3) N=33

E=13

Plain text(M) = 6

1. According to RSA encryption algorithm, we know that,

**C=ME (mod N)**

So, on substituting the respective values, we get,

C = 613 (mod 33)

C = 13060694016 (mod 33)

**C = 18**

1. Now we have to find Alice’s private key **D.**

We know that,

ED = 1 mod(S(N))

S(N) = (P-1) (Q-1) = (11-1) (3-1) = 20

13 \* D = 1 mod(20)

**D = 17**

1. Alice’s public/private key pair is weak because the number **N is 33, which is very small and can be easily factorize to prime numbers P and Q**. Also, (N,E) is public here. So, if the number is small, Private Key D can be easily determined by the attacker using ED = 1 mod(S(N)), where S(N) = (P-1) (Q-1).

In order to make RSA encryption algorithm more secure, it is recommended to **choose larger value of prime numbers P and Q** so that value of N becomes even much larger and the factorization will become more complex. Thus, it will almost become impossible for an attacker to know the private key (D) of the Alice.

2) No, the validation method is not secure.

**Reason**: The attacker who can modify or change the file and its data in the middle can also change hash value associated with it. So, both the file received by the bob and hash value might be corrupted and he might won’t able to know that the file and hash which he has received is sent by the attacker or the Alice.

**More Secure method:** More secure method is to encrypt a message and the hash of the message with the key, i.e. Ek(m, h(m)) and the key has been exchanged. This encryption of hash of the message with the Alice’s private key is called signing the document digitally. Now if the attacker gives a different message, we can immediately know that the message is not right. In this way, transmission of file between Bob and Alice can be carried out successfully.

1. As, both Alice and Bob knows the public key of each other, MITM attack is not possible. But, if MITM wants to attack this protocol, he has to do that initially, i.e. before the execution of the first step.

The attack might be possible in the following way:

* When Alice sends IDa and Na to Bob, MITM grabs this and send his nonce instead of Alice’s nonce and pretending to be Alice. So Bob will receive (Ida and Nm), where Nm is the nonce of MITM.
* On receiving Ida, Bob thinks that this is arrived from Alice, so he will send his signature to Alice which includes his nonce, IDa and plain text.

**Sb = Encskb (Nb, Nm, IDa, Plaintext)**

* Now, again MITM will intercept this and sends (Nm, IDa, IDb, Plaintext) to Alice pretending to be Bob.
* On receiving, IDa and IDb, Alice thinks that the message has been arrived from Bob and he will sends his signature along with the reply for that plain text and a nonce Na’.

**Sa = Encska(Nm, Na, IDb, Plaintext).**

Thus, in this way we can MITM will attack this mutual authentication Protocol and verify his identity pretending to be other user to both the Alice and the Bob.