MARK MUNENE

SCT 212-0224-2017

CRYTOGRAPHY ASSIGNMENT

1. Write a program that implements the Euclidean algorithm

Using c programming language

/\* GCD of two numbers using Euclid's algorithm\*/

#include <stdio.h>

void main()

{

    int m, n; /\* given numbers \*/

    clrscr();

    printf("Enter-two integer numbers: ");

    scanf ("%d %d", &m, &n);

    while (n > 0)

    {

        int r = m % n;

        m = n;

        n = r;

    }

    printf ("GCD = %d \n",m);

    getch();

}

1. Find the GCD of 117 and 299 using the eucllidean algorithm

299,117

299=117.2 + 65

117=65.1 +52

65=52.1 + 13

52= 13.4 + 0

Hence the gcd is 13 since it is the last non zero remainder

1. Find the intergers p and q ,solution 1002p + 71q=m

1002=71.14 + 8 14.71+ 8= 1.1002 -14.71

71=8.8 + 7 8.8 + 7=

8= 7.1 + 1 1.7 + 1=

7=1.7 + 0

8.Determine intergers x and y such that gcd (421,11)=421x + 11y

Gcd (421,11)

421=11.38 + 3 38.11 + 3 =1.421 -11.38

11 = 3.3 + 2 3.3 + 2 = 1.11 -3.3

3 = 2.1 + 1 1.2 + 1= 1.3 -2.1

2= 1.2 + 0

X and y will be 3 and 2

9.Explain the working mechanism of the following signature schemes

* RSA signature scheme

-RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and the Private key is kept private.

An example of asymmetric cryptography :

A client (for example browser) sends its public key to the server and requests for some data.

The server encrypts the data using the client’s public key and sends the encrypted data.

Client receives this data and decrypts it.

Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of browser.

* Digital signature scheme

-Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

* Schnorr signature scheme

-a Schnorr signature is a digital signature produced by the Schnorr signature algorithm that was described by Claus Schnorr. It is a digital signature scheme known for its simplicity, is efficient and generates short signatures. It is one of the protocols used to implement “Proof Of Knowledge”.In cryptography, a proof of knowledge is an interactive proof in which the prover succeeds in ‘convincing’ a verifier that the prover knows something ‘X’. For a machine to know ‘X’ is defined in terms of computation. A machine knows ‘X’ if this ‘X’ can be computed. The Verifier either accepts or rejects the proof. The signature proof is supposed to convince the Verifier that they are communicating with a user who knows the private key corresponding to the public key. In other words, the Verifier should be convinced that they are communicating with the Prover without knowing the private key.