Assignment 2

skolhap1@binghamton.edu
B00815336

Q1

→ Traffic Analysis.

Q2.

→ (a) Alice should encrypt the message using Bobs public key (P_{UB}), so, that only Bob can decrypt the message using this private key. - (P_{UB})

(b) To ~~protect the~~ provide digital signature Alice should use her private key (P_{rA}) which is known only to her and unique to her. (P_{rA})

(c) If Alice wants to protect data Integrity of the Message she should use (P_{rA}) - private keys of hirself because the private keys of Alice is only known to her and cannot be altered. -(P_{rA})

Q3.

(a) if we use symmetric cipher we will need in total 6 keys
A, B, C, D are 4 person than AB, AC, AD, BC, BD, CD
or $(4 * (4-1))/2 = 12/2 = 6$ keys

(b) if we use public key cipher we will need in total 8 keys

using public key we will encrypt the messag and using private key we will decrypt the message

Sidd

Q4.

→

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

ciphertext: trfaorrymoiowd

Q5

→ |cipher| = 20

|key| = 5

20/5 = 4

4 character per column

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

plain text :- israiinungtonorrowxyz

plain text removing extra character added during Encryption.

P. :- israihungtonorrow

Q6.

→ according this Input provided there are two 1's at first and second position.

1 1 0 1 0 0

So we will look for 1 and 2 in the permutation table.

1 is at 9th position

2 is at 17th position

9th and 17th bit of the output of the P table are 1

1 1 0 0

Q7

1 1 1 0 0 1

The first and last bits of the input to Si form a 2 bit binary number to select one of 4 substitution defined by the four row 0, 1, 2, 3 in the table for Si

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

∴ for 1st input as 2 is present in 1st row so 00 and column is 0100

1st input ⇒ :- 0 0 1 0 0 0

2nd 2 present in second row 01
and column is 0110

2nd :- 001011

3rd 2 present in third row 10
and column is 0110

3rd :- 101100

4th 2 present in fourth row 11
and column is 0011

4th :- 100111

Q.8 $\phi(55) = \phi(5 \times 11)$
$= \phi(5) \times \phi(11)$

But $\phi(p) = p-1$ is valid for prime number.

$(5-1) \times (11-1)$
4×10
$= 40.$

000100

~~There are 40~~

Q9.

(1) Take 1st bits of all the blocks having size 4.

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

2nd bits of all the block.

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

3rd bit of all th block.

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

4th bit of all the block.

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

$\therefore H(M) = 0111$

(2) if we consider .

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

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

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

$\therefore$ Simple hash function H is not secure