IMAGE ENCRYPTION/DECRYPTION USING RSA AND AES ALGORITHM

Introduction:

One of the major issue with transfer the data over the Internet is the security and authenticity. The security is basically protecting the data from an unauthorized users or attackers. Encryption is one of the technique which is use for secure the information. Image encryption is a technique that convert original image to another format with the encryption techniques. The same way in the decryption no one can access the information without knowing a decryption
key. Image security is an utmost concern in the web attacks are become more serious. The Image encryption and decryption has applications in internet communication, military communication, medical imaging, multimedia systems, telemedicine, etc. To make the data secure from various attacks the data must be encrypted before it is transmit. The government, financial institution, military,hospitals are deals with confidential images about their patient, financial status, geographical areas, enemy positions.Most of this information is now collected and stored on
electronic computers and transmitted over the network.

II. PURPOSE OF CRYPTOGRAPHY

Cryptography provides security to ensure the privacy of data, non-alteration of data and so on. Nowadays cryptography is widely using due to the great security. There are the various cryptography goals are following as,

A. Confidentiality

The transmission of data from one computer to another computer has to be accessed by an authorized user
and it not access by anyone else.

B. Authentication

The transmission of data from one computer to another computer has to be accessed by an authorized user and it not access by anyone else.

C. Integrity

Only the authorized party is allow to modify the transmitted information. And an unauthorized persons should not allow to modify in between the sender and receiver.

D. Non Repudiation

Ensures the message that sender or the receiver should be able to deny the transmission.

E. Access Control

The authorized persons only able to access the information while in transfer.

III. TYPES OF CRYPTOGRAPHY

Cryptography technique is secure the secret message when it is transfer from one place to another place over the
networks. The cryptography contains the two main categories which are following as,

1) Symmetric key cryptography
2) Asymmetric key cryptography

A. Symmetric key cryptography

Secret key cryptography is also known as symmetric key cryptography. In this type both the sender and the receiver know the same secret key. The sender is encrypt the data or the

information using the secret key and the receiver is decrypt the information using the same secret key. In the symmetric cryptography the key is playing a very important role which is depends on the nature of key.

B. Asymmetric key cryptography

Asymmetric cryptography is used encryption and decryption algorithm pair. With public key cryptography, keys work in pairs of matched public and private keys. Public key cryptography, also called asymmetric key cryptography which is using a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. The cryptography technique is using the secret message transfer from one place to another place over the networks. The cryptography technique is require some algorithms for encrypt the data.

RSA ALGORITHM:

RSA is an algorithm which is use provide the encryption and authentication system. This is developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. This algorithm is most commonly used encryption and authentication algorithm. The RSA algorithm is one of the first public key cryptosystems, and it is widely used for secure the data transmission. In such a cryptosystem, the encryption key is a public one and the decryption key is differ which is keep secret. In RSA, this asymmetry is based on the product of two large prime numbers, the factoring problem. The RSA encrypt key is encrypt the image, so that it convert into cipher text format and it will be store as a text file. The opposite method of encryption, the reverse process is compute by another one decryption key of RSA algorithm and it decrypts the image from the cipher text. Finally it will discover the resultant image by the decryption techniques.

The Fig.1 is describe the step by step manner of processing in the encryption and decryption.

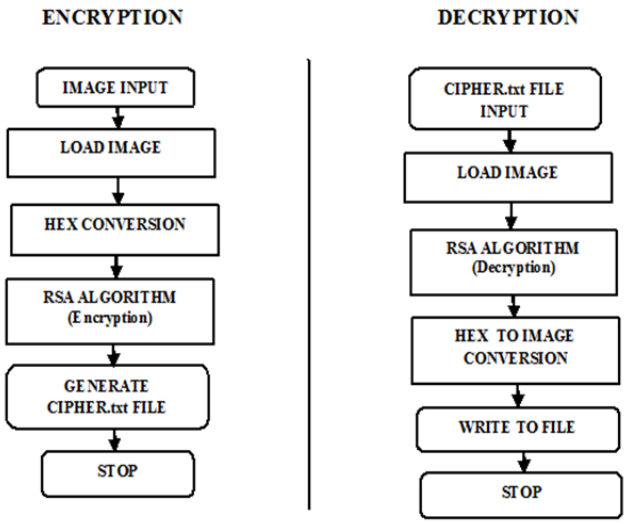
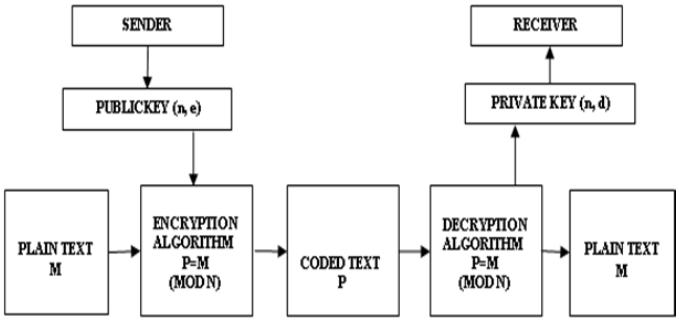


IMAGE CRYPTOGRAPHY METHODOLOGY BY RSA

The RSA is an cryptographic algorithm which is use to encrypt and decrypt the data. This algorithm developed in

1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA cryptosystem is also known as the public-key cryptosystems. RSA is normally used for secure data transmission. The encryption is starting on the RSA algorithm with the selection of two large prime numbers, along with an auxiliary value, as the public key. The prime numbers are keep in secret. The public key is used to encrypt a message, and private key is used to decrypt a message or information.The RSA algorithm is encrypt the original image and decrypts the image by the different keys. That is shown in
Fig.2.



The RSA algorithm is also called as an asymmetric cryptographic algorithm. Asymmetric cryptosystem means two different keys are using in the encryption and decryption. In the two keys one key is using for encryption and the second key is using for decryption. This RSA algorithm is also called as the public key cryptography. Because one of the secret key can be given to everyone which means public. The other key must be kept private. The RSA algorithm consists of three manor steps in encryption and decryption. The steps are following as,

1) Key Generation
2) Encryption
3) Decryption

A. Key generation
The key generation is the first step of RSA algorithm. The RSA involves a public key and a private key. On those keys the public key can be know everyone and it is use for encrypting messages. Messages encrypted with the public key can decrypt using the private key. The keys for the RSA algorithm is generated by the following steps,

1) First choose the two distinct prime numbers p and q.
2) For security purposes, the integer p and q should be chosen, and it should be the similar bit-length. Prime integers can be efficiently found by a primality testing.
3) Then compute the n value, n = pq.

4) n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

5) Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient function. This value is kept private.

6) Choose an integer e such that $1 < e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co-prime.e is the released as the public key.e has a short bit-length and small Hamming weight results in more efficient encryption.However, much smaller values of e have been shown to be less secure in some settings.

7) Determine d as $d \equiv e-1 \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo φ(n)). This is stated as, solve the d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$. This is computed using extended Euclidean algorithm. It using the pseudo code in the Modular integers section, inputs a and n correspond to e and φ(n), respectively.
8) d value is keep as the private key.The public key consists of the modulus n and the public key e. The private key have the modulus n and the private key d, and it keep in secret. p, q, and φ(n) values are keep in secret, because they can be used to calculate d.

B. Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key d secret. Bob then it is wish to send the
message M to Alice. So, first turns M into an integer m, such that $0 \leq m < n$ and gcd(m, n) = 1. Then it compute the cipher text c. This can done efficiently, even the numbers are 500-bit numbers, it is using the Modular exponentiation. Bob then transmits c to Alice. At least nine values of m will yield acipher text c equal to m.

C. Decryption

Alice can recover m from c by using her private key exponent d via computing. Given m, she can recover the original message M by reversing the padding scheme.

AES ALGORITHM SPECIFICATION

AES algorithm is of three types i.e. AES-128, AES-192 and AES-256. This classification is done on the bases of the key used in the algorithm for encryption and decryption process. The numbers represent the size of key in bits. This key size determines the security level as the size of key increases the level of security increases. The AES algorithm uses a round function that is composed of four different byte-oriented transformations. For encryption purpose four rounds consist of: • Substitute byte • Shift row • Mix columns • Add round key While the decryption process is the reverse process of the encryption which consists of: • Inverse shift row • Inverse substitute byte • Add round key • Inverse mix columns

There is a number of round present of key and block in the algorithm. The number of rounds depends on the length of key use for Encryption and Decryption.

AES algorithm uses a round function for both its Cipher and Inverse Cipher. This function is composed of four different byte-oriented transformations.

1. Encryption process

1.1Substitute byte transformation The Substitute bytes transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table S-box. The operation of substi-tute byte is shown in figure 1.

1.2 Shift rows transformation

In the Shift Rows transformation, the bytes in the last three rows of the State are cyclically shifted over different numbers of bytes. The first row, r = 0, is not shifted.This has the effect of moving bytes to “lower” positions in the row while the “lowest” bytes wrap around into the “top” of the row.

1.3 Mix columns transformation

The Mix Columns transformation operates on the State column-by-column, treating each column as a four-term poly-nomial. The columns are considered as polynomials over GF(2^8) and multiplied modulo x 4 + 1 with a fixed poly-nomial a(x), given by a(x) = {03}x ^3 + {01}x^ 2 + {01}x + {02} .
The resultant columns are shown in the figure below. This is the operation of mix columns.

1.4 Add round key transformation

In the Add Round Key transformation, a Round Key is added to the State by a simple bitwise XOR operation. The Round Key is derived from the Cipher key by means of key schedule process. The State andRound Key are of the same size and to obtain the next State an XOR operation is done per element:

$b(i, j) = a(i, j) \oplus k(i, j)$

2. Decryption process

2.1. Inverse shift row transformation

Inverse Shift Rows is the inverse of the Shift Rows trans-formation. The bytes in the last three rows of the State are cyc-lically shifted over different numbers of bytes. The first row, r = 0, is not shifted. The bottom three rows are cyclically shifted by Nb-shift(r, Nb) bytes, where the shift value shift(r,Nb) depends on the row number.

2.2 Inverse substitute byte transformation

Inverse Substitute Bytes is the inverse of the byte substitu-tion transformation, in which the inverse S-box is applied to each byte of the State. It is reverse process of Substitute byte transform. This is obtained by applying the inverse of the af-fine transformation followed by taking the multiplicative in-verse in GF (2^8). There is an inverse s-box table for substitute the value.

2.3 Inverse mix columns transformation

Inverse Mix Columns is the inverse of the Mix Columns trans-formation. Inverse Mix Columns operates on the State col-umn-by-column, treating each column as a four-term poly-nomial. The columns are considered as polynomials over GF(2^8) and multiplied modulo x^ 4 + 1 with a fixed poly-nomial (x), given by

a-1(x) = {0b}x^3 + {0d}x^ 2 + {09}x + {0e}

3 IMPLEMENTATION

A. ENCRYPTION ALGORITHM

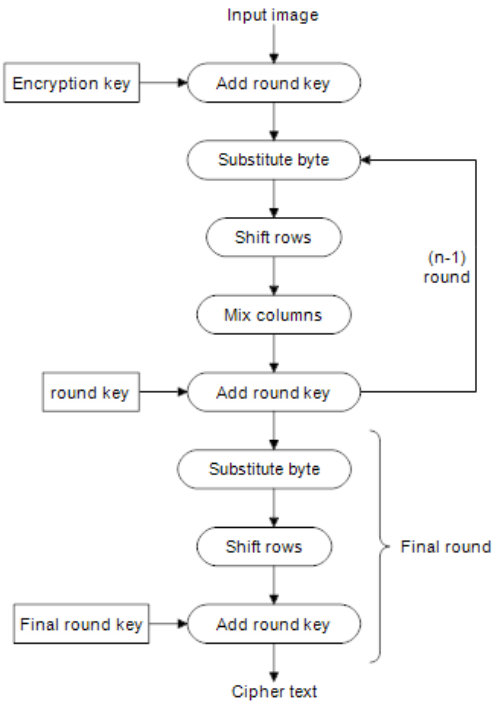
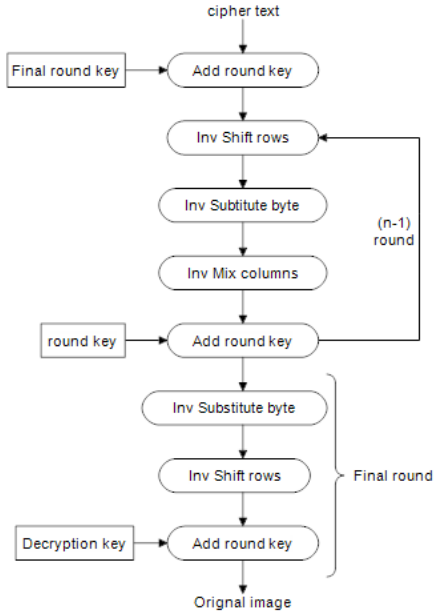


Fig. Flowchart of AES Encryption algorithm

The implementation of the AES-128 encryption and de-cryption algorithm with the help of Python in Jupyter Lab. In which the input is an image and the key in hexade-cimal format and the output is the same as that of input image. For encryption process first, dividing image and making it 4*4 byte state i.e. matrix format. Calculate the number of rounds based on the key Size and expand the key using our key sche-dule. And there are (n-1) rounds performed which are substi-tute byte, shift rows, mix columns and add round key. The final round "n" does not consist of mix column in the iteration. Figure shows the flow of algorithm.

B. DECRYPTION ALGORITHM

The AES decryption process is the revers process that of the encryption process. The above figure shows flow of the AES decryption algorithm. Which consist of cipher text as the input, the key is same for decryption process which for encryption. In case of decryption the inverse substitute byte, inverse shift rows and the inverse mix columns are to be im-plemented. While the add round key remains the same.



Flowchart of AES decryption algorithm

The original input image given to the algorithmis of JPG
And of 8.32 Kb size. The unreadable image is the encrypted image and by applying the decryption algorithm the original image is obtained in JPG format. In this paper, For Encryption and the decryption the same key is used. The key is in hexade-cimal form and length of key is 128 bits. Key used= 0123456789abcdef. Input= Image in JPG format.

CONCLUSION

The cryptography mechanism is using the RSA algorithm with the public key encryption is to increase the security levels of the encrypted. Here one key is needed to encrypt and another key is needed to decrypts the image. Finally the image cryptography experiment is provide the feasibility of security to the image in network security. The data is not view by no one without the knowledge of cryptography.
Image Encryption and Decryption using AES algorithm is implemented to secure the image data from an unauthorized access. A Successful implementation of symmetric key AES algorithm is one of the best encryption and decryption standard available in market. With the help of python coding implementation of an AES algorithm is synthesized and simulated for Image Encryption and Decryption. The original images can also be completely reconstructed without any distortion. It has shown that the algorithms have extremely large security key space and can withstand most common attacks such as the brute force attack, cipher attacks and plaintext attacks.