NAME- RAM CHANDRA JANGIR
ROLL NO. - CS21M517
Subject - CS6530 Assignment-6 (DSA)

Digital Signature Algorithm

(i) Introduction
(ii) Basic Requirements
(iii) How DSA works
(iv) My DSA program output

(i) Introduction:-

A digital signature - a type of electronic signature - is a mathematical algorithm routinely used to validate the authenticity and integrity of a message (e.g. an email).

(ii) Basic requirements:

(a) Private Key

The private key is one which is accessible only to the signer. It is used to generate the digital signature which is then attached to the message.

(b) Public Key -

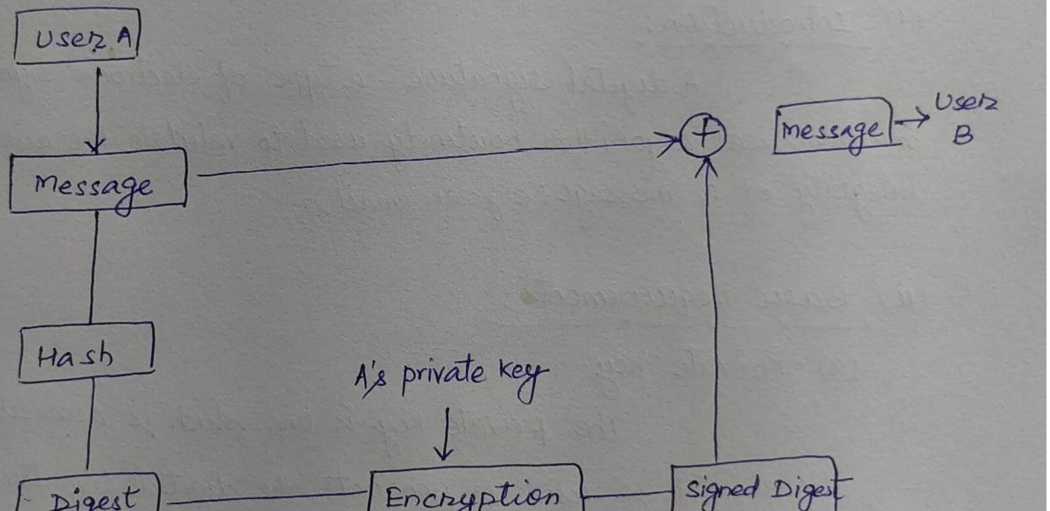
The public key is made available to all those who receive the signed messages from the sender. It is used for verification of the received message.

(c) Digital signature certificate -

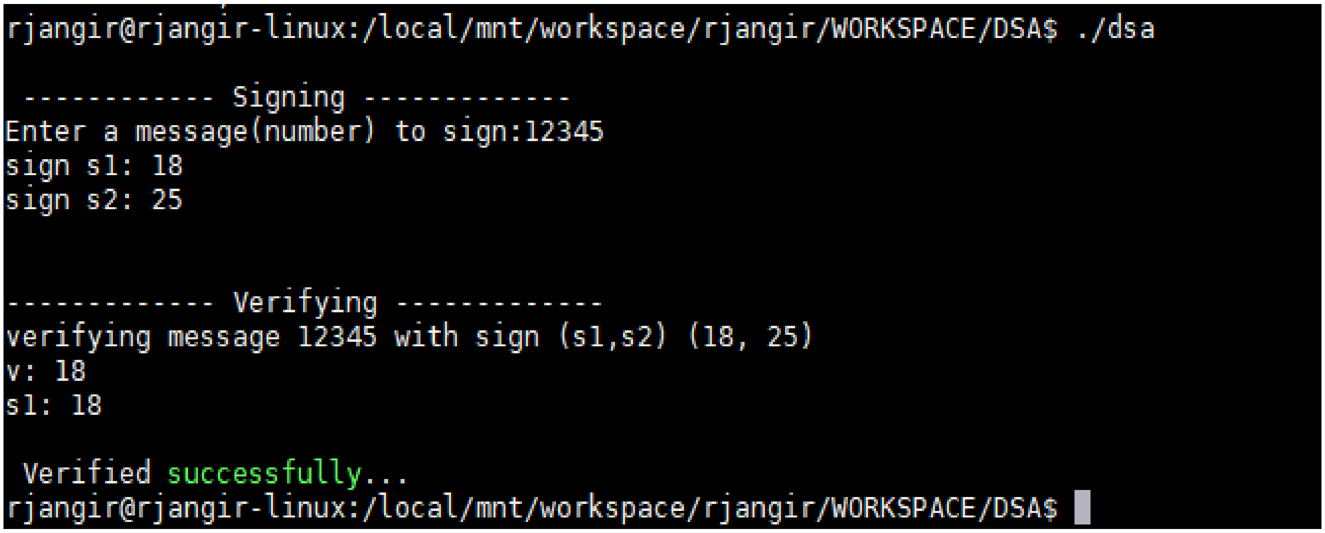
A subscriber of the private key and public key pair makes the public key available to all those who are intended to receive the signed messages from the subscriber.

But in case of any dispute between the two sides, there must be some entity with the receiver which will allow the receiver of the message to prove that the message was sent by the subscriber of the key pair. This can be done with the Digital signature certificate.

(iii) How DSA works-



(iv) My DSA program output:



```
rjangir@rjangir-linux:/local/mnt/workspace/rjangir/WORKSPACE/DSA$ ./dsa

 ------------ Signing -------------
Enter a message(number) to sign:12345
sign s1: 18
sign s2: 25


------------- Verifying -------------
verifying message 12345 with sign (s1,s2) (18, 25)
v: 18
s1: 18

 Verified successfully...
rjangir@rjangir-linux:/local/mnt/workspace/rjangir/WORKSPACE/DSA$
```