b) Cryptanalysis

(c) Key clustering

(d) Hashing ( )

39. One way authentication is:

(a) Single transfer of information

(b) Duplex transfer of information

(c) Half duplex transfer of information

(d) None of the above ( )

40. Session key:

(a) Establishes logical connection

(b) Establishes physical connection

(c) Both a and b

(d) None of the above ( )

Answer Key

1. (a)	2. (b)	3. (a)	4. (a)	5. (d)	6. (c)	7. (d)	8. (b)	9. (c)	10. (a)
11. (d)	12. (a)	13. (a)	14. (a)	15. (a)	16. (c)	17. (a)	18. (a)	19. (a)	20. (c)
21. (d)	22. (a)	23. (c)	24. (a)	25. (a)	26. (a)	27. (c)	28. (b)	29. (c)	30. (c)
31. (b)	32. (a)	33. (a)	34. (b)	35. (a)	36. (d)	37. (c)	38. (c)	39. (a)	40. (a)

DESCRIPTIVE PART - II

Year 2009

Time allowed : 2 Hours   ***Maximum Marks : 30***

Attempt any four questions out of the six. All questions carry 7½ marks each.

Q.1 (a) What do you understand by network secuirty?

(b) Define cryptography. Define approaches and phase in cryptography development.

Q.2 (a) Explain collision resistant has function by taking suitable example.

(b) Describe message authentication and explain the syntax of message authentication schemes.

Q.3 (a) What is the use of digital signature? What are the requirement of a digital signature Scheme?

(b) Explain DSS approach of Digital signature. How RSA approach different from it? List advantages of DSS over RSA approach.

Q.4 (a) What do you mean by pseudorandom generation? Explain

(b) What is coin flipping? Describe

Q.5 (a) What is symmetric encryption?

(b) What is difference between block cipher and stream cipher?

Q.6 Write note on:

(a) Firewall

(b) CBC-MAC

(c) Hash Function

(d) Asymmetric Encryption

(e) SHA-1 Algorithm

OBJECTIVE PART- I

Year - 2008

Time allowed : One Hour *Maximum Marks : 20*

The question paper contains 40 multiple choice questions with four choices and student will have to pick the correct one. (Each carrying ½ marks.).

1. Cryptography means:
(a) Secrete writing
(b) Application programming
(c) Word processing
(d) None of these ( )

2. In cryptography:
(a) Information is transmitted
(b) Information is transmitted from sender to receiver
(c) Information is damage
(d) None of these ( )

3. It is customary to use three character in an information exchange scenario:
(a) Alice
(b) Bob
(c) Alice & Bob
(d) None of these ( )

4. Input message in cryptography is called:
(a) Plain text
(b) Cipher text
(c) Plain text & cipher text
(d) None of these ( )

5. Output message in cryptography is called :
(a) Plain text
(b) Cipher text
(c) Plan text & cipher text
(d) None of these ( )

6. Symmetric key is also called:
(a) Secrete key
(b) Public key

(c) Private key
(d) None of these ( )

7. Asymmetric key is also called:
(a) Secrete key
(b) Public key
(c) Private key
(d) None of these ( )

8. A substitution cipher substitutes or replaces:
(a) One symbol with another
(b) Two symbols with another
(c) a and b
(d) None of these ( )

9. Who used the shift cipher to communicate with his office:
(a) Julius Caesar
(b) Alice
(c) Bob and Alice
(d) None of these ( )

10. Shift cipher is sometime referred to as:
(a) Caesar cipher
(b) Transposition cipher
(c) XOR cipher
(d) None of these ( )

11. DES stand for:
(a) Data Encryption standard
(b) Data Encryption source
(c) Data encryption system
(d) None of these ( )

12. What is size of data block in AES configuration:
(a) 128
(b) 64
(c) 256
(d) None of these ( )

13. Which of the following is not a block cipher operating mode:
(a) ECB
(b) CBC
(c) CFB
(d) None of these ( )

14. Who was designed RC5:
(a) Ron
(b) Rivent
(c) Ron & Rivent
(d) None of these ( )

15. RSA stands for:
(a) Rivest
(b) Shamir
(c) Rivest Shamir & Adleman
(d) None of these ( )

16. IDEA developed by:
(a) Xuijla Lai & James Massey
(b) Xaija
(c) James Massey
(d) None of these ( )

17. Blowfish was developed by Bruce Schneier. The block size is:
(a) 64
(b) 32
(c) 48
(d) None of these ( )

18. The symmetric (Shared) key in the Diffie - Helman Protocol is:
(a) $k = g^{xy}$ and p
(b) $K = g^{xy} \bmod q$
(c) $K = (R_2)^x$
(d) All of the above ( )

19. Triple DES was designed to increase the size of teh DES key for better security:
(a) 56 bits
(b) 112
(c) 256 bits
(d) None of these ( )

20. Which of the following is not a type of permutation in P-boxes:
(a) Plain permutation
(b) Straight permutation
(c) Expansion permutation
(d) Compression permutation ( )

21. A digital signature needs a:
(a) Plain permutation (b) Straight permutation

(c) Expansion permutation (d) compression permutation ( )

22. SHA-1 algorithm process data in block length of ....bits.
(a) 128 (b) 256
(c) 512 (d) 1024 ( )

23. The codified languages can be termed as:
(a) Clear text
(b) Unclear text
(c) Code text
(d) Cipher text ( )

24. To preserve the integrity of a message, the message is passed through an algorithm called a:
(a) Hash function (b) Finger Print Function
(c) N Hash function (d) None of these ( )

25. Secure socket layer is designed to provide security and compression services to data granted from...........
(a) Application layer
(b) Transport layer
(c) Application layer & transport layer
(d) None of these ( )

26. ....is an encryption method used to offer secure communication by e-mail:
(a) Mail Server (b) PGP
(c) SSL (d) None of these ( )

27. Which of the following is not a property of a packet filtering firewall :
(a) Network layer and transport layer
(b) Uses ACLs
(c) Considered first generation firewall
(d) None of these ( )

28. Which layer filter the proxy firewall:
(a) Application layer
(b) Transport layer
(c) Network layer
(d) None of these ( )

29. Which of the following is not a criteria of a hash function:
(a) Two-wayness
(b) Weak collision resistance
(c) Strong collision

(d) One - Wayness ( )

30. Network security:
(a) Data is protected during transmission
(b) Data is not protected at all
(c) Data is changed
(d) All of the above ( )

31. CBCM stands for:
(a) Cipher block chaining mode
(b) Cipher block changing mode
(c) Cipher block chaining method
(d) Cipher block changing method ( )

32. Cryptograph ensures:
(a) Confidentiality of data
(b) Authentication of data
(c) Integrity of data
(d) All of the data ( )

33. Secure hash function or algorithm developed by:
(a) National Institute of Standard & Technology
(b) IEEE
(c) ANSI
(d) Nose of these ( )

34. Deffie - Hellman protocol that provides a session key:
(a) One time
(b) Two time
(c) One time & two time
(d) None of these ( )

35. X.509 include which of the following authentication procedure:
(a) One way authentication
(b) Two way authentication
(c) Three way authentication
(d) None of these ( )

36. Which of the following is not provided by digital signature:
(a) Message integrity
(b) Authentication
(c) Non repudiation
(d) KDC ( )

37. PKI stands for:
    (a) Public key infrastructure
    (b) Public Key interface
    (c) Public key internet
    (d) None of these ( )

38. The most widely used public key algorithm are:
    (a) RAS
    (b) Diffie-Hellman
    (c) RAS & Diffie-Hellman
    (d) None of these ( )

39. ESP stands for:
    (a) Encryption Security Protocol
    (b) Entity Secure Protocol
    (c) Encapsulating Security payload
    (d) None of these ( )

40. Which of the following is not provided by ESP:
    (a) Source authentication (b) Data integrity
    (c) Privacy (d) Padding ( )

Answer Key

1. (a)	2. (b)	3. (c)	4. (a)	5. (b)	6. (a)	7. (b)	8. (a)	9. (a)	10. (a)
11. (a)	12. (a)	13. (d)	14. (c)	15. (c)	16. (a)	17. (a)	18. (b)	19. (b)	20. (b)
21. (c)	22. (c)	23. (d)	24. (a)	25. (b)	26. (b)	27. (d)	28. (a)	29. (a)	30. (a)
31. (a)	32. (d)	33. (a)	34. (a)	35. (c)	36. (d)	37. (a)	38. (a)	39. (c)	40. (a)

DESCRIPTIVE PART - II

Year 2008

Time allowed : 2 Hours *Maximum Marks : 30*

Attempt any four questions out of the six. All questions carry 7½ marks each.

Q.1 (a) Explain the operations of DES algorithm using diagram. What are the strength of a DES algorithm?

(b) Differentiate between strong and weak collision resistance.

Q.2 (a) Why do we require Hash Function? What are the requirement of a good Hash function?

(b) What is public key cryptography principle? What are its application.

Q.3 (a) Briefly explain RSA data encryption algorithm. What are the strength of a RSA algorithm?

Q.4 (a) What is digital signature? What are basic steps using for data encryption and decryption in digital signature.

(b) What is difference between block cipher and stream cipher?

Q.5 (a) What are the pseudorandom number? Explain their importance cryptography. How can they be generated? Explain

Q.6 Write short notes on any three of the following:

(a) Asymmetric key cryptography

(b) Triple DES

(c) Diffie - Hellman cryptosystem

(d) HMAC

(e) Proxy fire well

OBJECTIVE PART- I

Year - 2007

Time allowed : One Hour *Maximum Marks : 20*

The question paper contains 40 multiple choice questions with four choices and student will have to pick the correct one. (Each carrying ½ marks.).

1. Cryptography relates to........................
(a) Editing
(b) Security
(c) Testing
(d) All of the above ( )

2. Protocol refer to:
(a) Rules
(b) Methods
(c) Both rules and methods
(d) None of the above ( )

3. DES stands for:
(a) Data encryption standard
(b) Data Encryption security
(c) Data Embedded standard
(d) Data Easily substitutable ( )

4. In cryptography...................
(a) Data is encrypted while sending
(b) Data is encrypted while receiving
(c) Data is updated while communication
(d) None of the above ( )

5. Encrypted message is called.............in cryptography:
(a) Plain text (b) Cipher text
(c) Secret text (d) All of the above ( )

6. The message is decrypted at....................end:
(a) Receiver
(b) Sender
(c) Broker

(d) All of the above ( )

7. Authentication refers to:
(a) Verification of user's identity
(b) Checking user's privileges
(c) Auditing user's process
(d) None of the above ( )

8. Encryption protects against:
(a) Attacks (b) Viruses
(c) Manipulation of data (d) All of the above ( )

9. Public key is known to everybody:
(a) Attacks
(b) Viruses
(c) Manipulation of data
(d) All of the above ( )

10. AES stands for:
(a) Advanced Encryption System
(b) Advanced Encryption Solution
(c) Advanced Encryption strategies
(d) Advanced Encryption Standard ( )

11. The sender 'sings' a message as...............
(a) By hand
(b) By speaking
(c) Digital signature
(d) Any of the above ( )

12. CA stands for:
(a) Certified auditing (b) Certification authorities
(c) Cyper Abuses (d) Certified automation ( )

13. Hacking refers to:
(a) Data access without permission
(b) Data updation without permission
(c) Data deletion without permission
(d) All of the above ( )

14. TDES means:
(a) Triple digital Encryption standard
(b) Triple Data Encryption System
(c) Triple Data Encryption Standard
(d) Triple Digital Encryption System ( )

15. DSS stands for:
(a) Digital signature standard
(b) Digital Signature simulation
(c) Digital signature strategies
(d) Digital Signature system ( )

16. Network security ensures.................
(a) Detecting attacks
(b) Preventing attacks
(c) Recovering attacks
(d) All of the above ( )

17. In cryptography receiver encrypts the message and sender decrypts the message:
(a) True
(b) False
(c) Never
(d) Can't say ( )

18. Secure hash algorithm was developed by:
(a) IEE (b) NIST
(c) Never (d) None of the above ( )

19. The process to discover plaintext or key is known as:
(a) Cryptanalysis (b) Symmetric Hash Function
(c) Crypto processing (d) Observation Cryptographic ( )

20. SHF stands for.........................
(a) Secure Hash function (b) Symmetric Hash Function
(c) Crypto processing (d) Secure Hash file ( )

21. What is the length of key (without padding) in DES?
(a) 64 bits
(b) 128 bits
(c) 72 bits
(d) 56 bits ( )

22. KDC stands for:
(a) Karnaugh Display Cycle
(b) Key Distribution Center
(c) Key Display Cycle
(d) None of these ( )

23. Diffie - Hellman key exchange is vulnerable to:...................
(a) Discrete logarithm
(b) Elliptic curve cryptography

(c) Man in the middle attack
(d) None of these ( )

24. MAC means..................
(a) Message Authorization Code
(b) Message Authentication Code
(c) Message Approximation Code
(d) All of the above ( )

25. SHA-1 is similar to......................
(a) RSA
(b) DES
(c) MD5
(d) Rijndae! ( )

26. In PKI..................
(a) Public key is known, private key is secrete
(b) Private key is knwon, public key is secret
(c) Both keys are known
(d) Both keys are secret ( )

27. Cryptology means....................
(a) Cryptography + Cryptodesign
(b) Cryptography + Cryptanalysis
(c) Cryptography itself known as cryptology also
(d) None of the above ( )

28. RSA stands for......................
(a) Rivest, Shannon, Admand
(b) Rodger, Shannon, Admand
(c) Rivest, Shamir, Addleman
(d) Rivest, Shannon, Addleman ( )

29. RSA involves very large.........numbers:
(a) Prime (b) Even
(c) Odd (d) Any number ( )

30. Hash collision means................
(a) Two keys for one message
(b) One key for two message
(c) Two different keys for different message
(d) Always the same key ( )

31. ECB stands for:
(a) Emergency Code book (b) Electronic Code Book
(c) Elective Code Book (d) Encrypted Code Book ( )

32. DES involves the following block cipher technique............
(a) ECB
(b) RSA
(c) CBC
(d) SHAI ( )

33. Which of the following is a monoalphabetc cipher?
(a) Caesar Cipher (b) Lucifer cipher
(c) Contradictory cipher (d) Play fair cipher ( )

34. Which of the following is a transposition cipher................
(a) Caesar cipher (b) Vignere Cipher
(c) One time pad (d) Playfair cipher ( )

35. Which is not lreated to cryptography?
(a) ....machines (b) Enigma
(c) Steganography (d) Analytical Engine ( )

36. In stream ciphers..............
(a) One character is read at a time
(b) Two character are read at a time
(c) Eight character are read at a time
(d) 32 characters are read at a time ( )

37. Finding plaintext, without knowing key is known is:
(a) Cryptography
(b) Cryptanalysis
(c) Cryptology
(d) None of the above ( )

38. Which of the following algorithm is not based on block encryption?
(a) DES (b) TDES
(c) RSA (d) AES ( )

39. Which of the following is not used for symmetric encryption ?
(a) RSA (b) DES
(c) SHAI (d) RC4 ( )

40. Which of the following is not the basic principle of cryptography?
(a) Confidentiality
(b) Integrity

(c) Atomicity
(d) Non-repudiation ( )

Answer Key

1. (b)	2. (c)	3. (a)	4. (a)	5. (b)	6. (a)	7. (a)	8. (d)	9. (a)	10. (d)
11. (c)	12. (b)	13. (d)	14. (c)	15. (a)	16. (d)	17. (b)	18. (b)	19. (a)	20. (b)
21. (d)	22. (b)	23. (a)	24. (b)	25. (c)	26. (a)	27. (b)	28. (c)	29. (d)	30. (a)
31. (a)	32. (c)	33. (a)	34. (d)	35. (c)	36. (a)	37. (b)	38. (c)	39. (a)	40. (c)

DESCRIPTIVE PART - II

Year 2007

Time allowed : 2 Hours ***Maximum Marks : 30***

Attempt any four questions out of the six. All questions carry 7½ marks each.

Q.1 (a) What do you mean by coin flipping? In what context is it used? Explain in details.

(b) Define cryptography and describe phases in the cryptography development.

Q.2 (a) Explain 'Block Cipher' and its use in cryptography.

(b) What are the various pseudorandom function families? Explain each of them.

Q.3 (a) What do you mean by 'birthday attack' ? Explain

(b) Describe symmetric encryption and its schemes.

Q.4 (a) Explain collision resistant has functions by taking suitable examples.

(b) Describe message authentication and explain the syntax of message authentication schemes.

Q.5 (a) What do you mean by DES and AES? Explain

(b) What is Shannon Security for Symmetric encryption? Briefly explain.

Q.6 Write short notes on any three of the following:

(a) SHA-1

(b) The CBC-MAC Function

(c) RSA

(d) Asymmetric encryption

(e) Digital Signature

OBJECTIVE PART- I

Year - 2006

Time allowed : One Hour *Maximum Marks : 20*

The question paper contains 40 multiple choice questions with four choices and student will have to pick the correct one. (Each carrying ½ marks.).

1. Cryptography means:
(a) Secret writing (b) Word processing
(c) Parallel processing (d) All of the above ( )

2. In cryptography:
(a) Information is transmitted from sender to receiver
(b) No information is transmitted
(c) Information is damaged
(d) None of the above ( )

3. Input message in cryptography is called:
(a) Plain text
(b) Cipher text
(c) Both a and b
(d) None of the above ( )

4. Output message in cryptography is called:
(a) Plain text (b) Cipher text
(c) Both a and b (d) None of the above ( )

5. The process to discover plain text or key is known as:
(a) Cryptanalysis
(b) Crypto design
(c) Crypto processing
(d) Crypto graphic ( )

6. Block cipher process:
(a) 1000 bits at a time (b) Secure Hash Function
(c) Both a and b (d) None of the above ( )

7. SHF stands for:
(a) Symmetric Hash Function
(b) Securre Hash Function
(c) Simulated Hash Function

(d) None of these ( )

8. One way authentication is:
(a) Single transfer of information (b) Duplex transfer of information
(c) Half duplex transfer of information (d) None of the above ( )

9. Two way authentication is:
(a) Double transfer of information (b) No transfer of information
(c) Half duplex transfer of information (D) None of the above ( )

10. Authentication is:
(a) Verification of user's identification
(b) Verification of the data
(c) Both a and b
(d) None of the above ( )

11. Encryption protects against:
(a) Attacks
(b) Loss of data
(c) Both a and b
(d) None of the above ( )

12. Encryption algorithm:
(a) Encrypts input data (b) Encrypts output data
(c) Both a and b (d) None of the above ( )

13. Decryption algorithm:
(a) Encrypts input data
(b) Decrypts the encrypted data
(c) Both a and b
(d) None of the above ( )

14. Secret key is:
(a) Used with algorithms (b) Not used with algorithm
(c) Never used any where (d) None of the above ( )

15. CBCM stands for:
(a) Cipher Block Chaining Mode
(b) Cipher Block channing Mode
(c) Cipher block chaining method
(d) Cipher block chaining method ( )

16. DES stands for:
(a) Data Encryption Standard
(b) Data Encryption System

(c) Data Encryption Suggestions
(d) None of the above ( )

17. AES stands for:
(a) Advanced Encryption Standard
(b) Advanced Encryption System
(c) Advanced Encryption Suggestion
(d) None of the above ( )

18. Authentication is done by:
(a) Conventional encryption
(b) Scrambling data
(c) Both a and b
(d) None of the above ( )

19. In encryption:
(a) Public key is used
(b) Private key is used
(c) Both public and private keys are used
(d) None of the above ( )

20. The sender "signs" a message as:
(a) Digital Signature (b) Artificial Signature
(c) Encrypted Signature (d) All of the above ( )

21. In network security:
(a) Data is protected during transmission
(b) Data is not protected transmission
(c) Data is changed
(d) None of the above ( )

22. Cryptography ensures:
(a) Confidentiality of data
(b) Authentication of data
(c) Integrity of data
(d) All of the above ( )

23. TDEA stands for:
(a) Triple Data Encryption Standard
(b) Third Data Entity System
(c) Third Data Entry System
(d) All of the above ( )

24. Hash Function is used to produce:
(a) Finger print of a file

(b) Useful for message authentication
(c) Both a and b
(d) None of the above ( )

25. DSS stands for:
(a) Digital signature standard
(b) Digital sound system
(c) Digital simulation schemes
(d) None of these ( )

26. In network secruity:
(a) Data is Protected From Hackers
(b) Data is Protected From Cracker
(c) Both a and b
(d) None of the above ( )

27. In cryptography?
(a) Secret key is used
(b) Secret key is not used
(c) Secret key is damaged
(d) None of the above ( )

28. In private key cryptography:
(a) Sender and receiver both must have secret key
(b) Sender and receiver both need not have a secret key
(c) Only sender must have the secret key
(d) Only receiver must have the secret key ( )

29. IDEA stands for:
(a) International Data Encryption Algorithm
(b) International Digital Encryption Algorithm
(c) International Data Entity Authentication
(d) None of the above ( )

30. Security mechanism is ensured is:
(a) Detect attack
(b) Prevent Attack
(c) Recover From attack
(d) All of the above ( )

31. Conventional encryption is:
(a) Symmetric encryption
(b) Secret key encryption
(c) Single key encryption
(d) All of the above ( )

32. In cryptography:
    (a) Plain text is converted into cipher text
    (b) Plain text remains as it is
    (c) Plain text is updated
    (d) None of the above ( )

33. Data Encryption standard is:
    (a) Most widely used scheme
    (b) Rarely used
    (c) Not used
    (d) None of the above ( )

34. The most commonly used conventional encryption algorithms are:
    (a) Block ciphers
    (b) Transposition ciphers
    (c) Both a and b
    (d) None of the above ( )

35. Triple DEA (TDEA) was first proposed by:
    (a) tuchman (b) Rivest
    (c) both a and b (d) None of the above ( )

36. Session by:
    (a) Establishes Logical Connection
    (b) Establishes physical connection
    (c) Both a and b
    (d) None of the above ( )

37. Message authentication code:
    (a) Generates small block of data (b) Generates large block of data
    (c) Does not generate data (d) None of the above ( )

38. Data Encryption Algorithm:
    (a) Generates encrypted version of the message
    (b) Generates non-encrypted version of the message
    (c) Generates secret keys
    (d) None of these ( )

39. Secure hash algorithm developed by:
    (a) National Institute of Standards and Technology (NIST)
    (b) IEEE
    (c) ANSI
    (d) None of the above ( )

40. The most widely used public key algorithms are:

(a) RSA (b) Diffie Hellman
(c) Both a and b (d) None of the above ( )

Answer Key

1. (a)	2. (a)	3. (a)	4. (b)	5. (a)	6. (b)	7. (a)	8. (a)	9. (c)	10. (a)
11. (d)	12. (a)	13. (b)	14. (a)	15. (c)	16. (a)	17. (a)	18. (c)	19. (a)	20. (a)
21. (a)	22. (d)	23. (a)	24. (c)	25. (a)	26. (a)	27. (a)	28. (d)	29. (a)	30. (d)
31. (d)	32. (a)	33. (a)	34. (a)	35. (a)	36. (a)	37. (a)	38. (a)	39. (a)	40. (c)

DESCRIPTIVE PART - II

Year 2006

Time allowed : 2 Hours *Maximum Marks : 30*

Attempt any four questions out of the six. All questions carry 7½ marks each.

Q.1 (a) Describe 'Hash Function'

(b) Write and explain some symmetric encryption schemes.

Q.2 (a) Describe message authentication and explain the syntax of message authentication schemes.

(b) Explain Digital Signature and its schemes.

Q.3 (a) Explain cryptography and describe phases in the cryptography development.

(b) What is Shannon security for symmetric encryption? Briefly explain.

Q.4 (a) What is a 'Block Cipher'? Explain key recovery attacks on block ciphers.

(b) What do you mean by DES and AEF ? Explain.

Q.5 (a) What do you mean by Pseudorandom number generation? Explain

(b) What is coin flipping? Describe.

Q.6 Write short notes any three of the following:

(a) Cryptography and computer security

(b) Public key cryptography principle'

(c) Fire well

(d) Asymmetric encryption

(e) Random function

Multiple Choice Questions

1. Cryptography means:
(a) Secret writing (b) Word processing
(c) Parallel processing (d) All of the above ( )

2. In cryptography:
(a) Information is transmitted from sender to receiver
(b) No information is transmitted
(c) Information is damaged
(d) None of the above ( )

3. Input message in cryptography is called:
(a) Plain text
(b) Cipher text
(c) Both a and b
(d) None of the above ( )

4. Output message in cryptography is called:
(a) Plain text (b) Cipher text
(c) Both a and b (d) None of the above ( )

5. The process to discover plain text or key is known as:
(a) Cryptanalysis
(b) Crypto design
(c) Crypto processing
(d) Crypto graphic ( )

6. Block cipher process:
(a) 1000 bits at a time (b) Secure Hash Function
(c) Both a and b (d) None of the above ( )

7. SHF stands for:
(a) Symmetric Hash Function
(b) Securre Hash Function
(c) Simulated Hash Function
(d) None of these ( )

8. One way authentication is:
(a) Single transfer of information (b) Duplex transfer of information
(c) Half duplex transfer of information (d) None of the above ( )

9. Two way authentication is:
(a) Double transfer of information (b) No transfer of information
(c) Half duplex transfer of information (D) None of the above ( )

10. Authentication is:
(a) Verification of user's identification
(b) Verification of the data
(c) Both a and b
(d) None of the above ( )

11. Encryption protects against:
(a) Attacks
(b) Loss of data
(c) Both a and b
(d) None of the above ( )

12. Encryption algorithm:
(a) Encrypts input data (b) Encrypts output data
(c) Both a and b (d) None of the above ( )

13. Decryption algorithm:
(a) Encrypts input data
(b) Decrypts the encrypted data
(c) Both a and b
(d) None of the above ( )

14. Secret key is:
(a) Used with algorithms (b) Not used with algorithm
(c) Never used any where (d) None of the above ( )

15. CBCM stands for:
(a) Cipher Block Chaining Mode
(b) Cipher Block channing Mode
(c) Cipher block chaining method
(d) Cipher block chaining method ( )

16. DES stands for:
(a) Data Encryption Standard
(b) Data Encryption System
(c) Data Encryption Suggestions
(d) None of the above ( )

17. AES stands for:
(a) Advanced Encryption Standard
(b) Advanced Encryption System
(c) Advanced Encryption Suggestion
(d) None of the above ( )

18. Authentication is done by:

(a) Conventional encryption
(b) Scrambling data
(c) Both a and b
(d) None of the above ( )

19. In encryption:
(a) Public key is used
(b) Private key is used
(c) Both public and private keys are used
(d) None of the above ( )

20. The sender "signs" a message as:
(a) Digital Signature (b) Artificial Signature
(c) Encrypted Signature (d) All of the above ( )

21. In network security:
(a) Data is protected during transmission
(b) Data is not protected transmission
(c) Data is changed
(d) None of the above ( )

22. Cryptography ensures:
(a) Confidentiality of data
(b) Authentication of data
(c) Integrity of data
(d) All of the above ( )

23. TDEA stands for:
(a) Triple Data Encryption Standard
(b) Third Data Entity System
(c) Third Data Entry System
(d) All of the above ( )

24. Hash Function is used to produce:
(a) Finger print of a file
(b) Useful for message authentication
(c) Both a and b
(d) None of the above ( )

25. DSS stands for:
(a) Digital signature standard
(b) Digital sound system
(c) Digital simulation schemes
(d) None of these ( )

26. In network secruity:
    (a) Data is Protected From Hackers
    (b) Data is Protected From Cracker
    (c) Both a and b
    (d) None of the above ( )

27. In cryptography?
    (a) Secret key is used
    (b) Secret key is not used
    (c) Secret key is damaged
    (d) None of the above ( )

28. In private key cryptography:
    (a) Sender and receiver both must have secret key
    (b) Sender and receiver both need not have a secret key
    (c) Only sender must have the secret key
    (d) Only receiver must have the secret key ( )

29. IDEA stands for:
    (a) International Data Encryption Algorithm
    (b) International Digital Encryption Algorithm
    (c) International Data Entity Authentication
    (d) None of the above ( )

30. Security mechanism is ensured is:
    (a) Detect attack
    (b) Prevent Attack
    (c) Recover From attack
    (d) All of the above ( )

31. Conventional encryption is:
    (a) Symmetric encryption
    (b) Secret key encryption
    (c) Single key encryption
    (d) All of the above ( )

32. In cryptography:
    (a) Plain text is converted into cipher text
    (b) Plain text remains as it is
    (c) Plain text is updated
    (d) None of the above ( )

33. Data Encryption standard is:
    (a) Most widely used scheme
    (b) Rarely used

(c) Not used
(d) None of the above ( )

34. The most commonly used conventional encryption algorithms are:
(a) Block ciphers
(b) Transposition ciphers
(c) Both a and b
(d) None of the above ( )

35. Triple DEA (TDEA) was first proposed by:
(a) tuchman (b) Rivest
(c) both a and b (d) None of the above ( )

36. Session by:
(a) Establishes Logical Connection
(b) Establishes physical connection
(c) Both a and b
(d) None of the above ( )

37. Message authentication code:
(a) Generates small block of data (b) Generates large block of data
(c) Does not generate data (d) None of the above ( )

38. Data Encryption Algorithm:
(a) Generates encrypted version of the message
(b) Generates non-encrypted version of the message
(c) Generates secret keys
(d) None of these ( )

39. Secure hash algorithm developed by:
(a) National Institute of Standards and Technology (NIST)
(b) IEEE
(c) ANSI
(d) None of the above ( )

40. The most widely used public key algorithms are:
(a) RSA (b) Diffie Hellman
(c) Both a and b (d) None of the above ( )

41. Cryptography relates to.......................
(a) Editing
(b) Security
(c) Testing
(d) All of the above ( )

42. Protocol refer to:

(a) Rules
(b) Methods
(c) Both rules and methods
(d) None of the above ( )

43. DES stands for:
(a) Data encryption standard
(b) Data Encryption security
(c) Data Embedded standard
(d) Data Easily substitutable ( )

44. In cryptography...................
(a) Data is encrypted while sending
(b) Data is encrypted while receiving
(c) Data is updated while communication
(d) None of the above ( )

45. Encrypted message is called.............in cryptography:
(a) Plain text (b) Cipher text
(c) Secret text (d) All of the above ( )

46. The message is decrypted at....................end:
(a) Receiver
(b) Sender
(c) Broker
(d) All of the above ( )

47. Authentication refers to:
(a) Verification of user's identity
(b) Checking user's privileges
(c) Auditing user's process
(d) None of the above ( )

48. Encryption protects against:
(a) Attacks (b) Viruses
(c) Manipulation of data (d) All of the above ( )

49. Public key is known to everybody:
(a) Attacks
(b) Viruses
(c) Manipulation of data
(d) All of the above ( )

50. AES stands for:
(a) Advanced Encryption System

(b) Advanced Encryption Solution
(c) Advanced Encryption strategies
(d) Advanced Encryption Standard ( )

51. The sender 'sings' a message as...............
(a) By hand
(b) By speaking
(c) Digital signature
(d) Any of the above ( )

52. CA stands for:
(a) Certified auditing (b) Certification authorities
(c) Cyper Abuses (d) Certified automation ( )

53. Hacking refers to:
(a) Data access without permission
(b) Data updation without permission
(c) Data deletion without permission
(d) All of the above ( )

54. TDES means:
(a) Triple digital Encryption standard
(b) Triple Data Encryption System
(c) Triple Data Encryption Standard
(d) Triple Digital Encryption System ( )

55. DSS stands for:
(a) Digital signature standard
(b) Digital Signature simulation
(c) Digital signature strategies
(d) Digital Signature system ( )

56. Network security ensures.................
(a) Detecting attacks
(b) Preventing attacks
(c) Recovering attacks
(d) All of the above ( )

57. In cryptography receiver encrypts the message and sender decrypts the message:
(a) True
(b) False
(c) Never
(d) Can't say ( )

58. Secure hash algorithm was developed by:

(a) IEE (b) NIST
(c) Never (d) None of the above ( )

59. The process to discover plaintext or key is known as:
(a) Cryptanalysis (b) Symmetric Hash Function
(c) Crypto processing (d) Observation Cryptographic ( )

60. SHF stands for……………………..
(a) Secure Hash function (b) Symmetric Hash Function
(c) Crypto processing (d) Secure Hash file ( )

61. What is the length of key (without padding) in DES?
(a) 64 bits
(b) 128 bits
(c) 72 bits
(d) 56 bits ( )

62. KDC stands for:
(a) Karnaugh Display Cycle
(b) Key Distribution Center
(c) Key Display Cycle
(d) None of these ( )

23. Diffie - Hellman key exchange is vulnerable to:...................
(a) Discrete logarithm
(b) Elliptic curve cryptography
(c) Man in the middle attack
(d) None of these ( )

64. MAC means..................
(a) Message Authorization Code
(b) Message Authentication Code
(c) Message Approximation Code
(d) All of the above ( )

65. SHA-1 is similar to......................
(a) RSA
(b) DES
(c) MD5
(d) Rijndae! ( )

66. In PKI.................
(a) Public key is known, private key is secrete
(b) Private key is knwon, public key is secret
(c) Both keys are known

(d) Both keys are secret ( )

67. Cryptology means...................

(a) Cryptography + Cryptodesign
(b) Cryptography + Cryptanalysis
(c) Cryptography itself known as cryptology also
(d) None of the above ( )

68. RSA stands for.....................

(a) Rivest, Shannon, Admand
(b) Rodger, Shannon, Admand
(c) Rivest, Shamir, Addleman
(d) Rivest, Shannon, Addleman ( )

69. RSA involves very large.........numbers:

(a) Prime (b) Even
(c) Odd (d) Any number ( )

70. Hash collision means................

(a) Two keys for one message
(b) One key for two message
(c) Two different keys for different message
(d) Always the same key ( )

71. ECB stands for:

(a) Emergency Code book (b) Electronic Code Book
(c) Elective Code Book (d) Encrypted Code Book ( )

72. DES involves the following block cipher technique............

(a) ECB
(b) RSA
(c) CBC
(d) SHAI ( )

73. Which of the following is a monoalphabetc cipher?

(a) Caesar Cipher (b) Lucifer cipher
(c) Contradictory cipher (d) Play fair cipher ( )

74. Which of the following is a transposition cipher................

(a) Caesar cipher (b) Vignere Cipher
(c) One time pad (d) Playfair cipher ( )

75. Which is not lreated to cryptography?

(a) ....machines (b) Enigma
(c) Steganography (d) Analytical Engine ( )

76. In stream ciphers..............
(a) One character is read at a time
(b) Two character are read at a time
(c) Eight character are read at a time
(d) 32 characters are read at a time ( )

77. Finding plaintext, without knowing key is known is:
(a) Cryptography
(b) Cryptanalysis
(c) Cryptology
(d) None of the above ( )

78. Which of the following algorithm is not based on block encryption?
(a) DES (b) TDES
(c) RSA (d) AES ( )

79. Which of the following is not used for symmetric encryption ?
(a) RSA (b) DES
(c) SHAI (d) RC4 ( )

80. Which of the following is not the basic principle of cryptography?
(a) Confidentiality
(b) Integrity
(c) Atomicity
(d) Non-repudiation ( )

1. (a)	2. (a)	3. (a)	4. (b)	5. (a)	6. (b)	7. (a)	8. (a)	9. (c)	10. (a)
11. (d)	12. (a)	13. (b)	14. (a)	15. (c)	16. (a)	17. (a)	18. (c)	19. (a)	20. (a)
21. (a)	22. (d)	23. (a)	24. (c)	25. (a)	26. (a)	27. (a)	28. (d)	29. (a)	30. (d)
31. (d)	32. (a)	33. (a)	34. (a)	35. (a)	36. (a)	37. (a)	38. (a)	39. (a)	40. (c)
41. (b)	42. (c)	43. (a)	44. (a)	45. (b)	46. (a)	47. (a)	48. (d)	49. (a)	50. (d)
51. (c)	52. (b)	53. (d)	54. (c)	55. (a)	56. (d)	57. (b)	58. (b)	59. (a)	60. (b)
61. (d)	62. (b)	63. (a)	64. (b)	65. (c)	66. (a)	67. (b)	68. (c)	69. (d)	70. (a)
71. (a)	72. (c)	73. (a)	74. (d)	75. (c)	76. (a)	77. (b)	78. (c)	79. (a)	80. (c)

Key-Terms

Anti-virus

A software program designed to identify and remove a known or potential computer Virus:

API (Application program interface)

An API is the specific methodology by which a programmer writing an application program may make requests of the operating system or another application.

ARP (Address Resolution Protocol)

A protocol used to obtain the physical addresses (such as MAC addresses) of hardware

units in a network environment. A host obtains such a physical address by

Cipher

A mapping algorithm that is applied to a fixed number of characters at a time with an intent of concealing the contents of the message.

Code

A mapping algorithm that is applied to a variable number of characters (according to linguistic entities) at a time with an intent of concealing the contents of the message.

Cryptanalysis

The study of methods of reading enciphered and encoded messages without original knowledge of the cipher method used or the current keys.

Cryptography

The study of methods of enciphering and deciphering messages to conceal the contents of a message.

Cryptology

The study of both cryptography (enciphering and deciphering) and cryptanalysis (breaking or cracking a code system or individual messages).

Deciphering

The procedure of turning enciphered text into plain text with prior knowledge of the algorithms or keys involved. This is what the intended message receiver does.

Decryption

The science of turning enciphered text into plain text without prior knowledge of the algorithms or keys involved. This is what the interceptor or 'cracker' does.

Digraphs

A plaintext character pairing technique that prevents frequency analysis of commonly occurring pairs such as 'qu'. Note that trigraphs (three characters at a time) is an extension of the theme.

Homophones

Several replacement letters for the same letter in plaintext

Key

A word or phrase that modifies the enciphering/deciphering process in such a way that
knowledge of the algorithm alone is insufficient to decipher an enciphered message.

Monoalphabet

A single mapping of plaintext letters to ciphertext letters.
with homophones.

Plaintext

The original message to be encoded or enciphered

Polyalphabet

A method where several mappings of plaintext letters to ciphertext letters occur in a Message:

Public Key Cryptosystem

A system where a pair of keys are used, one freely distributed and the other known only to the recipient.

Steganography

The art of concealing a message's existence. One example would be through the use of
photographic microdots.

Substitution

Enciphering by replacing one letter by another.

Symmetric Key Cryptosystem

A system where both sender and receiver use the same key for enciphering and deciphering.

Transmission Security

The art of concealing an electrically transmitted message through burst encoding or spread spectrum methods.

Transposition

Enciphering by shuffling the order of letters.

Checksum or hash

A checksum is a count of the number of bits in a transmission unit that is included with the unit so that the receiver can check to see whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received.

Circuit-level gateways

Circuit-level gateways run proxy applications at the session layer instead of the application layer. They can't distinguish different applications that run on the same protocol stack. However, these gateways don't need a new module for every new application, either. Circuit-level gateway is a firewall feature which can, when needed, serve as an alternative to packet filtering or application gateway functionality.

Client

A client is the requesting program or user in a client/server relationship. For example, the user of a Web browser is effectively making client requests for pages from servers all over the Web. The browser itself is a client in its relationship with the computer that is getting and returning the requested HTML file.

Cookie

A message given to a Web browser by a Web server. The browser stores the message in a text file called cookie.txt. The message is then sent back to the server each time the browser requests a page from the server.

Cryptography

A branch of complex mathematics and engineering devoted to protecting information from unwanted access. In the context of computer networking, cryptography consists of encryption, authentication, and authorization.

Denial of service attack

A user or program takes up all the system resources by launching a multitude of requests, leaving no resources and thereby "denying" service to other users. Typically, denial-of-service attacks are aimed at bandwidth control.

DHCP (Dynamic Host Configuration Protocol)

DHCP enables individual computers on an IP network to extract their configurations from a server (the 'DHCP server') or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network.The most significant piece of information distributed in this manner is the IP address.

Diffie-Hellman

The Diffie-Hellman Method For Key Agreement allows two hosts to create and share a secret key. VPNs operating on the IPSec standard use the Diffie-Hellman method for key management. Key management in IPSec begins with the overall framework called the Internet Security Association and Key Management Protocol (ISAKMP). Within that framework is the Internet Key Exchange (IKE) protocol. IKE relies on yet another protocol known as OAKLEY and it uses Diffie-Hellman.

DiffServ (Differentiated Services)

Differential service mechanisms allow providers to allocate different levels of service to different users of the Internet. Broadly speaking, any traffic management or bandwidth control mechanism that treats different users differently - ranging from simple Weighted Fair Queuing to RSVP and per-session traffic scheduling - counts. However, in common Internet usage the term is coming to mean any relatively simple, lightweight mechanism that does not depend entirely on per-flow resource reservation.

Digital Certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a

recipient can verify that the certificate is real.

Digital Signature

A digital signature is an electronic rather than a written signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged. Additional benefits to the use of a digital signature are that it is easily transportable, cannot be easily repudiated, cannot be imitated by someone else, and can be automatically time-stamped.

DNS (Domain Name System)

The Internet protocol for mapping host names, domain names and aliases to IP addresses.

DNS spoofing

Breaching the trust relationship by assuming the DNS name of another system. This is

usually accomplished by either corrupting the name service cache of a victim system or by compromising a domain name server for a valid domain.

Domain

The unique name used to identify an Internet network.

Domain name server

A repository of addressing information for specific Internet hosts. Name servers use the domain name system to map IP addresses to Internet hosts.

DSS (Digital Signature Standard

The Digital Signature Standard (DSS) is a cryptographic standard promulgated by the

National Institute of Standards and Technology (NIST) in 1994. It has been adopted as the federal standard for authenticating electronic documents, much as a written signature verifies the authenticity of a paper document.

e-business

e-business" ("electronic business," derived from such terms as "e-mail" and "e-commerce") is the conduct of business on the Internet, not only buying and selling but also servicing customers and collaborating with business partners.

e-commerce

e-commerce (electronic commerce or EC) is the buying and selling of goods and services on the Internet, especially the World Wide Web. In practice, this term and e-business are often used interchangeably. For online retail selling, the term e-tailing is sometimes used.

email client

An application from which users can create, send and read e-mail messages.

email server

An application that controls the distribution and storage of e-mail messages.

Encryption

Scrambling data in such a way that it can only be unscrambled through the application

of the correct cryptographic key.

Ethernet

A local-area network (LAN) protocol developed by Xerox Corporation in cooperation with DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 100Mbps.

Firewall

A firewall is a program that protects the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet will want a firewall to prevent outsiders from accessing its own private data resources.

Firewall denial-of service

The firewall is specifically subjected to a denial-of-service attack.

FTP (File Transfer Protocol)

FTP is the simplest way to exchange files between computers on the Internet. Like the

Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, FTP is anapplication protocol that uses the Internet's TCP/IP protocols.

Gateway

A gateway is a network point that acts as an entrance to another network. In a company network, a proxy server acts as a gateway between the internal network and the Internet. A gateway may also be any machine or service that passes packets from one network to another network in their trip across the Internet.

Hacker

Hacker is a term used by some to mean "a clever programmer" and by others, especially journalists or their editors, to mean "someone who tries to break into computer systems."

Highjacking or hijacking

Control of a connection is taken by the attacker after the user authentication has been established.

HMAC (Header Message Authentication Codes)

HMAC is a hash function based message authentication code that was designed to meet the requirements of the IPsec working group in the IETF, and is now a standard.

HTML (HyperText Markup Language)

A standard set of commands used to structure documents and format text so that it can

be used on the Web.

HTTP (HyperText Transfer Protocol)

HTTP is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols(which are the basis for information exchange on the Internet), HTTP is an application protocol.

HTTPS (Secure Hypertext Transfer Protocol)

The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the World Wide Web. HTTPS is http using a Secure Socket Layer (SSL).

Hybrid Auth

The Hybrid Auth extension allows the asymmetric use of digital certificates between client and server. The client verifies the authenticity of the server's credentials (certificate), and the server verifies the authenticity of the client's credentials.

Companies benefit from the interoperability of standards-based IPSec with IKE as well as the increased security of the PKI at the central site, with no disruption to remote users.

IP (Internet Protocol)

The Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one address that uniquely identifies it from all other computers on the Internet.

IP spoofing

An attack where the attacker impersonates a trusted system by using its IP network address.

IP hijacking

An attack where an active, established session is intercepted and taken over by the attacker. May take place after authentication has occurred which allows the attacker to

assume the role of an already authorized user.

IPSec (Internet Protocol Security)

A developing standard for security at the network or packet processing layer of network communication. IPSec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well.

ISDN (Integrated Services Digital Network

A set of communications standards allowing a single wire or optical fibre to carry voice,digital network services and video. ISDN gives a user up to 56 kbps of data bandwidth on a phone line that is also used for voice, or up to 128 kbps if the line is only used for data.

Java

Java is a programming language expressly designed for use in the distributed environment of the Internet. It was designed to have the "look and feel" of the C++ language, but it is simpler to use than C++ and enforces a completely object-oriented view of programming. Java can be used to create complete applications that may run on a single computer or be distributed among servers and clients in a network. It can also be used to build small application modules or applets for use as part of a Web page.

Applets make it possible for a Web page user to interact with the page.

K Kerberos

Kerberos was created by MIT as a solution to network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

Key

In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text. The length of the key generally

determines how difficult it will be to decrypt the text in a given message.

Key Management

The establishment and enforcement of message encryption and authentication procedures, in order to provide privacy-enhanced mail (PEM) services for electronic mail transfer over the Internet.

MAC (Media Access Control)

On a network, the MAC (Media Access Control) address is your computer's unique hardware number. The MAC address is used by the Media Access Control sublayer of the Data-Link Control (DLC) layer of telecommunication protocols. There is a different MAC sublayer for each physical device type. The Data-Link Layer is the protocol layer in a program that handles the moving of data in and out across a physical link in a network.

Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, GIF file, URL request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).

Packet Filters

Packet filters keep out certain data packets based on their source and destination addresses and service type. Filters can be used to block connections from or to specific hosts, networks or ports. Packet filters are simple and fast. However, they make decisions based on a very limited amount of information.

Packet Sniffing

Intercepting packets of information (including such things for example as a credit card number) that are traveling between locations on the Internet.

Password-based attacks

An attack where repetitive attempts are made to duplicate a valid log-in and/or password sequence.

PGP (Pretty Good Privacy)

A cryptographic product family that enables people to securely exchange messages, and to secure files, disk volumes and network connections with both privacy and strong authentication.

KCS (Public-Key Cryptography Standards)

The Public-Key Cryptography Standards are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography. First published in 1991 as a result of meetings with a small group of early adopters of public-key technology, the PKCS documents have become widely referenced and implemented.

PKI (Public Key Infrastructure)

A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

Platform attack

An attack that is focuses on vulnerabilities in the operating system hosting the firewall.

PPP (Point-to-Point Protocol)

Point-to-Point Protocol (PPP) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server.

POP3 (Post Office Protocol 3)

An e-mail protocol used to retrieve e-mail from a remote server over an Internet connection.

Private Key

In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. A more recent alternative is to use a combination of public and private keys. In this system, a public key is used together with a private key.

Protocol

A special set of rules for communicating that the end points in a telecommunication connection use when they send signals back and forth. Protocols exist at several levels in a telecommunication connection. There are hardware telephone protocols. There are protocols between the end points in communicating programs within the same computer or at different locations. Both end points must recognize and observe the protocol.Protocols are often described in an industry or international standard.

Protocol Attacks

A protocol attack is when the characteristics of network services are exploited by the attacker. Examples include the creation of infinite protocol loops which result in denial of services (e.g., echo packets under IP), the use of information packets under the Network News Transfer Protocol to map out a remote site, and use of the Source Quench protocol element to reduce traffic rates through select network paths.

Proxy

An agent that acts on behalf of a user, typically accepting a connection from a user and completing a connection on behalf of the user with a remote host or service. See also gateway and proxy server.

Proxy Server

A proxy server is one that acts on behalf of one or more other servers, usually for screening, firewall, caching, or a combination of these purposes. Gateway is often used as a synonym for "proxy server." Typically, a proxy server is used within a company or enterprise to gather all Internet requests, forward them out to Internet servers, and then receive the responses and in turn forward them to the original requestor within the company.

Public Key

A public key is a value provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures. The use of combined public and private keys is known as asymmetric encryption. A system for using public keys is called a public key infrastructure (PKI).

QoS (Quality of Service)

On the Internet and in other networks, QoS is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information.

Rijndael Algorithm

The algorithm used by the Advanced Encryption Standard (AES). It's characteristics are very good performance in both hardware and software across a wide range of computing environments regardless of its use in feedback or non-feedback modes. Rijndael's key setup time is excellent, and its key agility is good. It has very low memory requirements making it very well suited for restricted-space environments, in which it also demonstrates excellent performance. Rijndael's operations are among the easiestto defend against power and timing attacks.

RIP (Routing Information Protocol)

The oldest routing protocol on the Internet and the most commonly used routing protocol on local area IP networks. Routers use RIP to periodically broadcast which networks they know how to reach.

Signatures

Viruses employ signatures by which they identify themselves to themselves and thereby avoid corrupting their own code. Standard viruses, including most macro viruses, use character-based signatures. More complex viruses, such as polymorphic viruses, use algorithmic signatures.

SLIP

SLIP is a TCP/IP protocol used for communication between two machines that are previously configured for communication with each other. SLIP has been largely supplanted by PPP.

SSL (Secure Sockets Layer)

A program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping your messages confidential ought to be contained in a program layer between an application

(such as your Web browser or HTTP) and the Internet's TCP/IP layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer.

Symmetric Encryption

The oldest form of key-based cryptography is called secret-key or symmetric encryption.

In this scheme, both the sender and recipient possess the same key, which means that both parties can encrypt and decrypt data with the key.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The standard family of protocols for communicating with Internet devices.

Telnet

A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You
can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console

Triple DES (3DES)

Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key.

Token Ring

A type of computer network in which all the computers are arranged (schematically) in a circle. A token, which is a special bit pattern, travels around the circle. To send a message, a computer catches the token, attaches a message to it, and then lets it continue to travel around the network.

Tracking

The logging of inbound and outbound messages based on a predefined criteria. Logging is usually done to allow for further analysis of the data at a future date or time.

Trojan horse

A software entity that appears to do something quite normal but which, in fact, contains a trapdoor or attack program.

UDP (User Datagram Protocol

A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.

URL (Uniform Resource Locator)

An address in a standard format that locates files (resources) on the Internet and the Web. The type of resource depends on the Internet application protocol. Using the World Wide Web's protocol, the Hypertext Transfer Protocol (HTTP) , the resource can be an HTML page (like the one you're reading), an image file, a program such as a **CGI**
application or Java applet, or any other file supported by HTTP. The URL contains the
name of the protocol required to access the resource, a domain name that identifies a

specific computer on the Internet, and a hierarchical description of a file location on the computer.

VBScript (Visual Basic Script)

VBScript is an interpreted script language from Microsoft that is a subset of its Visual Basic programming language. VBScript can be compared to other script languages designed for the Web such as Netscape's JavaScript

Virus

A virus is a piece of programming code inserted into other programming to cause some unexpected and, for the victim, usually undesirable event. Viruses can be transmitted by downloading programming from other sites or be present on a diskette. The source of the file you're downloading or of a diskette you've received is often unaware of the virus. The virus lies dormant until circumstances cause its code to be executed by the computer. Some viruses are playful in intent and effect and some can be quite harmful,erasing data or causing your hard disk to require reformatting.

Virus Scanner

A program that searches files for possible viruses, including email and attachments.

VPN (Virtual Private Networking)

A VPN is a technology that overlays communications networks with a management and security layer. Though VPN technology, network managers can set up secure relationships while still enjoying the low cost of a public network such as the Internet.

WAP (Wireless Application Protocol)

An open global standard for communications between a mobile handset and the Internet or other computer applications as defined by the WAP forum.

Web Attack

Any attack from the outside aimed at Web server vulnerabilities.

Web Browser

A Web browser is a client program that uses the Hypertext Transfer Protocol (HTTP) to make requests of Web servers throughout the Internet on behalf of the browser user.

Worm

A type of virus that disables a computer by creating a large number of copies of itself within the computer's memory, forcing out other programs. Worm viruses are generally constructed to also copy themselves to other linked computers.

X.509

The most widely used standard for defining digital certificates. X.509 is actually an ITU Recommendation, which means that has not yet been officially defined or approved.As a result, companies have implemented the standard in different ways. For example, both Netscape and Microsoft use X.509 certificates to implement SSL in their Web servers and browsers. But an X.509 Certificate generated by Netscape may not be readable by Microsoft products, and vice versa.

Bibliography

1.Cryptography by Atul Kahate
Tata McGraw-Hill Education, 2003

2. Network Security and Essentials by William Stalling
Pearson Education Asia 2003

3.Cryptography and network security principle and practices by William Stalling
Prentice hall