Lab Report 6

ESE – 3014

EMBEDDED SYSTEMS COMMUNICATION PROTOCOLS AND SECURITY

Submitted to :

Linchan Wang

Submitted by:

Gurvinder Singh(748418)

**1. Review our slide about the process of asymmetric cryptography (like RSA which have public key and private key), try to find an idea to crack it andget text message between A and B.**

Solution:- In Asymmetric cryptography, we use use two keys namely private key and private key and it is also known as Public cryptography. These keys are used for encryption and decryption of data. Public key is public in nature and can be used by anyone, however private key is secret key and used by the only person have the authority to use it. These two keys have different functions from each other. For encryption, we use public key and for decryption, private key is used. As discussed in class, Professor Linchan will use the public key to encrypt the message and Gurvinder Singh will use the private key to decrypt the message.

**How to hack the communication between Professor Linchan and Gurvinder Singh:**

So Now Professor Linchan and Gurvinder Singh want to send a message to each other and they donot want that Ronak or any other person read this message. Now Gurvinder creats two keys namely private key and public key. As name of private key depicts, it is not used by anyone. However public key is open for the public. Now Professor linchan use public key of Gurvinder to encode the message for Gurvinder Singh. Now message will pass through Ronak. Ronak is not able to decrypt the message with public key because for that task private key is required. Only Gurvinder Singh can decrypt the message by using the private key.

Now Ronak wants to decrypt Professor Linchan’s message. Now ronak have Public key and ciphertext of message. For that purpose, finding prime factors for value of public key and using the decryption software.

Consider two prime numbers say x and y for encrypting a message with the help of RSA.

Where x = 307 and y = 377.

So, p = 307\*377

p = 115739

As we know that primary condition for efficient cracking is that small numbers should be taken into

consideration.

We have chosen the Carmichael’s totient function for this procedure.

b(n) = LCM (x-1 , y-1), where b(n) represents Carmichael’s totient function for n and LCM represents

lowest commo0n multiple.

B(115,739) = LCM(307-1, 377-1)

= LCM(306, 376)

By calculation b(115739) = 115056

For Generating public keys, public keys are made of two prime number g and n, where value of g varies

from 1 and b(n), which in our case is 115056. consider small value of g which is 11. final encrypted data

called ciphertext (c) is calculated by

c = m^g mod n

To keep things simple consider the single number 4

= 4 ^ 11 mod 115739

c comes out to be 27700

This is the encrypted result, which can be securely send to the owner of key pair.