PSG College of Technology
Department of Applied Mathematics and Computational Sciences
MSc Theoretical Computer Science(2017-18)
15XT68 -Security in Computing Lab
Problem Sheet No 3

1.Cyclic attack in RSA

Perform a cyclic attack on a Cipher text C to find the plain text P. Consider a short message and a low value of n.

2.Broadcast Attack using CRT

An RSA public-key is a pair (n, e) where n = p ,q is the product of two primes.

$RSA_{n,e}(m) = m^e \bmod n$

Alice, Bob, and Carol use RSA public-keys (n_A, 3), (n_B, 3), and (n_C, 3), respectively. David wants to send the same message 'm' to three of them. So, David computes

$y_A = m^3 \bmod n_A$

$y_B = m^3 \bmod n_B$

$y_C = m^3 \bmod n_C$

and sends the cipher text Y to the respective users. Show how an eavesdropper Eve can now compute the message 'm' even without knowing any of the private keys of Alice, Bob, and Carol.

3. Chosen Cipher text attack

This is an attack against the textbook version of the RSA algorithm. In this attack, an attacker first chooses a message and encrypts it the victim's public key. Then, the attacker asks the victim to sign (decrypt) for him a specially crafted related message. Due to the following property of RSA

$$E_{PU}(M_1) \times E_{PU}(M_2) = E_{PU}(M_1 \times M_2) \text{ ----------,(1)}$$

the attacker can easily recover any message encrypted with the victim's private key,without ever learning this private key. For example, the attacker wants to decrypt the following ciphertext $C = M^e \bmod N$,without knowing the private key d. The attacker proceeds as follows. Knowing the victim's public key **e**, he prepares the following message

$$X = (C \times 2^e) \bmod N ,$$

gives it to the victim and asks her to sign it. The victim signs message X with its private key and sends the result Y back to the attacker.

$$Y = X^d \bmod N$$

$$\begin{aligned} X^d &= \left((C \bmod N) \times (2^e \bmod N)\right)^d \\ &= \left((M^e \bmod N) \times (2^e \bmod N)\right)^d \\ &= \left((2 \times M)^e \bmod N\right)^d \\ &= (2 \times M)^{ed} \bmod N \\ &= 2 \times M . \end{aligned}$$

Using Y and equation (1), the attacker can retrieve the encrypted message M as follows:

1. Show by example that equation (1) holds for the RSA encryption algorithm.
2. Demonstrate by example the chosen ciphertext attack against RSA.