**ESE-3014 EMBEDDED SYSTEMS COMMUNICATION PROTOCOLS AND SECURITY**

**LAB 2 Report**

**GROUP No. 2**

|  |  |
| --- | --- |
| **Group Members** | **Student ID** |
| Christy Rachel Philip | C0765535 |
| Fahad Rahman | C0769871 |
| James M Chacko | C0777192 |
| Premil Presannan | C0777191 |
| Vy Nguyen | C0776242 |

**Introduction:**

In this report, we will discuss the process of asymmetric cryptography (like RSA

which have a public key and private key), try to find an idea to crack it and get the text message between A and B.

**Discussion:**

**1. Simulate encryption communication, encrypt a message using an RSA public key, and try to decrypt it with an RSA private key.**

*Answer:*

We have:

Public key: (n &e)

Private key: (n&d)

To send the message m from A to B, we encrypt it by:

me mod n = c (c is the encrypted message)

To decrypt the message, we use

cd mod n = m

By using octave, we develop these functions:

First, we make a function that runs the power of modulo:

**Powermod function**

|  |
| --- |
| **function result = powermods(base, exponent, n)    base = mod(base, n);    result = 1;    for k = 1: exponent  result = result \* base;  result = mod(result, n);    endfor** |

**Encrypting function:**

|  |
| --- |
| function encryptedmessage = encrypt (m, e, n)  %(n, e) is the B's public key % m is the message within the range of {0;n) % m^e mod n = encryptedmessage(c)  encryptedmessage = powermods(m, e, n);  endfunction |

**Decrypting function**

|  |
| --- |
| **function decryptedmessage = decrypted (c, d, n)  %(n,d) is B's private key % c is the encrypted message decryptedmessage = powermods(c, d, n); % = m - the message endfunction** |

Now to simulate the encryption communication process we:

* Choose 2 distinct primes p & q
* Compute n= p.q
* Compute φ = (p-1)(q-1)
* Choose e such that 1<e< φ
* Find d where ed ≡ 1 (mod φ)

We have the function that generatimh e, n, and d

|  |
| --- |
| function [e, n, d] = KeyGenerator()  %choosing 2 random distinct primes  y = primes(500);  y = y(y>=2);  p = y(randperm(numel(y),1));  q = y(randperm(numel(y),1));     n = p\*q; %compute n   phi = (p-1)\*(q-1); %compute phi    for e = 2:phi-1  if gcd(phi, e) == 1; % check d.e mod phi = 1  break; %break when given the smallest valid e  endif  endfor    for d = 1:phi-1  if mod(e\*d,phi) == 1;%checking if exd mod phi =1  break  endif  endfor  endfunction |

Now we create a script that can simulate the process:

|  |
| --- |
| clc, clear  [e, n, d] = KeyGenerator(); %running KeyGenerator function to get e, n and d value  m = input('Enter your secret message ');  encryptmessage = encrypt(m, e, n); %encrypting the message  disp('Encrypted Message is: ') disp(encryptmessage)  pause(1) %for special effect  disp('Decrypting...')  pause(2) decryoedmessage = decrypted(encryptmessage, d, n); %decrypting the message disp('Secret message is ') disp(decryoedmessage) |

**Result:**

|  |
| --- |
| Enter your secret message 55 Encrypted Message is: 3043 Decrypting... Secret message is 55 >> |

2. Try to crack a private key with a known public key. And determine the key component to keep the security of RSA encryption communication. Hint: the key is to find out d, we can get a private key once we have d. Is it possible to derive d in the case of n and e?

1. ed (mod φ(n)) = 1

2. φ(n) = (p-1)(q-1)

3. n=pq

*Answer:*

A brutal force attack is one of the ways of cracking an asymmetric cryptographic message. It is defined as trying out several combinations of the password to guess the key’s combination to decrypt the sent or received message. This method can also be termed the password -guessing method. In this method, the prime numbers p and q are identified by guessing or by using supercomputers. If the prime numbers p and q of the RSA are identified, then we can identify n, which is "p\*q=n." from that private key can be discovered, and we can crack the RSA

The Equations for Encryption and Decryption are:

**P=prime number**

**q=prime number**

**n=p\*q**

**phi(n)=(p-1)(q-1)**

**e=exponent, and its value must be between 1 and phi(n)**

**d=private value(keep it secret)**

**d=inverse of e\*(mod(phi(n)))**

**for encryption**

**Secret message^e\*(mod(n)) ,which is the cypher text or encrypted message**

**for Decryption**

**cypher text^d\*(mod(n)), which is the secret message**

**Conclusion:**

In this report, we discussed the process of asymmetric cryptography (like RSA, which has a public key and private key). Then we found an idea named brutal force attack to crack it and get the text message between A and B.