Intro to Computer security

Assignment-2

Page No.
Date

Name: Rahul Verma
email: rverma4@binghamton.edu
B-number: B00892091

Ans1) Passive Attacks:

A) Traffic Analysis

Traffic Analysis may not be able to extract the information (encryption), but might still be able to observe the pattern of these messages
- Observe the frequency and length of messages being exchanged.

eg: Timing attack on the SSH Protocol used Timing information to deduce information about passwords.

Ans2)

a) If Alice wants to protect confidentiality of message (M), Alice should encrypt it with Bob's public key (Pu_B). Therefore, only Bob, using his private key (Pr_B) will be able to decrypt the message in this situation.

b) If Alice wants to provide digital signature, Alice should use her own private key. (Pr_A). Therefore, it guarantees that the message (M) was written by Alice alone.

c) If Alice wants to protect data integrity of the message (M), Alice should encrypt the message with her private key (Pr_A), as it can't be modified with out Alice's private key.

Page No.
Date

Ans 3)

a) In Symmetric cipher / Symmetric key cryptography we use one key which is shared by both sender and receiver. Here, we suppose there are 4 people, let the 4 people be A, B, C and D. As one key is shared between sender and receiver, we will make groups of 2 people where 1 key is used per group. AB, AC, AD, BC, BD, CD. Therefore, we can say that they would need 6 keys in total.

b) In Public-Key cipher / Asymmetric cryptography we make use of two keys: A public key which is used to encrypt messages and a private key which is used to decrypt messages. As each of the 4 people will require ~~2 keys~~, one public and one private key, that is in total 4 public and 4 private keys and total 8 keys.

Page No.
Date

Ans 4) Message: "tomorrow friday"
Depth: 4

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

→ Ciphertext: trfaorrymoiowd

Ans 5) Message: "rnoxitrzsunwinooagry"
Key: 35214

|ciphen| = 20, |key| = 5 → |row| = 4

Key:	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

→ Plaintext: is rainung tonorrowxyz

→ Plain text: is rainung tonorrow

Page No.
Date

Ans6) Given: Input of P Table is 1100000 ... 0

Here the first and the second bit is 1 and the rest is 0.
Here, we need to find which output bit is the first and the second bit of the Input. We will look for 1 and 2 in the Table, 1 is at the 9th bit position and 2 is at the 17th bit position.

→ Therefore, the 9th and 17th bit of the output is 1 and others are 0.

Ans7) Given: Output of the S-box is 2

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 Si form a 2-bit binary number to select one of 4 substitutions defined by the four rows (0,1,2,3) in table for Si
- The middle 4 bits select one of the 16 columns (0-15)

→ Therefore four possible inputs to S-box are:

001000 (2 at 0th row & 4th column)
001011 (2 at 1st row & 5th column)
101100 (2 at 2nd row & 6th column)
100111 (2 at 3rd row & 3rd column)

Page No.
Date

Ans 8)

Given:

Encryption : $C_i = E(\text{Counter} + i-1) \oplus P_i$

Decryption : $P_i = E(\text{Counter} + i-1) \oplus C_i$

To prove: $E(\text{Counter} + i-1) \oplus C_i$ is equal to P_i

Proof: We know that,

$A \oplus A = 0$

$0 \oplus A = A$

$P_i = E(\text{Counter} + i-1) \oplus C_i$

$P_i = E(\text{Counter} + i-1) \oplus E(\text{Counter} + i-1) \oplus P_i$

$\{C_i = E(\text{Counter} + i-1) \oplus P_i\}$

$P_i = 0 \oplus P_i \quad \{A \oplus A = 0\}$

$P_i = P_i \quad \{0 \oplus A = A\}$

→ Hence Proved, $E(\text{Counter} + i-1) \oplus C_i$ is equal to P_i
Therefore, the decryption process of counter mode is correct.

Page No.
Date

Ans 9) Compute: $\phi(55)$

Two prime numbers p and q with $p \neq q$, then

$$\phi(pq) = \phi(p) \times \phi(q) = (p-1) \times (q-1)$$

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

$$= (5-1) \times (11-1)$$

$$= (4) \times (10) = 40$$

$$\therefore \phi(55) = 40$$