Seat No.: _____ Enrolment No._____

# GUJARAT TECHNOLOGICAL UNIVERSITY

**M.E –I$^{st}$ SEMESTER–EXAMINATION – JULY- 2012**

**Subject code: 710104N** **Date: 11/07/2012**

**Subject Name: Information Security**

**Time: 2:30 pm – 05:00 pm** **Total Marks: 70**

## Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

**Q.1** **(a)** Encrypt using a one round version of DES. Key K is "133457799BBCDFF1" and message is "0123456789ABCDEF"; **07**

a) Derive $K_1$ the first round subkey.
b) Derive $L_0$, $R_0$
c) Expand $R_0$ to get $E[R_0]$
d) Calculate $A= E[R_0] \otimes \mathbf{K_1}$

**Permuted Choice One (PC-1)**

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 Two (PC-2)**

| | | | | | |
|---|---|---|---|---|---|
| 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 |

**(b)**

(i)When an attacker compromises a system, What does he do to remove evidence of an attack? What is a repudiation attack? **02**

(ii) How can an attacker come to know about web server type and versions? **02**

(iii) Write the snort rules for the following. **03**

a) Alert on traceroute attempts.
b) To detect invalid ICMP type values that are sometimes used in denial of service and flooding attacks

**Q.2** **(a)**

(i) Generate the plaintext, if the cipher text is "tepdmieorkdnejtyty" and keyword is "jitter". Use playfair encryption scheme. 04

03

(ii) Consider the set $\mathbf{Z}_4$ consisting of the numbers 0, 1, 2, 3 where addition and multiplication are defined as follows . For any $x$, $y$ in $\mathbf{Z}_4$, $x + y$ is defined to be their sum in **Z** (the set of *all integers*) mod 4. For any $x$, $y$ in $\mathbf{Z}_4$, $xy$ is defined to be their product in **Z** (the set of *all integers*) mod 4. **Is** $\mathbf{Z}_4$ a ring under these operations?

**(b)** Explain the three firewall technologies and compare these firewall technologies. **07**

**OR**

**(b)** Explain the two modes of intrusion detection. Do a state based analysis for Trojan horse installation attack. **07**

**Q.3 (a)**

(i) What is the strength of the Vigenère Cipher? Is it impossible for Cryptanalyst to decrypt the text generated by Vigenère Cipher? **04**

(ii) What are the observations from following commands. **03**

```
#netstat –ap
Active Internet Connections(servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address
State        PID/Program
name
tcp          0        0  *:pop3          *.*
LISTEN   2295/xinetd
#ps –aux|grep pop3
root     2307    0.0    0.0     3568    624    pts/2    S
07:44    0.00    grep pop3
```

**(b)**

(i) Write the Euclidean algorithm to find the greatest common divisor of two polynomials. **04**

(ii) Write extended Euclidean algorithm to find multiplicative inverse. **03**

**OR**

**Q.3 (a)**

(i) How is the S-box constructed in Advanced Encryption Standard(AES)? **04**

(ii)What are the observations from following commands? **03**

```
#ls  -l fake_exe
-rwxr-xr-x        1 root     root        0 Jun 13 12:25
fake_exe
#ls  -l fake_exe
-rwsr-sr-x        1 root     root        0 Jun 13 12:25
fake_exe
```

**(b)**

(i) Write examples of replay attack. List three approaches to deal with replay attacks. **04**

(ii) What is suppress-replay attack? **03**

**Q.4 (a)**

(i)List the common sources that cause threat of elevation of privileges. **04**

(ii)Explain the term **03**

a. Tampering

b) Phishing

**(b)**

(i) How non essential services help attackers? **04**

(ii) What will be the observation with following command? **03**

sc.exe \\192.168.1.1 queryex | findstr "SERVICE_NAME"

**OR**

**Q.4 (a)**

(i) Which client level counter measures can be taken to help mitigate the threat of malicious attachments? **04**

(ii) Explain the term **03**

a) Web Beacons

b) Reversible Encryption

**(b)**

(i) Prove Fermat's theorem **04**

$a^{p-1} \equiv 1 (\text{mod } p)$

(ii) What will be the observation with following command? **03**

Net.exe user TestUser /DOMAIN

**Q.5 (a)**

(i) Write the four approaches to attack the RSA algorithm. **04**

(ii) Explain the basic uses of Message Authentication code(MAC). **03**

**(b)**

(i) Domain name system(DNS) query and response messages are sent over TCP or UDP? Which port is used? **02**

(ii) What "Type" of DNS queries can be? Does the query message contain any "answers"? **02**

(iii) How many answers are provided in DNS response message? What do each of these answers contain? **03**

**OR**

**Q.5 (a)**

(i) What characteristics are needed in a secure hash function? **04**

(ii) What is the difference between weak and strong collision resistance? **03**

**(b)**

(i) In HTTP GET, if the response is long HTML file, that does not fit in one TCP packet then how http handles it? **02**

(ii) How does http do authentication? **02**

(iii) How can http version of browser and server be checked? **03**

**********