Assignment 2

Name: Shweta Sharad Mestry
B-Number: B00815342
Email: ~~smestry1@gmail~~. smestry1@binghamton.edu

1. A. Traffic analysis:
may not be able to extract the information, but might still be able to observe the pattern of these message.

2. a. 'Alice should use public key of Bob (PuB) to encrypt in order to protect confidentiality of M. In this case only Bob will be able to decrypt the message using his private key (PrB).

b. Alice should use private key (PrA) of her to create digital signature. This ensures that only Alice has prepared the message.

c. Alice should use private key (PrA) of her to encrypt M to provide integrity, because it is impossible to alter the message without knowing Alice's private key.

3. a. If ~~they~~ use symmetric cipher, there will be 6 symmetric key. Let's say there are 4 people A, B, C, D. So, there will AB, AC, AD, BD, BC, CD ⇒ 6 keys. In symmetric key, people shared key.
A − B ⇒ AB (symmetric key), A − C ⇒ AC (symmetric key) ......

b. If they use a public-key cipher, there will be total 8 keys.
In Public-key cipher, each person holds his private key and public key. The person will encryt the message with public key of other person whom he wants to submit message and the receipient person will decrypt message with his

private key. Hence there will be 8 keys.

4. Message : tomorrowfriday

Cipher : Rail fence cipher.

Depth : 4.

Write message letters out diagonally over a number of row (4)

```
t   r    r   f   a
  o    r    r   y
    m    o    i
      o    w    d
```

Ciphertext : trfaorrymoiowd.

5. Ciphertext : rnoxitrzsunwinooagry.

Cipher : Row transposition cipher.

key : 35214

|cipher| = 20

|key| = 5

|row| = 4

Key:	3	5	2	1	4
Ciphertext:	i	s	r	a	i
	n	u	n	g	t
	o	n	o	r	r
	o	w	x	y	z

Plaintext : israinungtonorrowxyz

Plaintext after removing Extra added characters: israinungtonorrow

6. In given input, first one is ~~fo~~ present at 1st position and second one is present at 2nd position. We will look for 1 and 2 in P-table. When we pass the given input to the given P table, We found 1 is at 9th position and 2 is at 17th position.

Hence, The output will contain; 1st one will be at ~~gt~~ 9th position and 2nd one will be at 17th position; others will be 0.

7. Output of S-box : 2 ($\because$ 0010)

~~The input~~

The substitution consists of a set of 8 S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

- The first and last bits of the input to S_i form a 2-bit binary number to select one of 4 substitutions defined by the four rows (0, 1, 2, 3) in the table for S_i.

- The middle 4 bits select one of 16 columns (0-15).

Hence 4 possible input to s-box.

001000 {$\because$ 2 is present at 0th row, 4th col.}
001011 {2 is present at 1th row, 5th col.}
101100 {2 is present at 2nd row, 6th col.}
100111 {2 is present at 3rd row, 3rd col.}

8.

$$\phi(55) = \phi(5 * 11)$$

$$= \phi(5) * \phi(11)$$

$$= (5-1) * (11-1) \quad \left\{ \begin{array}{l} \text{if } p \text{ is prime,} \\ \phi(p) = p-1 \end{array} \right\}$$

$$= 4 * 10$$

$$= 40$$

9.

1.

M = 0110 1001 1101 0101

Block size = 4

$$\begin{array}{ll} & 1\ 2\ 3\ 4 \\ B1 = & 0\ 1\ 1\ 0 \\ B2 = & 1\ 0\ 0\ 1 \\ B3 = & 1\ 1\ 0\ 1 \\ B4 = & 0\ 1\ 0\ 1 \end{array}$$

~~Give H(M') =~~

The 1st bit of hash code is formd using ~~EOR~~ XOR ~~all~~ 1st bit of all blocks.

$h1 = 0 \oplus 1 \oplus 1 \oplus 0 = 0$

The 2nd bit of hash code is formed using XOR ~~all~~ 2nd bit of all blocks

$h2 = 1 \oplus 0 \oplus 1 \oplus 1 = 1$

The 3rd bit of hash code is formed using XOR 3rd bit of all blocks.

$h3 = 1 \oplus 0 \oplus 0 \oplus 0 = 1$

The 4^{th} bit of hash code is formed using XOR 4 th bit of all blocks.

$h4 = 0 \oplus 1 \oplus 1 \oplus 1 = 1$

$\therefore$ $H(M) = 0111$

2.

To prove simple hash function is not secure, we need to prepare the desired alternate message and then append an n-bit block that forces the new message plus block to yield the desired hash code.

Let's consider:

$M' = 0000 \quad 0000 \quad 0000 \quad 0000 \quad 0111$

$$\begin{array}{r}
0000 \\
\oplus\ 0000 \\
\hline
0000 \\
\oplus\ 0000 \\
\hline
0000 \\
\oplus\ 0000 \\
\hline
0000 \\
\oplus\ 0111 \\
\hline
H(M') \rightarrow 0111
\end{array}$$

$\therefore$ $H(M) = H(M')$

This has proved, simple hash function is not secure.