Higher National Diploma in Information Technology

Second Year, First Semester Examination – 2017

HNDIT 2301 - Operating Systems & Computer Security - Answer

Instructions for Candidates:	No. of questions : 05
Answer Any Four (04) Questions Only	No. of pages : 03
All question carry equal marks	Time : **Two (02) hours**

Question 01

I. Explain the term cryptosystem. (2 marks)

The art of science encompassing the principals and methods of transforming an intelligible message into unintelligible and then transforming that message basic to its original form

II. What do you mean by cryptanalysis? (3 marks)

The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key

III. List out the three (3) concepts associate in information security and indicate one security services or mechanism for each. (6 marks)

Data confidentiality

Encryption

Non repudiation

Digital signature

Integrity

Digital signature /message authentication code

IV. Briefly explain the following terms.

Vulnerability : A weakness in the security system

Security Control: A set of circumstances that has the potential to cause loss or harm

Security Service: A tool or technique that is used to implement a security service.

(3*3= 09 marks)

V. Encrypt the message "BEST QUESTIONS" using Caesar encryption algorithm defined as C=E(P)=(Pi+3) mod 26. (5 marks)

7 mod 26 = 7 = H
3 mod 26 = 3 = D
21 mod 26 = 21 = S
27 mod 26 = 1 = B
19 mod 26 = 19 = T
23 mod 26 = 23 = X
7 mod 26 = 7 = H
21 mod 26 = 21 = V
22 mod 26 = 22 = W
11 mod 26 = 11 = L
17 mod 26 = 17 = R

16 mod 26 = 16 = Q
The encrypted message is HDVBTXHVWLRQ

(Total 25 Marks)

Question 02

I. What is encryption and decryption? (4 marks)

Encryption

The process of converting plaintext to cipher text

Decryption:-

The process of converting cipher text back into plaintext

II. List four basic properties of good encryption algorithm. (4 marks)

Provides high level of security (full or part of the text will not be revealed by analyzing encrypted data. Keys will not be found)
Efficient resources (memory usage etc) and time.
Economically cheep to implement as software or hardware tokens
Completely specified and is available for public access
Simple and easy to understand

III. What are the three (3) criteria to categories encryption methods? (6 marks)

Number of keys
- Pirate Key
- Public Key

How input process
- Stream cipher
- Block cipher

Operations or technique
- Substitution
- Transposition/permutation

IV. Compare and contrast between Symmetric and Asymmetric key encryption algorithms. (2x3=6 marks)

Secret Key (Symmetric*)*	Public Key (Asymmetric*)*
Number of keys 1	Number of keys 2
Must be kept secret	One key must be kept secret; the other can be freely exposed
Used in secrecy and integrity of data	Used in Key exchange, authentication
Fast	Slow

V. Write C++ programming language code to encrypt a given plain text using Caesar cipher. (5 marks)

```
char plaintext[] = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
int key =3;
int i=0;
for(i=0;i<26;i++)
        {
        cout<<char((65+(int(plaintext[i])-65+key)%26));
        }
```

Question 03

I. Give acronyms for the following security protocols and standards (5 marks)

a) S/MIME - Secure/Multipurpose Internet mail Extensions
b) PGP - Pretty Good Privacy
c) SET - Secure Electronic Transactions
d) TLS - Transport Layer Protocol
e) SSL - Secure Socket Layer

II. Give two security protocols to secure the Email. (4 marks)

S/MIME and PGP

III. Write the components of SET? (4 marks)

Card holder
Merchant
Issuer
Acquirer
Payment Gateway
Certificate Authority

IV. List three advantages of SET. (6 marks)

i. Eliminates the need for a third party to monitor Internet credit card transactions. This will lower the cost of doing credit card business over the Internet.
ii. Strong encryption and authentication scheme to be used.
iii. Merchant does not have access to the buyer's credit card number.
iv. Merchants do not have a waiting period for receiving payment, as with First Virtual. The merchant's bank account gets credited within in the usual time frame for credit card transactions.
v. Is backed by MasterCard and Visa.

V. List three ways to secure an Email. (6 marks)

i. Use a secure email client
ii. Always use text
iii. Use free Webmail accounts for subscriptions and postings
iv. Use additional multi-layered defenses
v. Encrypt sensitive emails

(Total 25 Marks)

Question 04

I. List three (3) limitations of firewall? (3 marks)

a. Not all firewalls offer full protection against computer viruses
b. Firewalls can't stop a hacker from masquerading as an employee
c. cannot protect from attacks bypassing it
    i. eg sneaker net, utility modems, trusted organisations, trusted services (eg SSL/SSH)
d. cannot protect against internal threats
    i. eg disgruntled or colluding employees
e. cannot protect against access via WLAN
    i. if improperly secured against external use
f. cannot protect against malware imported via laptop, PDA, storage infected outside

II. List four (4) basic types of firewall's names. (4 marks)

a. Packet filters
b. Stateful Packet filters
c. Application level gateway/ Proxy
d. Circuit level gateway

III. Briefly describe the term malicious software. (2 marks)

Software designed to do something that user did not intend to do

IV. Briefly describe the two categories of malicious code (4 marks)

a. Independent :
Self contained programs that can be scheduled and run by the OS.
Programs that can exist independently of another program.
b. Needs host:
Programs that cannot exist independently of another program

V. Write the short notes for the followings (12 marks)

a) Password Guessing

Password Guessing is common attacks

- one of the most common attacks

- attacker knows a login (from email/web page etc)
- then attempts to guess password for it
  - defaults, short passwords, common word searches
  - user info (variations on names, birthday, phone, common words/interests)
  - exhaustively searching all possible passwords
- check by login or against stolen password file
- success depends on password chosen by user
- surveys show many users choose poorly

b) password capture

Another attack involves password capture

Watching over shoulder as password is entered

Using a Trojan horse program to collect

Monitoring an insecure network login

eg. Telnet, FTP, web, email

Extracting recorded info after successful login (web history/cache, last number dialed etc)

c) Biometric authentication

Retina Pattern,

Iris Scan,

Fingerprint,

Handprint,

Voice Pattern,

Keystroke Biometric Authentication

d) DoS & DDoS attacks

DoS:

The idea of DOS attack is to reduce the quality of service offered by server, or to crash server with heavy work load. DoS (Denial of Service) attack does not involve breaking into the target server. This is normally achieved by either overloading the target network or target server, or by sending network packets that that may cause extreme confusion at target network or target server.

DDoS:

A Distributed Denial of Service (DDoS) attack is a type of Denial of Service (DoS). In Distributed Denial of Service (DDoS) attack multiple systems flood the bandwidth or overload the resources of a targeted server.

(Total 25 Marks)

Question 05

I. Define the following terms.

a) Digital certificate: Attachment to an email, or encoded data embedded in a webpage, which serves as a guaranty that the parties to a transaction are who they claim to be. Digital certificate is issued by an independent trusted Certification Authority. (02marks)

b) Digital signature: Binary coded that**,** like a handwritten signature, authenticates and executes a document and identifies the signatory. (02 marks)

II. List out four (4) possible digital certificate types. (04 marks)

a. Digital signature
b. Key Encryption
c. Object signing
d. Certificate signing
e. CRL signing

III. Write the contents of a “Digital Certificate"? (04 marks)

a. Version
b. Subjects
c. Issuers
d. Validity period
e. Public key
f. Algorithms used
g. Certificate extensions such as Key usage, CRL distribution point and Authority information access

IV. Write the two (2) vulnerabilities in general purpose operating systems. (04 marks)

a. Multi tasking/ multi processing- course buffer overflows
b. Remote login- allows remote attackers to control
c. Resource (File and Print) Sharing - allows remote attackers to access
d. Auto run - Allows local attackers to specify an alternate program to execute.
e. Programmability- attacker can execute harm full code(Active X, Scripting)

V. Write the security features in trusted operating systems. (04 marks)

a. Memory protection
b. Controlled access/ Access permission
c. Auditing& accountability

VI. Define hashing in computer security and list two different hashing algorithms.

When referring to security, hashing is a method of taking data, encrypting it, and creating unpredictable, irreversible output.
Hashing algorithms: MD2, MD5, SHA, and SHA-1

(03+02 =05marks)

(Total 25 Marks)