CHAPTER 2

LITERATURE REVIEW AND RELATED WORKS

2.1 Introduction:

Cryptography is the science of using mathematics to encrypt and decrypt data.

or it is the ability to send information between participants, in a mangled format, that prevents others from reading it[3] .

it enables you to store sensitive information or transmit it across insecure networks (like the internet) so that it cannot be read by anyone except the intended recipient.

2.1.1 How does cryptography work?

Acryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process.

acryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext.

The same plaintext encrypts to different cipher text with different keys. the security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

Acryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem.

2.2 Classical encryption techniques:

The techniques are the basic approaches to conventional encryption today. the two basic components of classical ciphers are substitution and transposition. then other systems described that combines both substitution and transposition.

2.2.1 Caesar Cipher:

Caesar Cipher is substitution method which is said to have been used by Julius Caesar to communicate with his army. Caesar is considered to be one of the first persons to have ever employed encryption for the sake of securing messages. Caesar decided that shifting each letter in the message would be his standard algorithm, and so he informed all of his generals of his decision, and was then able to send them secured messages. using the Caesar Shift (3 to the right).

Caesar Cipher replaces each letter of the message by a fixed letter a fixed distance away e.g. uses the third letter on and repeatedly used by Julius Caesar [4](Guru 2007) . Can describe the Cipher as:

Encryption: C=E (P)=(P+3) mod 26.

Decryption: P=D(C) =(C-3) mod26.

For example the message is :

Plaintext: COMPUTER FIELD

Ciphertext: FRPSXWHUILHOG

the Caesar cipher is a *shift cipher* since the ciphertext alphabet is derived from the plaintext alphabet by shifting each letter a certain number of spaces.

2.2.2 Playfair Cipher:

the Playfair is a substitution cipher invented by Charles Wheatstone in around 1854.

the Playfair Cipher was developed for telegraph secrecy and it was the first literal digraph substitution cipher. this method is quite easy to understand and learn but not easy to break, because you would need to know the "keyword" to decipher the code. the system functions on how letters are positioned in a 5*5 alphabet matrix.

a"KEYWORD" sets the pattern of letters with the other letters the cells of the matrix in alphabetical order (I and j are usually combined in one cell).

2.2.3 Poly-alphabetic Cipher:

A poly-alphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. Mono-alphabetic Cipher can be broken. the reason is same plain letters are encoded to same cipher letters; the underlying letter frequencies remain unchanged.

Cryptographers have tried to overcome this dilemma simply by assigning various cipher letters or symbols to same plain letters. Such ciphers are called Poly-alphabetic Ciphers.

the most popular of such ciphers is the "Vigenère Cipher".

2.2.3.1 Vigenère algorithm:

The Vigenère cipher, proposed by Blaise de Vigenère from the court of Henry III of France in the sixteenth century, the Vigenère cipher is an improvement of the Caesar Cipher key is multiple letters long K=k1, K2, k3….kd [4].

the Vigenère cipher uses this table together with a keyword to encipher a message.

For example, suppose we wish to encipher the plaintext message:

Computer field

Using the keyword Cryptography. we begin by writing the keyword, repeated as many times as necessary, above the plaintext message. to derive the ciphertext using the tableau, for each letter in the plaintext, one finds the intersection of the row given by the corresponding keyword letter and the column given by the plaintext letter itself to pick out the ciphertext letter.

Keyword: CRYPT OGRAP HYC

Plaintext: COMPU TERFI ELD

Ciphertext: EFKEN HKIFX LJF

Decipherment of an encrypted message is equally straightforward. One writes the keyword repeatedly above the message:

Keyword: CRYPT OGRAP HYC

Ciphertext: EFKEN HKIFX LJF

Plaintext: COMPU TERFI ELC

This time one uses the keyword letter to pick a row of the table and then traces across the row to get the column containing the ciphertext letter. the index of that column is the plaintext letter.

2.3Cryptographic systems Classification:

Cryptographic systems are generally classified along three independent dimensions:

1. Type of operations used for transforming plaintext to cipher text.

all encryption algorithms are based on two general principles those are:

a- substitution, in which each element in the plain text is mapped into another element.

b- transposition in which elements in the plaintext are rearranged.

the fundamental requirement is that no information be lost. most systems referred to as product systems, involved multiple stages of substitution and transposition.

2. The number of keys used:

a- Symmetric if the sender and receiver use the same key, the system is referred to as single key or secret key conventional encryption.

b- Asymmetric if the sender and receiver each uses a different key the system is referred to as asymmetric, two key, or public-key encryption.

3. The way in which the plaintext is processed:

a- A block cipher processes the input on block of elements at a time, producing an output block for each input block.

b- A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Conventional Encryption is referred to as symmetric encryption or single key encryption.

It was the only type of encryption in use prior to the development of public-key encryption. conventional encryption can further be divided into the categories of classical and modern techniques.

the hallmark of the classical technique is that the cipher or the key to the algorithm is shared i.e. known by the parties involved in the secured communication[4].

So there are two types of cryptography: secret key and public key cryptography .in secret key same key is used for both encryption and decryption and in public key cryptography each user has a public key and a private key.

2.3.1 Symmetric Cryptography:

In a cryptosystem that uses symmetric cryptography, both parties will be using the same key for encryption and decryption [5].

Symmetric keys are also called secret keys because this type of encryption relies on each user to keep the key a secret and properly protected. if this key got into an intruder's hand, that intruder would have the ability to decrypt any intercepted message encrypted with this key.

each pair of users who want to exchange data using symmetric key encryption must have their own set of keys.

the security of the symmetric encryption method is completely dependent on how well users protect the key. this should raise red flags to you if you have ever had to depend on a whole staff of people to keep a secret. if a key is compromised, then all messages encrypted with that key can be decrypted and read by an intruder. this is complicated further by how symmetric keys are actually shared and updated when necessary.

If Dan wants to communicate to Norm for the first time, Dan has to figure out how to get Norm the right key. it is not safe to just send it in an e-mail message because

the key is not protected and it can be easily intercepted and used by attackers. Dan has to get the key to Norm through an out-of-band method. Dan can save the key on a floppy disk and walk over to Norm's desk, send it to him via snail mail, or have a secure carrier deliver it to Norm.

this is a huge hassle, and each method is very clumsy and insecure.

Because both users use the same key to encrypt and decrypt messages, symmetric cryptosystems can provide confidentiality, but they cannot provide authentication or non-repudiation. there is no way to prove who actually sent a message if two people are using the exact same key.

The symmetric cryptosystems have so many problems and flaws, but we use them they are very fast and can be hard to break. Compared to asymmetric systems, symmetric algorithms scream in speed. they can encrypt and decrypt large amounts of data that would take an unacceptable amount of time if an asymmetric algorithm was used instead. It is also very difficult to uncover data that is encrypted with a symmetric algorithm if a large key size was used.

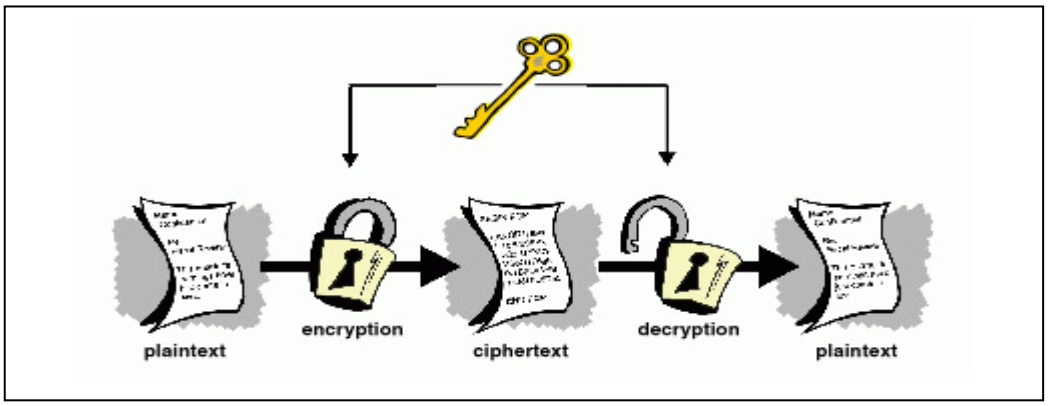

Figure 2.1 show Symmetric cryptography system.

The following list outlines the strengths and weakness of symmetric key systems:

2.3.1.1Symmetric Strengths

• Much faster than asymmetric systems.

• Hard to break if using a large key size.

2.3.1.2Symmetric Weaknesses

• Key distribution it requires a secure mechanism to deliver keys properly.

• Scalability each pair of users' needs a unique pair of keys, so the number of keys grow exponentially.

• Limited security it can provide confidentiality, but not authenticity or non-repudiation.

2.3.2 Asymmetric Cryptography:

In symmetric key cryptography, a single secret key is used between entities, whereas in public key systems, each entity has different keys, or asymmetric keys. the two different asymmetric keys are mathematically related. if a message is encrypted by one key, the other key is required to decrypt the message.

In a public key system, the pair of keys is made up of one public key and one private key [5].

the public key can be known to everyone, and the private key must only be known by owner.

Many times, public keys are listed in directories and databases of e-mail addresses so they are available to anyone who wants to use these keys to encrypt or decrypt data when communicating with a particular person.

The public and private keys are mathematically related, but cannot be derived from each other. this means that if an gets a copy of Bob's public key, it does not mean he can now use some mathematical magic and find out Bob's private key.

If Bob encrypts a message with his private key, the receiver must have a copy of Bob's public key to decrypt it. the receiver can decrypt Bob's message and decide to reply evildoer back to Bob in an encrypted form .all she needs to do is encrypt her reply with Bob's public key, and then Bob can decrypt the message with his private key. it is not possible to encrypt and decrypt using the exact same key when using an asymmetric key encryption technology.

Bob can encrypt a message with his private key and the receiver can then decrypt it with Bob's public key. By decrypting the message with Bob's public key, the receiver can be sure that the message really came from Bob. A message can only be decrypted with a public key if the message was encrypted with the corresponding private key.

this provides authentication, because Bob is the only one who is supposed to have his private key. When the receiver wants to make sure Bob is the only one that can read her reply, she will encrypt the response with his public key. only Bob will be able to decrypt the message because he is the only one who has the necessary private key.

Now the receiver can also encrypt her response with her private key instead of using Bob's public key. Why would she do that? she wants Bob to know that the message came from her and no one else. If she encrypted the response with Bob's public key, it does not provide authenticity because anyone can get a hold of Bob's public key. If she uses her private key to encrypt the message, then Bob can be sure that the message came from her and no one else. Symmetric keys do not provide authenticity because the same key is used on both ends. using one of the secret keys does not ensure that the message originated from a specific entity.

if confidentiality is the most important security service to a sender, she would encrypt the file with the receiver's public key. this is called a secure message format because it can only be decrypted by the person who has the corresponding private key.

If authentication is the most important security service to the sender, then she would encrypt the message with her private key. this provides assurance to the receiver that the only person who could have encrypted the message is the individual who has possession of that private key. if the sender encrypted the

message with the receiver's public key, authentication is not provided because this public key is available to anyone.

Encrypting a message with the sender's private key is called an open message format because anyone with a copy of the corresponding public key can decrypt the message; thus, confidentiality is not ensured.

For a message to be in a secure and signed format, the sender would encrypt the message with her private key and then encrypt it again with the receiver's public key. the receiver would then need to decrypt the message with his own private key and then decrypt it again with the sender's public key.

this provides confidentiality and authentication for that delivered message.

each key type can be used to encrypt and decrypt, so do not get confused and think the public key is only for encryption and the private key is only for decryption.

An asymmetric cryptosystem works much slower than symmetric systems, but can provide confidentiality, authentication, and non repudiation depending on its configuration and use.

Asymmetric systems also provide for easier and more manageable key

distribution than symmetric systems and do not have the scalability issues of symmetric systems.

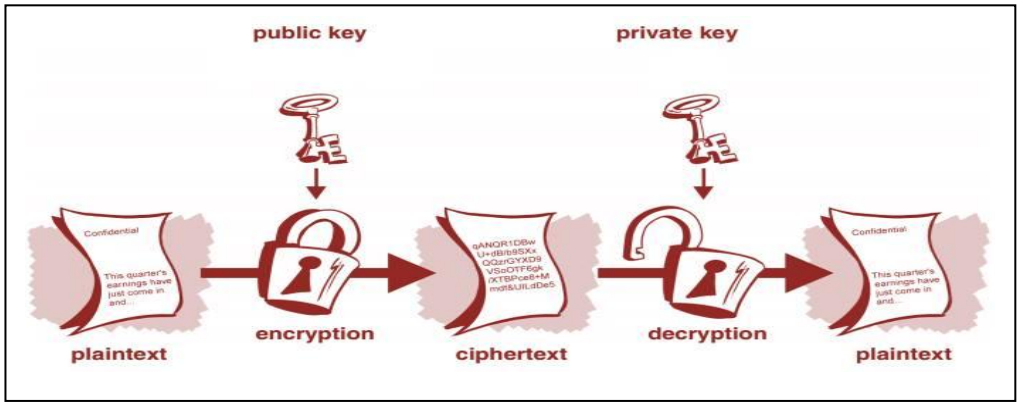

Figure2.2 show Asymmetric cryptography system

The following outlines the strengths and weaknesses of asymmetric key systems:

2.3.2.1 Asymmetric Strengths:

• Better key distribution than symmetric systems.

• Better scalability than symmetric systems.

• Can provide confidentiality, authentication, and non repudiation.

2.3.2.2Asymmetric Weaknesses:

• Works much slower than symmetric systems.

2.3.3Block cipher:

Symmetric-key block ciphers are the most prominent and important elements in many cryptographic systems. individually, they provide confidentiality. as a fundamental building block, their versatility allows construction of pseudorandom number generators, stream ciphers, MACs, and hash functions.

they may furthermore serve as a central component in message authentication techniques, data integrity mechanisms, entity authentication protocols, and (symmetric-key) digital signature schemes.

no block cipher is ideally suited for all applications, even one offering a high level of security. this is a result of inevitable tradeoffs required in practical applications, including those arising from, for example, speed requirements and memory limitations (e.g., code size, data size, cache memory), constraints imposed by implementation platforms (e.g., hardware, software, chip cards), and differing tolerances of applications to properties of various modes of operation. in addition, efficiency must typically be traded off against security. thus it is beneficial to have a number of candidate ciphers from which to draw . of the many block ciphers currently available. while not guaranteed to be more secure than other published candidate ciphers (indeed, this status changes as new attacks become known), emphasis is given to those of greatest practical interest. among these, DES is

paramount; FEAL has received both serious commercial backing and a large amount of independent cryptographic analysis; and IDEA (originally proposed as a DES replacement) is widely known and highly regarded. other recently proposed ciphers of both high promise and high profile (in part due to the reputation of their designers) are SAFER and RC5.

2.3.3.1Data Encryption Standard (DES):

DES is a symmetric, block-cipher algorithm with a key length of 64 bits, and the algorithm operates on successive 64 bit blocks of plain text. due to symmetric, the same key is used for encryption and decryption, and also uses the same algorithm for encryption and decryption.

initially a transposition is carried out according to a set table (the initial permutation), the 64-bit plaintext block is then split into two 32-bit block, and 16 identical operations called rounds are carried out on each half.

the two halves are joined back together, and the reverse of the initial permutation is carried out. the purpose of the first transposition is clear; it does not affect the security of the algorithm, but is through for the purpose of allowing plaintext and cipher text to be loaded into 8-bit chip in byte-sized pieces.

in any round, only one half of the original 64-bit block is operated on. the rounds alternate between the two halves.

2.3.3.2 Advanced Encryption Standard (AES):

AES is symmetric key encryption standard adopted by the U.S government .the standard comprise three block cipher AES 128 , AES 192, AES 256 adopted from long collection originally published as Rijndael .the Rijndael proposal for AES defined a cipher in which the block length and the key length can be independently specified to be 128, 192, 256 bits. a number of AES parameters depend on the key length.

The AES ciphers have been analyzed extensively and are now used worldwide , as was the case with its the procedure, the data encryption standard.

Rijndael was designed to resistance against all known attacks, speed , code compactness on a wide range of platforms and design simplicity.

2.3.3.3 RC2:

RC2 is a block cipher that was designed in 1989 by Ron Rivest for RSA data Security, initially held as a confidential and proprietary algorithm, RC2 was published as an Internet Draft during 1997 [6] .

RC2 has many interesting and unique design features, particularly so when one considers the style of ciphers that dominated both the literature and the market at the time of its invention. the cipher was intended to be particularly efficient on 16-bit processors and with a 64-bit block size it was intended as a drop-in replacement for DES.

a significant feature of RC2 is the flexibility offered to the user in terms of the effective key-size.

this has now become a common feature of many block cipher proposals and it is a property that has proven to be important in commercial applications. over the years RC2 has been deployed widely and it features prominently in the S/MIME secure messaging standard.

2.3.4 Stream cipher:

Stream ciphers are an important class of encryption algorithms. They encrypt individual characters (usually binary digits) of a plaintext message one at a time, using an encryption transformation which varies with time. Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry. They are also more appropriate, and in some cases mandatory (e.g., in some telecommunications applications), when buffering is limited or when

characters must be individually processed as they are received. Because they have limited or no error propagation, stream ciphers may also be advantageous in situations where transmission errors are highly probable.

There is a vast body of theoretical knowledge on stream ciphers, and various design principles for stream ciphers have been proposed and extensively analyzed. However, there are relatively few fully-specified stream cipher algorithms in the open literature. This unfortunate

state of affairs can partially be explained by the fact that most stream ciphers used in practice tend to be proprietary and confidential. By contrast, numerous concrete block cipher proposals have been published, some of which have been standardized or placed in the public domain. nevertheless, because of their significant advantages, stream ciphers are widely used today, and one can expect increasingly more concrete proposals in the coming years. stream ciphers can be either symmetric-key or public-key.

2.4 Shift register:

Shift registers are at the heart of cryptography and error-correction.

in cryptography they are the main tool for generating long pseudorandom binary sequences which can be used as keys for two communicating parties in symmetric cryptography.

2.4.1 A5 – Encryption:

To protect privacy all over-the-air transmissions on a GSM network are encrypted with a stream cipher known as A5 [7].

Four different variants of the algorithm exist: A5/0 is a no-operation cipher which does not encrypt data. A5/1 is the standard version and was specified in the mid 1980's after a dispute between several NATO countries about the strength of the algorithm: Germany wanted it to be strong because of its long borders to Eastern

Europe, but was later overruled by the other countries and a relatively simple design for A5/1 was specified. A5/2 is a weakened version which was chosen to deal with export restrictions on strong ciphers. A5/3 was later added for 3G networks (UMTS -successor to GSM) and is a totally new algorithm based on the clock cipher KASUMI by Mitsuru Matsui who designed KASUMI (also named MISTY) to be resistant against differential and linear cryptanalysis.

though the A5 algorithm is described in the specifications of GSM it has never been made public officially. Companies implementing GSM networks have to buy the GSM specifications from ETSI, most likely accompanied by strong non-disclosure agreement contracts. Through leaking of documents a first draft of the algorithm was made public by Ross Anderson in 1994 and fully discovered through reverse engineering of a mobile phone's firmware by Brienco citebgwa5 in 1998/1999, and even later confirmed by the GSM group to be correct.

A5 is a stream cipher4, it operates on 228-bit blocks called "frames" sent and received over the air every 4.6 milliseconds. 114 bits represent data sent from the MSE and the other 114 bits are data received by the MSE, both mainly containing digitized audio signals (after error correction). taking the session key Kc produced by A8 and a frame counter5 Fn, A5 generates 228 pseudo random bits (PRAND) which are XOR'ed with the plaintext frame resulting in 228 bits of ciphertext.

The most important part in A5 is generating the pseudo random bits (function GEN). in A5/0, as a no-op cipher, the PRAND is generated by negating the input frame. or in other words, the XOR function is left out, using the input frame as output.

2.4.2 A5/1:

A5/1 implements PRAND generation by 3 linear feedback shift registers6 (LFSRs) denoted as R1, R2 and R3. In this case an LFSR feedback function is an XOR of all its input bits7, meaning that when the register is clocked, its input bits are XOR'ed and the result is stored in the rightmost bit [7].

2.5 RC4 Encryption Algorithm:

RC4 is an encryption algorithm that was created in 1987 by Ronald Rivest of RSA Security. it is used in WEP and WPA, which are encryption protocols commonly used on wireless routers. the workings of RC4 used to be a secret, but its code was leaked onto the internet in 1994. RC4 was originally very widely used due to its simplicity and speed. typically 16 byte keys are used for strong encryption, but shorter key lengths are also widely used due to export restrictions.

over time this code was shown to produce biased outputs towards certain sequences, mostly in first few bytes of the key stream generated. This led to a future version of the RC4 code that is more widely used today, called RC4-drop[n], in which the first n bytes of the key stream are dropped in order to get rid of this biased output. Some notable uses of RC4 are implemented in Microsoft Excel, Adobe's Acrobat 2.0 (1994), and Bit Torrent clients.to begin the process of RC4 encryption, you need a key, which is often user-defined and between 40-bits and 256-bits.

2.5.1 RC4 Features:

• RC4 uses a variable length key from 1 to 256 bytes to initialize a 256-byte state table. the state table is used for subsequent generation of pseudo-random bytes and then to generate a pseudo-random stream which is XORed with the plaintext to give the ciphertext. each element in the state table is swapped at least once.

• the RC4 key is often limited to 40 bits, because of export restrictions but it is sometimes used as a 128 bit key. It has the capability of using keys between 1 and 2048 bits. RC4 is used in many commercial software packages such as Lotus Notes and Oracle Secure SQL.

• the RC4 algorithm works in two phases, key setup and ciphering. Key setup is the first and most difficult phase of this algorithm. During a N-bit key setup (N being your key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing operations. these mixing operations consist of swapping bytes, modulo operations, and other formulas. A modulo operation is the process of yielding a remainder from division. for example, 11/4 is 2 remainder 3.

• once the encrypting variable is produced from the key setup, it enters the ciphering phase, where it is XORed with the plain text message to create an encrypted message. XOR is the logical operation of comparing two binary bits. if the bits are different, the result is 1. If the bits are the same, the result is 0.

once the receiver gets the encrypted message, he decrypts it by XORing the encrypted message with the same encrypting variable.

2.5.2 RC4 Strengths:

• the difficulty of knowing where any value is in the table.

• the difficulty of knowing which location in the table is used to select each value in the sequence.

• a particular RC4 key can be used only once.

• encryption is about 10 times faster than DES.

2.5.3 RC4 Weakness:

• the RC4 algorithm is vulnerable to analytic attacks of the state table.

• one in every 256 keys can be a weak key. These keys are identified by cryptanalysis that is able to find circumstances under which one of more generated bytes are strongly correlated with a few bytes of the key.

• WEAK KEYS: these are keys identified by cryptanalysis that is able to find circumstances under which one or more generated bytes are strongly correlated with small subset of the key bytes. These keys can happen in one out of 256 keys generated [8] .

2.6 Cryptanalysis:

Is the science of analyzing and breaking secure communication. classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.

Cryptology embraces both cryptography and cryptanalysis.

Cryptographic strength is measured in the time and resources it would require to recover the plaintext. the result of strong cryptography is cipher text that is very difficult to decipher without possession of the appropriate decoding tool. How difficult?

given all of today's computing power and available time—even a billion computers doing a billion checks a second—it is not possible to decipher the result of strong cryptography before the end of the universe.

one would think, then, that strong cryptography would hold up rather well against even an extremely determined cryptanalyst. Who's really to say? no one has proven that the strongest encryption obtainable today will hold up under tomorrow's computing power. However, the strong cryptography employed by PGP is the best available today. vigilance and conservatism will protect you better, however, than claims of impenetrability.

2.7 Related Studies:

Numerous researchers attempt to enhance the RC4 and create variant algorithms.

2.7.1- Maytham M. Hammood, et al [8]. they proposed RC4 stream cipher with two state tables (RC4-2S) as an enhancement to RC4. RC4-2S stream cipher system solves the correlation problem between the public known outputs of the internal state using permutation between

state 1 (S1) and state 2 (S2). Furthermore, key generation time of the RC4-2S is faster than that of the original RC4 due to less number of operations per a key generation required by the former. The experimental results confirm that the output streams generated by the RC4-2S are more random than that generated by RC4 While requiring less time than RC4. Moreover, RC4-2S's high resistivity protects against many attacks vulnerable to RC4 and solves several weaknesses of RC4 such as distinguishing attack [8].

2.7.2-The proposed algorithm by Jian Xie et al. [9].is an extension of the improved RC4 Stream Cipher .It uses three secret keys- two secret keys K1 and K2 as seeds for Enhanced RC4 and K3 as the key for Vigenère cipher substitution. It also uses two S-Boxes S1 and S2. Both of them contain N elements from 0 to N-1. The Key Scheduling Algorithm is the same as original RC4 except that it uses two S-boxes instead of one, as proposed in the Enhanced RC4 Algorithm.

In PRGA two output streams are obtained from S1 and S2. The output streams are XORed with each other. The resulting stream is then XORed with the plaintext P, to obtain the intermediary cipher text, X. this intermediary cipher text is then fed as the input of Vigenère cipher. In this final phase of the encryption process, substitution on the intermediary cipher text X takes place using the key K3. This gives us the final cipher text C. The encryption process is stated below-

in the algorithm proposed, Vigenère Cipher is used in the final phase of the encryption process to perform substitution. Vigenère Cipher is a polyalphabetic stream cipher. Each character of the intermediary cipher text X is encrypted using K3 as the key. This final phase of encrypting using Vigenère Cipher can be summarized as follows-

Encryption: $Ca = (Xa + ka) \bmod 256$ where C = C0…..Cn is the Cipher text, X = X0…..Xn is the Intermediary Cipher text and K3 = k0…..km is the key used.

decryption process is similar to encryption obeying the laws of symmetric cryptography algorithms. the cipher text C is first decrypted using Vigenère Cipher with K3 as the key. the output of this process is the intermediary plaintext Y. in the next phase, keys K1 and K2 are used as the seed for the Pseudorandom Stream Generator using improved RC4. two output streams are obtained as the output of the stream generation phase. the output streams are XORed with each other. the resulting stream is then XORed with the intermediary plaintext Y to give the final plaintext P.

2.7.3-The algorithm developed by Deep Desai1, et al[10] .provides a method for purpose of encrypting and decrypting the image of any size and shape. It allows the user to select an image of his choice from a specified location on the computer, external hard drive or any other hardware devices connected to the computer. The system is able to support all standard image formats (e.g.:-TIFF, JPEG, BMP…..).The image selected by the user could be a Square image or a rectangular image of any dimension. The user is able to apply encryption to images captured via the camera and Personal pictures.

The image selected should be a color image where the pixels are represented in the RGB model. Each pixel should be represented using minimum 24 pixels. Once the

keys have been entered by the user in any form, a standard chaotic map is generated. The chaotic map generated using Mathematical equations and theory is completely reversible, efficient enough to produce diffusion on the entire image pixels and the computation time is less. The chaotic map produced is

then used for diffusing the image pixels. The image obtained from this chaos is completely distorted and the output is not Recognizable by the end user.

2.7.4-Yu and Zhang et.al [11] presented RC4 state combined with the hash function without affecting the simplicity and efficiency. The RC4 state based on hash function can generate Message Authentication Code (MAC). The enhancement includes the offset, forward, and backward properties of RC4 states where the authors use offset to ignore the first few bytes of the key and started encrypt the data in determine position which has led to increase the time of execution.

2.7.5- Ni G. A. P. Harry et.al .[12] Saptarini proposed a new method for Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map The structure consists of three main units: converter unit, CLM function unit, and RC4 stream cipher unit. The converter unit will convert key to initial value. The output of converter unit is an initial value which will be used by CLM function unit to generate 256-bytes of array or also known as key array. The last step is RC4 stream cipher process where the content of array and array is swapped between each other then the result will be XORed with the byte streams of plain-image to produce cipher-image or XORed with the cipher-image to produce plain-image.