AS-2362

MCA - V th sem Examination, 2013

Network Security

Paper : MCA - 504

Maximum Marks : 60

Note : Draw Diagram where ever necessary. Proper Explaination and Definition is necessary.

Section — A

1. (a) Fill in the blanks : 5×2 = 10

(i) In Data Encryption standard IP stands for Initial Permutation.

(ii) In Euclidean algorithm, gcd stands for Greatest common Divisor.

(iii) In symmetric cryptography Private key is used as secret key.

(iv) In Hill cipher, Full Name of Hill is Lester Hill.

(v) An active attack attempts to alter system resources or affect their operations.

1. (b) True / False 5×2 = 10

(vi) AES stands for Advanced Encryption System. [False]

(vii) In digital signature, the sender signs the message with it's Public Key. [False]

(viii) Relative Frequency Of letters is used in Monoalphabetic Cipher. [True]

(ix) Number 12 is a Prime Number. [False]

(x) Key 4312567 is used in substitution Techniques. [False]

Section - B

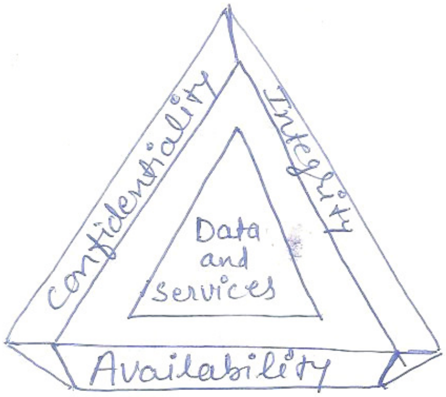
4×10 = 40

Qu-② Draw and explain OSI security Architecture ?

Ans -

(a) Explaination about Security Need.

(b) Security Requirement Triad.



(i) Confidentiality : Preserving authorised restrictions on information access and disclosure., including means for Protecting Personal Privacy and Proprietary information.

(ii) Integrity :- Guarding against improper information, modification or destruction, including ensuring information non-repudiation and authenticity.

(iii) Availability :- Ensuring timely and reliable access to and use of information.

c) OSI security Architecture

i) Security attack :- Any action that compromises the security of information owned by an organization.

(ii) Security Mechanism :- A Process that is designed to detect, Prevent or recover from a security attack.

(iii) security service :- A Processing or communication service that enhances the security of the data Processing systems and the information transfers of an Organization.

i) security attack :-

a) Definition

b) Purpose

c) figure and explaination

Two Types of attack.

I) Active Attack

- Masquerade
- Replay
- Modification of message
- Denial of service

II) Passive Attack ├─ Release of message contents
└─ Traffic Analysis

Masquerade → when one entity Pretends to be a different entity.

Replay → Involves the Passive capture of a data unit and its subsequent retransmission to Produce an unauthorized effect.

Modification of Message → Some Portion of a legitimate message is altered or that message are delayed or reordered to Produce an unauthorized effect.

Denial of service → Prevents or inhibits the normal use of management of communication facilities.

(Explain above categories with figure and Explaination and advantages)

(ii) Security Mechanism →
⇒ Structure
⇒ Importance and Explaination.

(iii) security services :- X.800 defines a security service as a service Provided by a Protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfer.

security service (X.800)

a) Authentication
1) Peer Entity Authentication
2) Data Origin Authentication

b) Access control :- The Prevention of unauthorized use of a resource.

c) Data confidentiality :- The Protection of data from unauthorized disclosure.

i) connection confidentiality
ii) connectionless confidentiality
iii) Selective - field confidentiality
iv) Traffic flow confidentiality

d) Data Integrity :- The assurance that data received are exactly as sent by an authorized entity.

i) connection Integrity with Recovery.
ii) connection Integrity without recovery.
iii) Selective field connection Integrity.
iv) connectionless Integrity.
v) Selective - field connectionless Integrity.

e) Non - repudiation :- Provides Protection against denial by one of the entities involved in a communication of having Participated in all or Part of the communication.

i) Non-repudiation, origin.
ii) Non-repudiation, Definition.

Security Mechanism :- The mechanism are divided into those that are implemented in a Specific Protocol layer and those that are not specific to any other Protocol layer or security service.

Specific Security Mechanism :- It is incorporated into the appropriate Protocol layer inorder to Provide some of the OSI security services.

1) Encipherment 2) Digital signature 3) Access control
4) Data Integrity 5) Authentication Exchange
6) Traffic Padding 7) Routing control 8) Notarization

Pervasive security Mechanism

→ Trusted functionality
→ security Label
→ Event Detection.
→ Security Audit Trail
→ Security recovery

Qu-3 what are Block ciphers? Explain it with an example?

Ans - A block cipher is an encryption/decryption scheme in which a block of Plaintext is treated as a whole and used to Produce a ciphertext block of equal length. Many block ciphers have a Feistel structure such structure consists of a number of identical rounds of Processing. In each round, a substitution is Performed on one half of the data being Processed, followed by a Permutation that interchanges the two halves. The original key is expanded so that a different key is used for each round.

⇒ Explaination about Feistel cipher structure.

⇒ Figure of Feistel Encryption and Decryption.

Block cipher Modes of operation

→ Electronic codebook mode
→ Cipher Block chaining mode
→ Cipher feedback mode
→ Output feedback Mode
→ Counter mode

Examples

1) DES 2) AES 3) Double DES
4) Triple DES.

⇒ Introduction
⇒ Explaination of concept
⇒ figure used
⇒ Algorithm & Logic used
⇒ structure used
⇒ Explaination of various rounds.

Qu-(4) what are the Principles of Public key cryptosystem ? Explain.

Ans- Asymmetric encryption is a form of cryptosystem in which encryption and decryption are Performed using the different keys - one a Public key and one a Private key. It is also known as Public-key encryption. It transforms Plaintext into ciphertext using a one of two keys and a decryption algorithm, the Plaintext is recovered from the ciphertext. confidentiality, authentication or both is used in asymmetric encryption. The most widely used Public-key cryptosystem is RSA Algorithm.

Principles of Public key cryptosystems

The concept of Public key cryptosystems evolved from two types of Problems face on Symmetric cryptography that was firstly key distribution and secondly Digital signatures.

Basic Principles for Public cryptography

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a Public register or other accessible file. This is the Public key. The companion key is kept Private.
3. If first user wishes to send a confidential message to second user, then first user encrypts the message using second user's Public key.
4. when second user receives the message, then he decrypts using his Private key.

Figures Needed for supporting Principles of Public key cryptography

a) Public key cryptosystem : secrecy
b) Public key cryptosystem : Authentication
c) Public key cryptosystem : Authentication & secrecy.

Various Applications for Public-key cryptosystems

use of Public-key cryptosystems fall into three categories :

a) Encryption / Decryption (Explaination)
b) Digital signature (Explaination)
c) Key Exchange (Explaination)

Qu-⑤ what do you mean by Playfair cipher? Explain it's concept also ?

Ans — The two basic building blocks of all encryption techniques are substitution and TransPosition.

Substitution Technique :- In this technique, the letters of Plaintext are replaced by other letters or by numbers or symbols. If the Plaintext is viewed as a sequence of bits, then substitution involves replacing Plaintext bit Patterns with ciphertext bit Patterns.

TransPosition Technique :- This technique systematically transPose the Positions of Plaintext element. Here, mapping is achieved by Performing some sort of Permutation on the Plaintext letters.

Playfair cipher :- The best known multiple-letter encryption cipher is the Playfair, which treats diagram in the Plaintext as single units and translates these units into ciphertext diagrams. It is based on the use of a 5×5 matrix of letters constructed using a keyword.

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

The following rules are adopted

1. Repeating Plaintext letters that are in the same Pair are separated with a filler letter such as x, so that balloon would be treated as balxloon.

2. Two Plaintext letters that fall in the same row the matrix are each replaced by the letter to the right, with the first element of the row circulary following the last.

eg → ar is encrypted as RM.

3. Two Plaintext letters that fall in the same column are each replaced by the letter beneath. with the top element of the column circularly following the last.

eg → mu is encrypted as CM.

4. Otherwise, each Plaintext letter in a Pair is replaced by the letter that lies in its one row and the column occupied by the other. Plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM).

Qu-(6) write a short note on secure Electronic Transaction (SET)?

Ans - SET is an open encryption and security specification designed to Protect credit card transactions on the Internet. It is a set of security Protocols and formats that enables users to employ the existing credit card Payment infrastructure on an open network, such as Internet in a secure fashion.

key features of SET

a) confidentiality of information b) Integrity of data
c) cardholder account authentication d) Merchant Authentication.

SET Participants

a) cardholder b) Merchant c) Issuer d) Acquirer
e) Payment gateway f) certification authority.

SET Diagram used for Explaination

SET Transaction Types

a) cardholder registeration b) Merchant registeration
c) Purchase request d) Payment Authorization
e) Payment capture f) Purchase inquiry g) Authorisation reversal h) credit i) Payment Gateway certificate request j) Batch administration k) Error Message

SET will be explained with below topics also.

1) OLAP (online Analytical Processing)
2) OLTP (online Transaction Processing)
3) OLCP (online control Processing)

Examples

1) credit cards 2) e- banking 3) Master card
4) Visa cards.

Qu-(7) write in brief about Transposition Techniques?

Ans - This technique Systematically transpose the Positions of Plaintext elements. Here, mapping is achieved by Performing some sort of Permutation on the Plaintext letters.

Transposition technique is divided into two techniques
1) Rail fence Technique 2) Rectangle Technique

1) Rail-fence Technique :- Here, the Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Eg :- " meet me after the toga Party" is written as

```
m   e   m   a   t   r   h   t   g   p   r   y
  e   t   e   f   e   t   e   o   a   a   t
```

encrypted message is

MEMATRHTGPRYETEFETEOAAT

Rectangle Technique :- This technique is used to write the message in a rectangle, row by row and read the message off, column by column, but Permute the order of the columns. The order of the columns then becomes the key to the algorithm.

Example

key :

4	3	1	2	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

ciphertext : TTNAAPTMTSUOAODWCOIXKNLYPETZ

Thus, with 28 letters in the message, the original sequence of letters is

01 02 03 04 05 06 07 08 09 10 11 12 13 14

15 16 17 18 19 20 21 22 23 24 25 26 27 28

Qu-(8) Explain Intrusion Detection system?

Ans - Intrusion detection systems have been developed to Provide early warning of an intrusion so that defensive action can be taken to Prevent or minimize damage. It involves detecting unusual Patterns of activity or Patterns of activity that are known to correlate with intrusions.

One important element of intrusion Prevention is Password management, with the goal of Preventing unauthorized users from having access to the Passwords of others.

Three classes of intruders :-

1) Masquerader :- An individual who is not authorized to use the computer and who Penetrates a system's access controls to exploit a legitimate user's account.

2) Misfeasor :- A legitimate user who access data, Programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her Privileges.

3) clandestine user :- An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

Intrusion Techniques :-

a) one - way Function b) Access control

Following approaches to intrusion detection

1. statistical anomaly detection -> Threshold detection
   -> Profile based
2. Rule - based detection -> Anomaly detection
   -> Penetration Identification

=> Explaination with example
=> Diagram used
=> Advantages
=> concept of Distributed Intrusion Detection
=> Intrusion Detection Exchange format
=> Password Protection Management

— X ———— X ——— X ———

By: H. S. P. Tende