CS DEPT
MILITARY COLLEGE OF SIGNALS, NUST
SOLUTION NETWORK SECURITY
BESE-14

Q1. During the enciphering of a message using DES algorithm, the following 48 bit data is input to the S-boxes. For this input find the binary output of S-box 2 and 6.

11010101 01010111 11110101 11010000 00010101 11011111 **[2+2]**

```
S-Box 2:
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
```

```
S-box 6:
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
```

Answer: **S-Box 2 output = 0001**

S-Box 6 output = 1010

Q2. During the enciphering process the following matrix is obtained using AES algorithm after substitution is performed on the input message. **[2+5]**

Message after substitution:

53	CA	70	0C
B7	D6	DC	D0
F8	32	51	04
79	63	BA	68

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

You are required to perform the following operations on the above data.

a. Shifting of Rows
b. The first two bytes (in hexadecimal) obtained after applying Mix Column Transformation.

Answer:

a)

53	*CA*	70	0*C*
*D*6	*DC*	*D*0	*B*7
51	04	*F*8	32
68	79	63	*BA*

b) **Without applying row shift specified in part "a" answer is FF 4C**
After applying row shift answer is E4 65

Q3. Suppose an adversary listen to an encrypted communication and some how finds that cipher text 58 corresponds to a plain text 16. Moreover, he learns that RSA algorithm was used for the encryption of the message and the public key used was (7, 77). Find the private key based on the known information. **[6]**

Answer: **Private key (43, 7, 11)**

Q4. The following cipher is obtained using PlayFair Cipher algorithm. **[6]**

SHBWHRMXXEWPMCICRDSHIC

Find the plaintext if the key is: MIDTERM EXAM

Answer: **PLAYFAIR CIPHER EXAMPLE**

Q5. With the help of a small network diagram, explain how ICMP based route spoofing attack can be launched. What measures should be taken to avoid such attacks. **[5]**

Answer:

Here's how a route spoof can occur:

A machine always sends a transmission to the default router first. If the default router is not the best choice for the transmission, it sends an ICMP redirect message back to the host on the same network segment, and forwards the datagram to the

appropriate router. The redirect message basically says "it would be best to send datagrams to a router with IP address A.B.C.D for network W.X.Y.Z". Host machine updates its routing table so it doesn't make the mistake again.

A machine can create ICMP redirect messages and send them to any other machine in the network. The routing table could be unusable (DoS attack). A machine could send an ICMP redirect with it's own IP address, and pose as a router, therefore filtering ALL traffic. Simplest way to avoid ICMP spoofing is disable ICMP redirect messages, in both the hosts and the routers.

Q6. Suppose a 456723 bits message is given/input to the SHA-512 algorithm. For this message find the following **[2]**

a. Number of padding bits to be appended
b. Number of blocks in which the message will be broken

Answer: **a)** **877**

b) **447**
