RSA ENCRYPTION TECHNIQUE

RSA (Rivest-Shamir-Adleman) is an asymmetric cryptographic algorithm used to encrypt and decrypt messages by modern computers. Asymmetric states that there are two different keys used in the encryption and decryption process, which also is called public-key cryptography. This is simply because one of the two keys can be given to anyone without exploiting the security of the algorithm. The RSA algorithm involves both private and public keys. The public key can be known and published to anyone, as it is used to encrypt the messages from plaintext to ciphertext. The messages that are encrypted with this specific public key can however only be decrypted with the corresponding private key. The key generation process of the RSA algorithm is what makes it so secure and reliable today, as it contains a high level of complexity compared to other cryptographic algorithms.
Also note that we generally use RSA algorithm for passwords or to encrypt the key generated by AES encryption technique. AES encrypts the file data and generates a key which is encrypted by RSA algorithm and sent to other person securely.

KEY GENERATION

Unlike symmetric algorithms like AES , RSA requires computation of pair (K_{public} , $K_{private}$).
It consist of following steps -
1) Chose two large prime numbers let’s say p and q.
2) Compute n=p.q
3) Calculate a variable say t=(p-1)*(q-1).
4) Compute the encryption key let’s say e such that
   a) 1<e<t
   b) e and t are co-prime or gcd(e,t)=1.
5) Compute the decryption key let’s say d such that (de)mod t = 1.

We have made two keys encryption key and decryption key.The public key consists of n and e, while the private key consists of d,n.

$$K_{public} = \{e,n\} \qquad K_{private} = \{d,n\}$$

Also it is safer to use large prime numbers p and q since it increases the level of complexity and makes the cryptanalysis process considerable harder in terms of bruceforce attacks.

ENCRYPTION AND DECRYPTION

The formula for encryption states that :

c = pow(m,e) mod n .

Here c is the cypher text or encrypted text , m is the message text and e is public key.

The formula for decryption states that :

m = pow(c,d) mod n .

Here c is the cypher text or encrypted text , m is the message text and d is private key.

Anyone who wants to encrypt a message needs to use the public key of the receipent, in order to ensure that the message is only decryptable by the correct individual so that it only decrypts with a specific private key. The receipent shares the public key, while keeping the private key secret.

PADDING

1) The padding scheme used in the encryption process is quite important. The padding scheme ensures that no values of the message are insecure, such as for example the values m = 0 or m = 1 will respectively compute ciphertexts equal to 0 or 1, which is caused by the properties of the exponentiation. When the exponent used in the key generation process is small, this might cause the non-modular result of me to be less than the modulus n. This means that ciphertexts may be bruteforced and decrypted easily by calculating the e-th root of the ciphertext without necessarily regarding the modulus.

2) For example when encrypting a text with the numeric value of 0, it would encode as m = 0, which then again computes the ciphertext c = 0, with no concern about the values of n and e. The same goes for the numeric value of 1, which produces the value of 1 in ciphertext. This creates an insecure pattern, which might be analyzed by attackers and easily decrypted after gaining some knowledge about the encryption process. To avoid such problems in the algorithm, it is common to implement a randomized padding into the message before the encryption happens. This is to ensure that the message does not contain some insecure values and that the encrypted ciphertext contains some padded values that generate a larger ciphertext. This increases the level of complexity of the encryption, and will most likely make a dictionary attack harder to succeed.

Once the message arrives on the recipient’s side of the communication channel, the ciphertext gets decrypted using the private key in the following procedure: m ≡ c d (mod n), where c is the ciphertext.