Chapter 1

Introduction
1.1 Introductory Discussions

“Cryptography” is a Greek word means hidden or secret writing.[1] It is a way of securing communication in the presence of third parties called adversaries.[2] It can also be expressed as a tool used to maintain data confidentially, integrity and authentication.[3] Section 1.2 discussed some classical encryption techniques, that of some other available techniques have been presented in section 1.3 of this chapter. A comprehensive survey of literature has been presented in section 1.4. Objectives of the study are given in section 1.5. Organization of the thesis is given in section 1.6. Metrics for evaluation of proposed algorithms have been given in section 1.7. Some salient features of the thesis are described in section 1.8.

1.1.1 Classical Cryptography

Around 1900BC from old kingdom of Egypt the earliest known use of cryptography was found in non-standard hieroglyphs carved into monuments.[4] For protection of information similar technique was used that was discovered later in form of clay tablets. For example, nearly 1500BC one clay tablets was found to encrypt a craftsman’s methods for pottery glaze, presumably commercially valuable. Around 500 to 600BC Hebrew scholars used simple mono-alphabetic substitution ciphers (such as the Atbash ciphers).[5][6] The ancient Greeks are said to have known the use of ciphers. On the other hand scytale transposition cipher used by Spartan military served in the same way. However it is difficult to identify whether the scytale was for inscription, authentication, or avoiding bad omens in speech.[7][8] Herodotus used to conceal secret messages beneath wax on wooden tablets or by making a tattoo containing the message on a slave’s hand which was covered by growing hair. Romans were even aware of the uses and advantages of cryptography.

1.1.2 Medieval Cryptography

Sometime around 800 AD, possibly Al-Kindi, an Iraqi Muslim Arab mathematician unanimously hailed as the “Father of Islamic or Arabic Philosophy”, invented the frequency analysis technique for breaking mono-alphabetic substitution ciphers.[4] Religious motivation of textual analysis of Quran led to this vital invention. It was the most fundamental
cryptanalytic methodology known until WWII. *Rishlah fi Istikhraj al-Mu’amma*, a book written by Al-Kindi contains description of first cryptanalysis techniques. Arabic phonetics and syntax gave the first description on frequency analysis.[9] Methods of encipherments, cryptanalysis of certain encipherments, and statistical analysis of letters and letter combination in Arabic was also describe.[10]

*Subh al-a ‘sha*, a 14-volume encyclopedia included cryptology written by Ahmad al-Qalqashandi, a medieval Egyptian writer and mathematician. This information was attributed to Ali ibn Muhammad Ibn al-Durayhim, an Arab cryptologist, who lived from 1312 to 1361. List of ciphers like substitution and transposition, both are included in this work and for the first time, a cipher with multiple substitutions for each plaintext letter. Also traced to Ibn al-Durayhim is an exposition on and worked example of cryptanalysis. The use of tables of letter frequencies and set of letters which cannot occur together in a word

Leon Battista Alberti, an Italian cryptographer, known as “father of Western cryptology” clearly explained the poly-alphabetic cipher around the year 1467.[11] The tabula recta, a critical component of the Vigenere cipher was invented by Johannes Trithemius, in his work *Poligraphia*. Again a practical poly alphabetic system the Vigenere cipher, was devised by French cryptographer Blaise de Vigenere.[11]

As a result of political competition and religious revolution cryptography gained its importance in Europe. For example, during and after the Renaissance in Europe citizens of the various Italian states-the Papal States and the Roman Catholic Church included-were responsible for rapid proliferation of cryptographic techniques, few of which reflect understanding of Alberti’s polyalphabetic advance. Even after Alberti, ‘Advanced ciphers’ weren’t as advanced as predicted by the user or the inventor. Cryptography, cryptanalysis, and secret agent betrayal were the important features of Babington plot. During the reign of Queen Elizabeth I the Babington plot led to the execution of Mary, Queen of Scots. Cryptography remained undeveloped of outside Europe after Muslim golden age at the hand of Mongols.
1.1.3 Cryptography from 1800 to World War II

Cryptography has a long and complex history but could not develop anything more than ad hoc approaches to either encryption or cryptanalysis (science of finding weakness in crypto systems) until 19th century. At this time basis of cryptography consisted of hard-won rules of thumb, for example Auguste Kerckhoffs’ cryptographic writings in the latter 19th century. Edgar Allan Poe solves ciphers in the 1840s by certain systematic methods.\cite{10} In particular he informed about his abilities in the Philadelphia paper *Alexander’s Weekly (Express) Messenger*, inviting submission of ciphers of which he stepped forward to solve almost all. His essay on methods of cryptography proved useful as an introduction for the novice British cryptanalysis who attempted to solve German codes and ciphers during World War I.

The plotting of the execution of Mata Hari and in the conniving which led to the travesty of Dreyfus’ conviction and imprisonment, both in the early 20th century throws light on the misuse of cryptography. Fortunately, the machinations by the cryptographer had led to Dreyfus’ problems.

In World War I the breaking of German naval codes by Admiralty’s Room 40 played an important role in several naval engagement during the war. The Zimmermann Telegram, a cable from the German Foreign Office was sent via Washington to its ambassador Heinrich von Eckardt in Mexico. It is a major part in bringing the United States into the war. This telegram was decrypted.

A tele-printer cipher containing previously-prepared key, kept on paper tape, is combined character by character with the plaintext message to produce the cipher text, was proposed by Gilbert Vernam in 1917 and with time electromechanical devices as cipher machines and the one time pad, the only unbreakable cipher came into use. Mathematical implications proliferated in the period prior to World War II in 1932.

1.1.4 Cryptography in World War II

Mechanical and electromechanical and cipher machines were in wide use by World War II although manual machines were used in places where such machines were not available. Cipher design and cryptanalysis made great success but all in secrecy.
Electromechanical rotor machine, Enigma was widely used by the Germans. Detailed structure of German Army Enigma was deduced by Mathematician Marian Rejewski at Poland’s Cipher Bureau in December 1932 by using mathematics. Rejewski and his mathematical Cipher Bureau colleagues kept themselves updated with the evolution of the German Army machine’s components and encipherment procedures along with this they continued reading Enigma.

Immediately after World War II broke out on 1st September 1939, key Cipher Bureau personnel were evacuated south-eastward. As Poland attacked Soviet Union on 17th September, they crossed Romania. Then they reached Paris, France and they continued breaking Enigma, as the British desperately wanted to break Enigma they collaborated with British cryptologists at Bletchley Park. The scale and technology of Enigma decryption was upgraded by the British cryptographers- including many chess masters and mathematics dons such as Gordon Welchman, Max Newman and Alan Turing (the conceptual founder of modern computing). The breaking of Naval Cipher No.3 (German code) was a great success in World War II. It enables them to track and sink Atlantic convoys.

Several Japanese Navy crypto systems were broken by US Navy cryptographers (with cooperation from British and Dutch cryptographers). JN-25 was one of them which led to the US victory in the Battle of Midway. Highest security Japanese Navy crypto system (an electromechanical ‘stepping switch’ machine called Purple by the Americans) was broken by a US Army group, the SIS, even before WWII began. The intelligence evolving from cryptanalysis, especially from the Purple machine is known as ‘Magic’. The British eventually settled on ‘Ultra’ for intelligence resulting from cryptanalysis, particularly that from message traffic protected by the various Enigmas. ‘Boniface’, an earlier British term for Ultra is an attempt to suggest, if betrayed, that it might have an individual agent as a source. Several mechanical attempts were deployed by the German military at a one-time pad. They were called Fish ciphers by Bletchley Park; Heath Robinson was designed and deployed by Max Newman and colleagues, and the Colossus, the world’s first programmable digital electronic computer, to help with the cryptanalysis. The use of one-time pad was started in 1919 by the German Foreign Office.
A locally developed electrical stepping switch system (called the purple by US) was used by the Japanese Office along with several similar machines for attaches in certain German embassies. ‘M-machine’ and ‘Red’ are some of them. Allies has broken one degree to another.

The British TypeX and the American SIGABA were some allied cipher machines used in WWII. These are type of electromechanical rotor designs like that of Enigma, albeit with major improvements. No one break them during the war. Lacida machine used by the Poles has less security than intended by the Polish Army cryptographers in UK and its use was discontinued. US troops used M-209 machines and M-94 family machines. ‘Poem ciphers’ (memorized poems were the encryption or decryption keys) initially used by British SOE replaced one-time pads later in the war.

According to David Kahn in *Kahn on Codes*, the VIC cipher (used at least until 1957 in connection with Rudolf Abel’s NY spy ring) is the most complicated hand cipher known which is used by the Soviets.

1.1.5 Modern Cryptography

Cryptography and cryptanalysis became more mathematical since World War II. Wide availability of computers and the Internet as a communication medium has been able to make cryptography a common use by anyone other than national governments or similarly large enterprises.

The period of modern cryptography actually starts with the work Claude Shannon (known as father of Mathematical Cryptography) during WWII on communication security. Communication Theory of Secrecy System was published by him in 1949 in the Bell System Technical Journal. Later, he wrote a book “*A Mathematical Theory of Communication*”. All these along with his works on information and communication theory established a solid theoretical basis for cryptography and cryptanalysis. After that cryptography almost disappeared into secret governments communications organizations like NSA, GCHQ etc. Almost no work was made public until mid1970s, when everything changed. The present
proposal focuses on the major part of modern field of cryptography though it can be divided into various types such as symmetric and public key cryptography.

Encryption method in which both receiver and sender share the same key (or, less commonly, in which their keys are different, but related in an easily computable manner) is referred to as symmetric-key cryptography. This particular kind of encryption was only publicly known until June 1976. \[12\]

Block ciphers or stream ciphers are the two ways in which symmetric ciphers are implemented. A block cipher enciphers input in blocks of plaintext whereas individual characters are the form of input by a stream cipher.

Block cipher designs like the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) have been designated cryptography standards by the US government (though later DES was withdrawn and replaced by AES).\[13\][14] Despite not being an official standard anymore, DES (especially its still approved and much more secure variety, triple-DES) still holds a firm position. Its application is of wider range, from ATM encryption to e-mail privacy and secure remote access. There are many ciphers that have been designed and released with variation in quality whereas many have been thoroughly broken like FEAL.\[15][3\]

Unlike block cipher, stream cipher creates an arbitrarily long stream of key which is combined bit-by-bit or character-by-character (similar to one-time pad). The output stream, in a stream cipher is created based on hidden internal state which changes as the cipher operates. The secret key is used to set up the internal state. Block ciphers can be used as stream ciphers where RC4 is a widely used stream cipher.\[3\]

A third type of cryptographic algorithm is cryptographic hash functions. Message of any length is accepted as input and output a short, fixed length hash which can then be used in digital signature. For good hash functions, two messages producing same hash cannot be decoded by an attacker. MD4 and MD5 (a strengthened variant of MD4) are widely used but broken in practice. The Secure Hash Algorithm series of MD5-like hash functions have been developed by the US National Security Agency: the agency withdrew SHA-0 as it was a flawed algorithm; SHA-1, more secure than MD5 is widely deployed but attacks have been
identified by the cryptanalysts; the SHA-2 family is more developed over SHA-1 but it is not as widely deployed and moreover the US standard authority thought it “prudent” from security perspective to develop a new standard to “significantly improve the robustness of NIST’s overall hash algorithm toolkit”. Thus the best hash function design is yet to come and hold the position of a new U.S. national standard that is to be called SHA-3, by 2012.

There is much similarity between message authentication codes (MACs) and cryptographic hash functions excepting the fact that MACs has a secret key that can be used to authenticate the hash value \[3\] upon a receipt.

The public key cryptography has two different keys but mathematically related to each other. A public key and a private key was proposed by Whitfield Diffie and Martin Hellman in a ground breaking 1976 paper.\[16\] A public key is related to private key but a public key is constructed in such a way that calculation of one key (‘private’ key) is computationally infeasible from the other (the ‘public’ key). But still both the keys are generated secretly as an interrelated pair. Public key cryptography is described as “the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance”.\[17\]

The public-key is freely distributed in a public-key cryptosystems, while its paired private key must remain secret. In a public-key encryption system, encryption is done by using public key while for decryption private or secret key is used. Being unsuccessful in finding such a system Diffie and Hellman showed that by presenting the Diffie-Hellman key exchange protocol, public-key cryptography was indeed possible—a solution that is now widely use in secure communication to allow two parties to secretly agree on shared encryption key.\[12\]

A widespread academic effort in finding a practical public-key encryption system was initiated due to Diffie and Hellman’s publication, as a result in 1978 Ronald Rivest, Adi Shamir and Len Adleman design the technique which is known as RSA algorithm.\[18\] Some other examples are Cramer-Shoup cryptosystem, ElGamal encryption and various elliptical curve techniques.

The revelation of the fact that cryptographers at General Communication Headquarters (GCHQ), a British intelligence organization, had anticipated several academic developments
in a document published by the GCHQ in 1997 was a surprising event.\cite{19} It has been reported that James H. Ellis around 1970 had conceived the principles of asymmetric key cryptography. In 1973 a solution that resembles the RSA algorithm was invented by Clifford Cocks.\cite{19,20} Malcolm J. Williamson has claimed to have developed the Diffie-Hellman key exchange in 1974.\cite{7}

Public key cryptography is also used for implementing digital signature schemes. A digital signature is an indicative form of an ordinary signature. They both are easy to produce but difficult for anyone else to forge. It is possible to permanently tie the digital signature to the content of the message being signed; they cannot then be ‘moved’ from one document to another, for any attempt will be detectable. There are two algorithms in a digital signature schemes, one for signing—here a secret key is used to process the message or a hash of the message or both and another one for verification—here a matching public key is used with the message to check the validity of the signature. Two of the most popular digital signature schemes are RSA and DSA. The central to the public key infrastructure and many network security schemes (like SSL/TLS, many VPNs etc.).\cite{15}

The basis of public-key algorithm is computational complexity of hard problems, often from number theory. For example, the integer factorization problem forms the basis of the hardness of RSA, while Diffie-Hellman and DSA are related to the discrete logarithm problem. Recently, security based on number of theoretic problems involving elliptic curves has been developed by elliptic curve cryptography. To do away with the number of underlying problems, most of the public-key algorithms involve operations such as modular multiplication and exponentiation. These operations are much more computationally expensive than techniques used in most block ciphers majorly with typical key sizes. As a result, public-key cryptosystems are commonly hybrid cryptosystems. In this systems, a fast high quality symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent for the message but a public-key algorithm is used for encryption. Similarly, hybrid signature schemes in which a cryptographic hash functions computed are often used, and only the resulting hash is digitally signed.\cite{3}
1.2 Some Existing Encryption Techniques

Encryption algorithms are broadly divided into two categories

- Symmetric Key Encryption Algorithms
- Asymmetric Key Encryption Algorithms

Very common Symmetric Key Encryption Algorithms are

- AES
- Blowfish
- DES
- Triple DES
- Serpent
- Twofish

Less common Symmetric Key Encryption Algorithms are

- Camellia
- RC2
- CAST-128
- RC5
- IDEA
- SEED
- Skipjack
- TEA
- XTEA

Other Symmetric Key Encryption Algorithms are

- 3-Way
- Akellar
- Anubis
- ARIA
- BaseKing
- BassOmatic
- BATON
- BEAR and LION
- CAST-256
- CIKS-1
- CIPHERUNICORN-A
- CIPHERUNICORN-E
- CLEFIA
- CMEA
- Cobra
- COCONUT98
- Crab
- Cryptomeria/C2
- CRYPTO
- CS-Cipher
- DEAL
- DES-X
- DFC
- E2
- FEAL
- FEA-M
- FROG
- G-DES
- GOST
- Grand Cru
- Hasty Pudding cipher
- HIERO
- ICE
- IDEA NXT
- Intel Cascade Cipher
- Iraqi
- KASUMI
- KeeLoq
- KHAZAD
- Khufu and Khafre
- KN-Cipher
- Ladder-DES
- Libelle
- LOKI97
- LOKI89/91
- Lucifer
- M6
- M8
- MacGuffin
- Madryga
- MAGENTA
- MARS
- Mercy
- MESH
- MISTY1
- MMB
- MULTI2
- MultiSwap
- New Data Seal
- NewDES
- Nimbus
- NOEKEON
- NUSH
- PRESENT
- Q
- RC6
- REDOC
- Red Pike
- S-1
- SAFER
- SAVILLE
- SC2000
- SHACAL
- SHARK
- SMS4
- Spectr-H64
- Square
- SXAL/MBAL
- Threeps
- Treyfer
- UES
- Xenon
- XXTEA
- Zodiac
Some Asymmetric Key Encryption Algorithms are

- Benaloh
- Blum–Goldwasser
- Cayley–Purser
- CEILIDH
- Cramer–Shoup
- Damgård–Jurik
- DH
- DSA
- EPOC
- ECDH
- ECDSA
- EKE
- ElGamal (signature scheme)
- GMR
- Goldwasser–Micali
- HFE
- IES
- Lamport
- McEliece
- Merkle–Hellman
- MQV
- Naccache–Stern
- NTRUEncrypt
- NTRUSign
- Paillier
- Rabin
- RSA
- Okamoto–Uchiyama
- Schnorr
- Schmidt–Samoa
- SPEKE
- SRP
- STS
- Three-pass protocol
- XTR
- YAK

Out of these algorithms, few are discussed in section 1.2.1 to 1.2.9.

1.2.1 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the National Institute of Standard and Technology (NIST) as FIPS 197 in the Federal Register in December 2001. AES allows for three different key lengths: 128-bit keys, 192-bit keys and 256-bit keys where encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. In each case, all other rounds are identical except for the last round. There are four steps for each round of processing: One single-byte based substitution, a row-wise permutation, a column-wise mixing and the addition of the round keys. The order of the above four steps is different for encryption and decryption.

1.2.2 Data Encryption Standard (DES)

Data Encryption Standard (DES) is a symmetric-key based block cipher. It was the result of a research project set up by International Business Machines (IBM) Corporation in the late 1960’s. DES is based on Feistel block cipher and only operates on 64 bit blocks of data at a time. After an initial permutation, the block is broken into a right half and a left half, each 32 bits long. There are 16 rounds of identical operations in which the data are combined with
the key with key length 56 bits. In each round, the bits of the key are shifted and then 48 bits are selected from the 56 bits of the key. The right half of the data is expanded to 48 bits via an expansion permutation, combined with 48 bits of a shifted and permuted key via an XOR, sent through 8 S-boxes producing 32 new bits and permuted again. After these four operations, the output is combined with the left half via another XOR. The new right half is generated from the above operations and the old right half becomes the new left half. These operations are repeated for 16 times making 16 rounds of DES. After the sixteenth round, the right and left halves are joined and a final permutation, which is the inverse of the initial permutation, finishes off the DES algorithm.

1.2.3 Triple Data Encryption Standard (Triple DES)

The man-in-the-middle attack on Double DES has made the technique impractical and Double DES is seemed to be inadequate, therefore it paving the way for Triple DES.[13] Triple DES block cipher applies DES cipher thrice to each data block, where the block size is 64 bits. Triple DES uses three DES keys, K1, K2 and K3 (each of 56 bits, excluding parity bits), and the key sizes are 168 (=56*3), 112 (=56*2) or 56 bits with respect to keying option 1, 2 or 3 as follows:

Keying Option 1: All of the keys are independent.
Keying Option 2: K1 and K2 are independent and K3 = K1.
Keying Option 3: All of the keys are identical i.e. K1 = K2 = K3.

Keying Option 1 is the strongest with three independent keys with 168 key bits. Keying Option 2 provides less security with 112 key bits but stronger than the simply DES encrypting twice with keys K1 and K2. Keying Option 3, which has backward compatibility with DES, is equivalent to DES with 56 key bits.

The encryption and decryption algorithms of Triple DES with three independent keys are

\[
\text{Cipher Text} = E_{K3} (D_{K2} (E_{K1} (\text{Plain Text})))
\]

\[
\text{Plain Text} = D_{K1} (E_{K2} (D_{K3} (\text{Cipher Text})))
\]

The encryption and decryption algorithms of Triple DES with two independent keys are

\[
\text{Cipher Text} = E_{K1} (D_{K2} (E_{K1} (\text{Plain Text})))
\]

\[
\text{Plain Text} = D_{K1} (E_{K2} (D_{K1} (\text{Cipher Text})))
\]
1.2.4 SERPENT

Serpent is a symmetric key block cipher which was designed by Ross Anderson, Eli Biham and Lars Knudsen. Serpent has a block size of 128 bits and supports a key size of 128, 192 or 256 bits. This cipher is a 32-round substitution-permutation network operating on a block of four 32-bit words. Each round applies one of eight 4-bit to 4-bit S-boxes 32 times in parallel.

Serpent cipher consists of three basic functions:

1) An initial permutation of bits named IP
2) A round function named R which consists of a key mixing operation, a pass through S-boxes and a linear transformation. In the last round, this linear transformation is replaced by an additional key mixing operation
3) A final permutation of bits named FP

1.2.5 Twofish

Twofish is a symmetric block cipher proposed by Schneier et al. It has a block size of 128 bits, and accepts a key of any length up to 256 bits. A single key is used for encryption and decryption. Twofish is a Feistel network. Feistel network, invented by Horst Feistel, is a general method of transforming any function (usually called the $F$ function) into a permutation. In a Feistel network, the round function consists of taking one part of the data being encrypted, feeding it into some key dependent function $F$, and then XORing the result into another part of the block. Twofish algorithm is an 8-cycle algorithm having 16 rounds. Each step of the round function is bijective i.e. every output is possible.

1.2.6 Blowfish

Blowfish is a 64-bit symmetric key block cipher that uses a variable length key varies from 32 bits to 448 bits. In 1993, Bruce Schneier published this block cipher. Blowfish incorporates a 16 round Feistel network. The operations performed for this algorithm are table lookup, modular-multiplication, addition and exclusive-OR. It consists of a variable number of iterations and uses subkeys that are a one-way hash of the key. Each round consists of a key-dependent permutation and a key – and data-dependent substitution. All
operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

1.2.7 RSA Algorithm

In 1978, Ron Rivest, Adi Shamir and Leonard Adleman introduced RSA algorithm which is an asymmetric key cryptosystem. RSA involves the use of two keys: a public key, which may be known by anyone and used to encrypt messages and a private key, known only by the recipient and used to decrypt messages.

The steps for key generation of RSA algorithm are as follows:

1. **Choose p and q, two distinct random prime numbers**
2. **Compute** \( n = p \times q \).
3. **Compute** \( \phi(n) = (p-1) \times (q-1) \) [Euler’s Totient function]
4. **Choose an integer e such that** 1 < e < \( \phi(n) \) and \( \gcd(e, \phi(n)) = 1 \)
5. **Compute** \( d \equiv e^{-1} \mod \phi(n) \)
6. **Public encryption key is** (e,n) and **Private decryption key is** (d,n)

A plaintext \( P \) is encrypted to ciphertext \( C \) by \( C = (P^e \mod n) \) and the ciphertext \( C \) is decrypted into plaintext \( P \) by \( P = (C^d \mod n) \). An example for RSA algorithm is as follows:

- Let \( p = 17 \) and \( q = 23 \)
- Value of \( n = p \times q = 17 \times 23 = 391 \)
- So \( \phi(n) = (p-1) \times (q-1) = 16 \times 22 = 352 \)
- \( e = 13 \) is so chosen that 1 < e < \( \phi(n) \) and \( \gcd(e, \phi(n)) = 1 \)
- Value of \( d \) is the multiplicative inverse of 13 modulo 352, i.e. \( d = 325 \)
- The encryption key is (13,391) and decryption key is (325,391)
- Let us encrypt the plaintext \( P = 127 \) into ciphertext \( C \)
  - So ciphertext \( C = P^e \mod n = 127^{13} \mod 391 = 213 \)
- Let us decrypt the ciphertext \( C = 213 \) into plaintext \( P \)
  - So plaintext \( P = C^d \mod n = 213^{325} \mod 391 = 127 \)

Since knowing the factors of \( n \), which will give away \( \phi(n) \) and therefore \( d \), a cryptanalyst would break the algorithm. The authors of RSA recommended that the length of \( n \) be about
200 digits long. However, this length may be varied based on the importance of the speed of encryption versus security.

1.2.8 Knapsack Cryptosystem

Knapsack cryptosystem was introduced by Merkle and Hellman in 1978.[14] The encryption and decryption algorithms are based on solving a knapsack problem. The basic idea behind this scheme is to encode a binary message as a solution to a knapsack problem reducing the ciphertext to the target sum obtained by adding terms corresponding to 1s in the plaintext i.e. blocks of plain text are converted to knapsack sums by adding into the sum the terms that match with 1 bits in the plaintext.

1.2.9 NTRUEncrypt Cryptosystem

The NTRUEncrypt was first introduced at Crypto’96. The maiden version of this system was developed by three mathematicians J. Hoffstein, J. Pipher and J.H. Silverman.[22] In 1996 these mathematicians together with D. Lieman founded the NTRU Cryptosystems, Inc. and patented NTRUEncrypt cryptosystem. NTRUEncrypt is the fastest known lattice-based public key cryptosystem. It is based on the shortest vector problem in a lattice and its operations are carried out in the ring $\mathbf{R} = \mathbf{Z}[X] / (X^N - 1)$, the ring of truncated polynomials with convolution multiplication. Four sets of polynomials $L_f$, $L_g$, $L_m$ and $L_r$ (a polynomial part of the private key, a polynomial for generation of the public key, the message and a blinding value, respectively) in that ring have integer valued coefficients and degree at most $N-1$. NTRUEncrypt is actually a cryptosystem of parametrised family where each system is specified by three integer parameters $(N, p, q)$ where it is assumed that $N$ is prime, $p$ and $q$ are coprime, and $q$ is always larger than $p$.

The main advantages of the system is that the key generation, encryption and decryption can be carried out at a high speed and it can be efficiently implemented on very limited systems like single 8-bit processors. The quick key generation allows a new key to be created for every transaction. It is a probabilistic cryptosystem where a random element is used for encryption such that two different encryptions of the same message with the same key will yield different ciphertext. Its moderate key-sizes, excellent asymptotic performance and
conjectured resistance to quantum computers could make it a desirable alternative to factorization and discrete-log based encryption schemes.

1.3 Other Cryptographic Techniques

Multiple disciplines have started to work together more closely for last few decades to improve the network security for reliable communication. A number of alternative cryptosystems have gained significant attention during these periods. Few of them are discussed here.

Heisenberg’s uncertainty principle gives rise to novel cryptographic phenomena when elementary quantum systems such as polarized photons are used to transmit digital information. A quantum channel, which is not used directly to send meaningful information, can be used in conjunction with ordinary insecure classical channels to distribute random key information between sender and receivers where it remains unknown to others. The essential quantum property is the existence of pairs of properties that are incompatible in the sense that measuring one property necessarily randomizes the value of the other. In quantum physics, the measurement of linear polarization of a single photon randomizes its circular polarization. In general, any pair of polarization states will be referred to as a basis if they correspond to a reliably measurable property of a single photon and two bases will be said to be conjugate if quantum physics decrees that measuring one property completely randomizes the other. For quantum key distribution, very popular two conjugate bases are the rectilinear basis (horizontal vs. vertical polarization) and the circular basis (left-circular vs. right-circular). Though the distribution of random key information is very secure through the quantum channel but the quantum transmissions are very weak and cannot be amplified in transmit.

Another promising alternative to number-theoretic constructions are lattice–based cryptosystems which admit security proofs based on well-studied problems that currently cannot be solved by quantum algorithms. Lattice–based cryptography is nothing but the asymmetric cryptographic primitives based on lattices. Lattices were first introduced by two mathematicians Joseph Louis Lagrange and Carl Friedrich Gauss. A lattice $L$ is a set of
points in the \(n\)-dimensional Euclidean space \(\mathbb{R}^n\) with a strong periodicity property. A basis of \(L\) is a set of vectors such that any element of \(L\) is uniquely represented as their linear combination with integer coefficients. When \(n\) is at least 2, each lattice has infinitely many different bases. Mathematical problems based on lattices are the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). These problems are normally hard to solve. There are algorithms to solve these problems with a good basis. Lattice basis reduction is a transformation of an integer lattice basis into a basis with short, nearly orthogonal vectors. If we compute such a lattice basis then the CVP and SVP problems can be solved easily. Lattices have been used in different computer algorithms and in cryptanalysis. In 1996, Miklós Ajtai showed in a seminal result the use of lattices as cryptography primitive.\(^{[23]}\) In 2009, Craig Gentry using lattice-based cryptography showed the first fully homomorphic encryption scheme as announced by IBM.\(^{[24]}\) The benefits promised by Lattice-based cryptography are very strong security proofs based on worst-case hardness, relatively efficient implementations and great simplicity.

Elliptic Curve Cryptography (ECC) is a public key cryptosystem which was first suggested independently by N. Koblitz\(^{[25]}\) and V. S. Miller\(^{[26]}\) in 1985 and accepted as an alternative to existing cryptosystems over finite fields. ECC is based on the algebraic structure of elliptic curves over finite fields. An elliptic curve is a plane curve which has a set of points satisfying the equation \(y^3 = x^3 + ax + b\), along with a distinguished point at infinity. This set of points together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key. Several discrete logarithm based cryptographic scheme have been adapted to elliptic curves, replacing the group \((\mathbb{Z}_p)^X\) with an elliptic curve, like the Elliptic Curve Diffie-
Hellman (ECDH) key agreement scheme, Elliptic Curve Integrated Encryption Scheme (ECIES), Elliptic Curve Digital Signature Algorithm (ECDSA) etc.

Visual cryptography (VC) is a recent tool which encrypts the material in a perfectly secure way and uses the characteristics of human vision to decrypt the encrypted information without using any complex cryptographic computation. In 1994, Moni Naor and Adi Shamir introduced the basic model of VC for binary images.[27] For a visual variant of the k out of n secret sharing problem, the secret information is encrypted into n transparencies (for each of the n user one transparency) so that the original information is visible if k or more users stack their transparencies but totally invisible if less than k transparencies stack together. The decryption algorithm is not required. In VC, perfect alignment of the transparencies is also troublesome.

DNA based cryptosystem is another state of the art scheme for security. DNA stands for Deoxyribo Nucleic Acid. DNA represents the genetic blueprint of living creatures which contains instructions for assembling cells. For human body, every cell has a complete set of DNA which is unique for each individual. DNA is a polymer made of monomers called deoxyribo nucleotides where each nucleotide has three basic parts: deoxyribose sugar, phosphate group and a nitrogenous base. The nitrogenous bases are of two types: purins (Adenine and Guanine) and pyrimidins (Cytosine and Thymine). Adenine binds with Thymine and Guanine binds with Cytosine. The various operations performed on DNA are ligation, polymerase chain reaction (PCR), gel electrophoresis and affinity purification. DNA coding is a new area of cryptography which has appeared in recent years along with DNA computing. DNA computing is an inter-disciplinary area concerned with the use of DNA molecules for the implementation of computational processes. DNA cryptography is a subject of study about how to use DNA as an information carrier and it uses modern biotechnology as a measure to transfer plaintext into ciphertext. Plaintext message data encoded in DNA binary strands by use of an alphabet of short oligonucleotide sequences. DNA binary strands support feasibility and applicability of DNA based cryptography. The main difficulties of DNA cryptography are the requirement of high tech biomolecular laboratory and computational complexity.
1.4 Literature Survey

Currently information is electronically processed and conveyed through unreliable public networks. Data security is the main aspect for secure data transmission. Therefore, computer network security is a fast moving technology in the field of computer science. Network security using cryptography originally focused on mathematical and algorithmic aspects. As security techniques continue to mature, there is an emerging set of cryptographic techniques always. This advancement of digital communication technology benefitted the field of cryptography. The efficient encryption schemes were designed and implemented and also broken subsequently over time.

Mukherjee et al proposed two methods to reduce the number of keys to be communicated by using dependent keys related one-way functions for encrypting different parts of the bit-stream with various keys.\[28] The first method is based on using separate one-way function chains for the keys for each scalability dimension and the second method allows simultaneous key progression along multiple dimensions by using special types of quasi-commutative one-way functions called one-way accumulators. Both the methods are based on complex mathematics. Introducing the concepts of interlacing and decomposition, a block cipher has been developed.\[29] During encryption key has taken in matrix form and plain text as column vectors. The modular arithmetic inverse of the key matrices has used during decryption. A compliant authenticated encryption achieved through a novel secure encryption and authentication scheme for JPEG2000 code-streams.\[30] This proposed scheme has computational efficiency and it introduces a different public key method. An approach of encryption/decryption process has been introduced using products of primes.\[31] This generates a group from any general natural numbers which used for generation of a secured encryption/decryption process. The approach is not simple and not suitable for light weight devices having very low processing capabilities. Omary et al proposed two symmetric evolutionist-based ciphering algorithms using genetic algorithm approach.\[32] Both of algorithms generate a resistant session encryption key and formalize the problem of encryption as a combinatorial optimization problem. Some modified approach to the basic NTRU method were proposed where entire polynomial ring divided into small subsets of polynomials which can run concurrently to generate the keys and more than one person can
do the encryption and decryption at the same time. An algorithm counts n! permutations in (n-1) steps and defines a bijective function from the natural numbers to the set of permutations. In this algorithm the set of keys grows factorially and the iterative cryptosystem using the DES boxes illustrated with an example. Proposed technique is not suitable for devices having limited computing power. Multiple symmetric keys are generated using a mathematical technique which is useful for the refinement of the cipher text to increase the complexity to produce the better cipher text where the refinement process may be continued to give next better cipher text. The key, the key stream and the necessary properties are analyzed to assume from the underlying hash function for the stream cipher and conjecture the most efficient way to break the proposed stream cipher is to break the hash function or through exhaustive search for the key space K of k bits. The existing Twofish is expanded to a 256-bit block encryption algorithm which enables the 4 mutually-independent S-boxes in g-function to interacts one another and substantially raise complexity for the purpose of heightening avalanche effect. An algorithm for public key encryption using modified ML decoding technique has been introduced for finding closest vectors in a lattice to a given point (CVP). This technique is asymptotically very efficient and suitable for multicast security based on the lattice reduction problems. Doliskani et al devised a public-key cryptosystem based on the symmetric group S_n. The technique has some important properties such as non commutative, high flexibility for selecting keys that makes DLP more resistant to known attacks and added advantages of easy and fast implementation. Two substitution based block cipher were introduced which encrypt any sort of file at bit level with possible lossless data compression which ensure storage efficiency. This symmetric data encryption algorithm is much more similar to that of RijnDael where RijnDael algorithm starts with 128 bits but proposed algorithm starts with 200 bits. A technique has been introduced based on the combination of image permutation, followed by the RijnDael algorithm. Using the technique the correlation between image elements significantly decreased and higher entropy achieved. The proposed technique for efficient transmission of data from source to destination dynamically based on optimum path selection in certain distributed models and security enhancement through quantum channels can be ensured by varying the key i.e. changing the phase using non-orthogonal measurement
bases. The characteristics of Advanced Encryption Standard (AES) using S-box and Inverse S-box explained to ensure that no trapdoor is present in the cipher and to expand the key-space to slow down attacks.\[^{45}\] This property makes the S-box key dependent without changing its values and without touching Inverse S-box. A variable block length based bit level transformation has been proposed for encryption where the block is passed through a substitution operation followed by various transpositions using multi dimensional array.\[^{46}\] Different types of files are encrypted at bit level using Helical transposition and columnar transposition.\[^{47}\] A different technique has been introduced for encrypting different types of files at bit level using Fibonacci based position substitution method and compared the proposed technique with RSA and Triple DES in terms of frequency distribution and Chi-Square value.\[^{48}\] The cryptography model generates real-time based multiple symmetric keys during the complete session of the data transfer by using Quaternion Julia fractal images.\[^{49}\] The cryptographic technique overcomes noninvertible key matrix problem of Hill Cipher algorithm\[^{50}\] and this technique enhances the security of Hill Cipher against the known plaintext attack. The cryptographic algorithm considers the representation of the cipher text as elements which make up the transfer function of a discrete time system in the pole-zero form and during decryption the pole-zero form is converted into the rational form to extract the encrypted data.\[^{51}\]\ Ghosh et al proposed a private key cryptographic technique to encrypt any size as well as any sort of file at bit level.\[^{52}\] A multistage cipher technique has been introduced in which substitution, folding and permutation operations using variable multi-dimensional matrix enhance the strength of the scheme and the use of multiple numbers of keys of non-uniform lengths in various stages of the encoding process along with random session keys enhance the security features.\[^{53}\] A modification to the Advanced Encryption Standard has been presented to reflect a high level security and better image encryption by adjusting the Shift-Row phase.\[^{54}\]\ Ahmad et al compared between stream cipher and block cipher using RC4 and Hill Cipher.\[^{55}\] The authors introduced two keys used for encrypting the information transferred during communication by using the Meet in the Middle Attack on triple S-DES algorithm, instead of using Brute force attack. A modified version of existing Little Dragon cryptosystem has been introduced where the public key is bijective in nature and is mixed type i.e. quadratic in plain text and cipher text variables.\[^{56}\] proposed approach
is based on complex mathematics. A symmetric key based block encryption technique using the concept of Reversible Programmable Cellular Automata theory has been proposed which ensures to generate $2^{256}$ potential keys which means that a brute force attack impossible. A variable length data encryption technique has been introduced where grids with variable lengths are constructed from the input file which is treated as a stream of binary bits and square grid transposition is applied to form encrypted grid. In this technique, key is wrapped up with public key during encryption and wrapped up with receiver’s private key during decryption. An encryption technique which emphasizes on improving classical encryption techniques by integrating modern cipher with classical methods which is blended with Playfair and Vigenere cipher in respect of structural aspects of DES and SDES. A cryptographic technique using the combination of Zigzag, Partitioning and Swapping encrypts MPEG files. During encryption, input stream divided into $2^N$ partitions using N-bit partitioning and zigzag rule is applied on each partition before rearrange them into M number of partitions using swapping. Kaushik et al devised a symmetric key based block encryption technique which divides data into blocks of equal length and encrypts each block using a special mathematical set of functions. Proposed technique is not suitable for light weight devices having limited computing power. A cryptographic technique based on Genetic Algorithm with poly substitution methods in a linear way in which the letters in the plain text are enciphered differently based upon their placement in the text using two, three or more random keys combinations. A cryptographic technique exists at bit level consists of five stages, where in each of first four stages binary field arithmetic based substitution technique along with key association process is used and the last stage consists of a nonlinear S-box operation to generate the cipher block. An ID-based cryptosystem based on double discrete logarithm problem with distinct discrete exponents in the multiplicative group of finite fields has been introduced which does not require any interactive preliminary communications in each data transmission and has no assumption. A technique of different kind has been introduced which encrypts messages using the concept of multi codes for each character where multi numbers are assigned for each code. The encryption technique on matrix scrambling has been devised which is based on random function, shifting and reversing techniques of circular queue. This scheme consisting of
the statistical analysis, sequence random analysis and sensitivity analysis of plain text and key. Mathematical computation based private key cryptographic algorithm has been introduced which implements each character with a natural number.\textsuperscript{[67]} The one time pad encryption technique based on 9’s complement approach has been proposed in which random key stream can be used to create lifetime supply of keys for one time pad.\textsuperscript{[68]} A symmetric key cryptographic algorithm based upon 3D block ciphering technique and bit level encryption uses transposition, substitution and chaining.\textsuperscript{[69]} This approach is not preferable for devices having low processing capabilities. Incze et al describe the roadmap from the graphic encryption to the file encryption version of the pixel sieve.\textsuperscript{[70]} The weakness regarding network security in matrix NTRU cryptosystem has been exposed and a novel solution to that weakness has been proposed.\textsuperscript{[71]} The twofold selection scheme has been demonstrated which is superior to the original matrix NTRU cryptosystem and which will help cryptosystems to function under a safer environment by creating one public key and two private keys. A cryptographic system termed as Rubicryption has been introduced which uses a device named as Rubik based on the concept of Rubik’s Cube where rows and columns are shifted.\textsuperscript{[72]} Cyclic Cryptography, a different cryptographic system, has been proposed and its allied characteristics are implemented.\textsuperscript{[73]} Another symmetric key block encryption technique with multiple sub-keys has been introduced where plain text is considered as a binary bit stream and is divided into blocks.\textsuperscript{[74]} EX-OR operation is performed between these blocks and sub-keys to get cipher text. A symmetric key cryptographic system has been proposed where substitution based block cipher encryption technique is applied.\textsuperscript{[75]} A cryptosystem, based on matrix and mutation, combines and conjures up the features of matrix transposition and shifting of rows and columns along with hexadecimal number system.\textsuperscript{[76]} A data encryption technique using genetic crossover of robust biometric key and session based password has been introduced where the key is obtained by crossing over of the session key generated from the password given by the legitimate user and the biometric key generated from the fingerprint of the same user.\textsuperscript{[77]} A public key cryptosystem based on the system of higher order Diophantine equations has been proposed.\textsuperscript{[78]} In this system those Diophantine equations are used as public keys for sender and recipient, and both sender and recipient can obtain the shared secret through a trapdoor, while attackers must solve those Diophantine
equations without trapdoor. This technique is based on complex mathematics. Different research works towards text encryption and decryption using block cipher were described and reviewed and finally suggested a cryptography model in the block cipher.\cite{79} Goswami et al introduced a cryptographic algorithm based on Discrete Wavelet Transform (DWT) where the key consists of the code number of the wavelet used and the bookkeeping vector.\cite{80} Cipher text is generated using DWT where the wavelet decomposition vector contains the approximation and the detail coefficients whereas plain text is regenerated from the wavelet decomposition vector using the inverse DWT algorithm. A data security scheme has been introduced with increased data transfer rate reducing data size using data compression technique and provides data security using private key encryption system based on arithmetic coding.\cite{81} A cryptosystem based on the Martin-Hellman knapsack cryptosystem has been introduced\cite{82} which creates a subset problem which can be solved easily and then to hide the super-increasing nature by modular multiplication and permutation. The transformed vector forms the encrypted message and the original super-increasing vector forms the private key and is used to decipher the message. A new key generation mechanism has been introduced and amalgamated with the technique termed as “Fauzan-Mustafa Encryption Technique (FMET)”.\cite{83} Another variant of symmetric key cryptography scheme has been proposed which is based on changing the relative position of the bit in the eight bits data block by rotation with certain angle in either anti clockwise or clock wise direction.\cite{84} The rotation of odd or even indexes, rotation angle and rotation direction are used together as key. Another symmetric key based cryptographic algorithm using dual key for encryption with variable size of blocks with 3, 4, 5 or 6 bits has been proposed.\cite{85} Each block is interpreted as an element of a finite field and the mathematical operations performed on it are based on mathematical theory of Galois field $GF(2^n)$. This approach is not simple and not easy to implement. A hardware design of FPGA has been implemented with the dynamic key management based on conventional DES algorithm.\cite{86} This independent FPGA implementations of round-function and key generator can not only reduce the logic complication of adjacent pipeline but also realize the reconfiguration design of DES algorithm. Rasool et al proposed a symmetric key encryption technique which provides security to both the message and the secret key achieving confidentiality and
In this technique, the security level is higher due to the inherent polyalphabetic nature of the substitution mapping method used here, together with the translation and transposition operations performed in the algorithm. A new distributed key generation technique for threshold cryptography has been introduced using bivariate symmetric polynomials. The technique is based on some group $G^6$ which is either a cyclic additive group of prime order $q$ or a cyclic multiplicative group with an element of prime order $q$. A review and comparative study of block based symmetric key cryptographic techniques has been performed for image encryption which presents advantages and disadvantages of existing algorithms for encryption and decryption of an image. This review also contains the analysis of entropy and correlation between pixels value of various image encryption technique. The modification to AES has been proposed for complex encryption without increasing the size of the key block. The proposed changes in the processing of the algorithm will help to encrypt the data by making stronger diffusion and confusion. Srikantaswamy et al demonstrated that one-time pad can be used as an efficient encryption scheme by involving arithmetic and logical operations. A key generation technique has been proposed to generate a key of any length just by providing a seed value. The performance of RSA variants and Elliptic Curve Cryptography on Handheld Devices like mobile phones, PDAs etc evaluated. An encryption scheme has been introduced for Block ciphers in N-alphabet, where every member of any m-block of plain text is enciphered by different permutations which are generated by the help of a secret key word. An encryption technique using Residue Number System and a compression technique using Huffman coding and Lempel-Ziv-Welch (LZW) compression technique were introduced. A novel $(2, m + 1)$ visual cryptographic technique has also been proposed where $m$ number of secret images has been encrypted based on a randomly generated master as a common share for all secrets which is decodable with any of the shares in conjunction with master share out of $m + 1$ generated shares. In this technique, instead of generating new pixels for share except the master share, Hamming weight of the blocks of the secret images has been modified using random function to generate shares corresponding to the secrets. A block based image encryption algorithm has been introduced where the original image is divided into a number of blocks and then rows and columns are shifted within the image using a
shifted table generated by hash function and finally the encrypted image is formed from this generated image using the proposed encryption algorithm.\cite{96} A high performance AES architecture has been proposed with MUX based substitution box (S-Box) and random round selection using hardware description language (HDL).\cite{97} In this technique, the byte substitution is implemented using Field Programmable Gate Array (FPGA). An extensive and careful study has been performed on the applications of elliptic curve cryptography (ECC) and on different forms of elliptic curve in various coordinate systems specifying which is most widely used and why, on extended form of elliptic curve i.e. hyper-elliptic curve (HEC) with its pros and cons, on the performance of ECC and HEC based on scalar multiplication and DLP.\cite{98} A cryptographic scheme has been proposed which provides first level of security with smaller key size and less computation overhead using DNA Computing technique and the second level of security is provided by using the encryption and decryption algorithms of low computation Elliptic Curve Cryptography (ECC).\cite{99} The novelty of this scheme is advantages of both ECC and DNA computation is exploited in providing a high level of data security. A public key cryptographic technique has been introduced using Genetic algorithm where bit level XOR operation followed by Genetic crossover and mutation during encryption.\cite{100} Another symmetric key cryptographic technique based on secure key exchange has been proposed using elliptic curve cryptography.\cite{101} Das et al have introduced an integrated symmetric key cryptographic method combining two independent methods modified generalized Vernam cipher method and DJSA method.\cite{102} A hybrid encryption technique has been introduced using Tiger algorithm.\cite{103} In Tiger algorithm there is double protection of Data using triple DES and with the help of this algorithm transmission of data will be more secure for exchanging data over short distances from one device to another. The characteristics and performance related issues has been discussed for several symmetric block cipher algorithms like MARS, RC6, Serpent, Twofish, Rijndael and asymmetric cryptosystems like RSA, ECC, ECRYPT, HASH, DSAsg.\cite{104} An S-box construction of AES-128 block cipher has been proposed which is more robust to differential power analysis (DPA) attacks than that of AES-128 implemented with Rijndael S-box.\cite{105} The design has been prototyped on Xilinx FPGA Spartan device XC3S400-4PQ208 and the power traces of the two different running AES-128 algorithms with the proposed and
Rijndael S-boxes have been analyzed separately. A new encryption algorithm based on the modified DES algorithm has been introduced that uses an optimized framework for the throughput and security.\cite{106} The proposed algorithm outperforms the use of the same optimization framework over the variable length Rijndael algorithm and the fixed length 256-bit advanced encryption standard (AES). A different symmetric key based cryptographic algorithm has been developed where block based substitution method, logical operations like XOR and shifting operations are used.\cite{107} Banerjee et al designed an asymmetric cryptographic scheme using the phenomena of chaos synchronization with bidirectional linear feedback coupling.\cite{108} The scheme utilizes the factorization problem of two large primes and is implemented only by using the multiplication operation for both encryption and decryption. A cryptographic system has been introduced for encryptions of data streams using Pauli spin ½ matrices and finite state machine.\cite{109} This approach is based on complex mathematics. A block cipher by offering a modification to the classical Feistel cipher has been developed which includes a key on both the sides of plaintext.\cite{110} The proposed technique used XOR operation and a pair of functions for thoroughly mixing and permuting the binary bits of the plaintext and the key (in each round of the iteration process) before the result assumes the form of the cipher text. A modified Feistel cipher has been developed using a key as a multiplicand on both the sides of the plain text matrix and supplemented with mixing, permutation and modular arithmetic addition.\cite{111} A secure encryption methodology has been devised for shielding data from unauthorized access in MANET using Chinese Remainder Theorem.\cite{112} Som et al proposed a cryptographic technique to develop a character oriented poly-alphabetic cipher using a simple algebraic equation and introduced a key obtained by permuting the elements of a given key seed value.\cite{113} After a detail study of AES keys and round functions for data security, the plain text encrypted by using different key size 128, 192, 256.\cite{114} On the basis of encryption time, other parameters like processing time, round time, throughput etc were determined. Based on the concept of Rijndael algorithm, a cryptographic algorithm has been developed.\cite{115} The algorithm uses various invertible, self-invertible and non-invertible components of modern encryption ciphers and key generation same as that of AES. A symmetric key based block cipher has been introduced which is based on principles of modular arithmetic and it employs triple prime
integers as private key-spaces of varying lengths to encrypt data files. Another cryptographic algorithm based on Data Encryption Standard (DES) has been developed where one round function concept of DES were used in three different customs. A modeling method has been proposed to enhance the network security using game theory where reconnaissance is applied as a game strategy to obtain more information about the enemy’s strategic intentions. In this method, the course of action for a player in multi-player game environment with the mixed strategy has been determined, the Nash equilibrium computed and best-response strategies for the players (administrator and attacker) were found. This technique is based on complicated mathematical approach. A symmetric key based image encryption technique has been developed where block based shuffling using Arnold Cat transformation and chaotic logistic mapping using symmetric keys were performed to produce the ciphered image for transmission. A hybrid security enhancement algorithm has been designed and implemented based on AES-DES algorithms using 128 bit key. The performance of two symmetric key algorithms Data Encryption Standard (DES) and Advanced Encryption Standard (AES) analyzed with respect to the following parameters: simulation time for encryption, memory required for implementation, avalanche effects. Enhanced Identity-Base Cryptography (EIBC) has been proposed which is an efficient key management mechanism that minimizes control packets to reduce the communication overheads. An image encryption technique which is modified from DES has been introduced. In this technique the length of block and secret key reduced. Iwakiri et al described the fundamental idea of a novel DRM (Digital Rights Management) system which is composed of an incomplete cryptography and user identification mechanism to control the quality of digital contents. The PRESENT cipher which is symmetric block cipher with 64 bits of data block and 80 (or 128) bits of key analyzed and the resistance of PRESENT against brute-force attack evaluated. A one-time pad encryption algorithm, based on one-way hash algorithm and conventional block cipher, has also introduced. Cryptanalytic attack on DES, which is a known-plaintext attack based on neural networks, has been discussed. In this attack a trained neural network retrieves parts of plaintext from cipher text without retrieving the key used in encryption. The enhancement of the Data Encryption Standard (DES) block cipher studied which working in cipher feedback model
(CFB) when adjustable noise is introduced into the encrypted data in an application layer.\footnote{128} A verification strategy in the exhaustive search step of the linear attack has been designed to allow Eve to mount a successful attack in the noisy environment. The most popular and efficient encryption algorithms in smart cards such as RSA, ECC, DES and ECDSA were described and compared between these algorithms to find out the differences.\footnote{129} The confidence of detection of redundant estimated when exclusive use of statistical tests is made.\footnote{130} For detection, so-called “Crypt-X'98” suite applied on a suitably modified version of the “Serpent” cipher (finalist, AES). Battey et al introduced a new quasi-group based block encryption system with and without cipher block chaining.\footnote{131} A power analysis resistant DES algorithm architecture has been proposed to deal with the threat of power analysis to encryption device, which is combined with "asymmetric" mask technique.\footnote{132} An image encryption scheme has been introduced which employs both compressive sensing and Arnold scrambling method.\footnote{133} The design principles of elliptic curve public key cryptography analyzed and the selection method of secure elliptic curve along with its implementation has been discussed in details.\footnote{134} Advanced Encryption Standard (AES) algorithm implemented and Avalanche effect calculated by changing one bit in plaintext keeping the key constant and by changing one bit in encryption key keeping the key constant.\footnote{135} A simple and secure method of key generation has been introduced in the transmitter and the receiver using self organizing maps instead of exchange them over a public communication channel.\footnote{136} The PRESENT cipher which is symmetric block cipher with 64 bits of data block and 80 (or 128) bits of key analyzed and the resistance of PRESENT against time-memory trade-off attack evaluated using Rainbow Tables method.\footnote{137} A symmetric cryptographic algorithm has been introduced which uses new S-boxes during the encryption process where the cipher ensures high-level of confidentiality due to key-dependent S-boxes.\footnote{138} Bhadra et al introduced a different symmetric key cryptographic method called Bit Level Encryption Standard (BLES) Version-II which is based on bit exchanging or bit reshuffling method from left to right as well as from right to left of the entire bit stream.\footnote{139} A new framework has also proposed for automatically proving the security of public-key cryptographic schemes in computational model where the sequence-of-games approach has been used to construct security proof.\footnote{140} In this model, a
probabilistic polynomial-time process calculus has been designed to describe the attack games and the game transformations are executed with the help of observational equivalence. Data Encryption Standard (DES) implemented using MATLAB software and Avalanche effect calculated by changing one bit in plaintext keeping the key constant and by changing one bit in encryption key keeping the key constant.\textsuperscript{[141]} The security of PRESENT S-box studied and analyzed thoroughly in relation with linear and differential cryptanalysis.\textsuperscript{[142]} A hybrid crypto system has been proposed which utilizes benefits of both symmetric key and public key cryptographic methods.\textsuperscript{[143]} Symmetric key algorithms (DES and AES) were used in this crypto system to perform data encryption and Public key algorithm (RSA) was used in this crypto system to provide key encryption before key exchange. Combination of both the symmetric-key and public-key algorithms provides greater security and some unique features in that hybrid system. This system is not suitable for light weight devices having very low processing capabilities. A block cipher system based on the discretized Bernoulli map has been introduced that can be implemented by nonlinear feedback shift registers (NFSRs).\textsuperscript{[144]} In this system, several new methods of secret key setting of the block cipher were proposed for improvement of the key sensitivity. A design has been developed for verification of strategy against block ciphered system in linear attack and numerically optimized to allow Eve to mount a successful attack in noisy environments.\textsuperscript{[145]} Zodpe et al have introduced a different design for Hardware implementation of Data Encryption Standard (DES) cryptanalysis on Field Programmable Gate Arrays (FPGA) using exhaustive key search.\textsuperscript{[146]} Two architectures viz. Iterative and Loop unrolled DES architecture are implemented in this design. The basic block cipher algorithm described, design theory and structure were explained, and cryptanalysis discussed according to recent trend of development.\textsuperscript{[147]} A different cryptographic algorithm has been introduced which provides two phase security to the quantum cryptography system.\textsuperscript{[148]} In this algorithm the presence of the eavesdropper will not affect the security of the system as the secret key bits are modified at both sender and receiver end based on the concept of prime factor. A new parallel cryptography technique has been proposed which used DNA molecular structure, one-time-pad scheme and DNA hybridization technique.\textsuperscript{[149]} This technique certainly minimizes the time complexity. Hossain et al presented a reconfigurable system that can encrypt digital data where the system
provides the option of choosing one of familiar encryption methods DES, 3 DES and AES to the user.\(^{[150]}\) A different Substitution Permutation Network (SPN) type, symmetric-key block cipher architecture has been introduced to strengthen it against fault attack.\(^{[151]}\) The proposed SPN type architecture employs two different types of diffusion layers. A different design has been proposed for improvement of Cipher Block Chaining (CBC) encryption technique by using the Merkle-Hellman Knapsack Cryptosystem.\(^{[152]}\) This design focused on enhancing the confidentiality of the message transfer. An implementation of the three-stage quantum communication protocol in free-space has been presented where multiple photons can be used for secure communication.\(^{[153]}\) Another new symmetric key cryptographic technique has been introduced using generating function single point crossover on binary field.\(^{[154]}\) A block cipher scheme by using circular substitution and reversal transposition has been proposed to reduce both time and space complexities.\(^{[155]}\) This scheme used an arbitrarily variable key length which may even be equal to the length of the plaintext or as small as a few bits coupled with an arbitrary reversal factor. An enhanced version of RC6 block cipher algorithm has been presented which is a symmetric encryption algorithm designed for 256-bit plain text block.\(^{[156]}\) Yang et al proposed the concept to provide stream cipher service in Java Cryptographic Architecture (JCA).\(^{[157]}\) The implementation of this concept provides an abstract class for efficiently writing and maintaining any stream cipher algorithm by developers. An encoding-encryption approach has been developed to take advantage of intentional noise introduced in cipher texts for a block cipher working in cipher feedback model (CFB) or cipher block chaining (CBC) mode.\(^{[158]}\) Three encryption algorithms namely DES, AES and Blowfish were analyzed by considering certain performance metrics such as execution time, memory required for implementation and throughput.\(^{[159]}\) A new symmetric key cryptographic method has been proposed using Modified generalized Vernam cipher method with feedback along with different block sizes.\(^{[160]}\) A different image encryption technique has been presented based on DNA sequence addition operation.\(^{[161]}\) A different symmetric cryptographic technique has been developed which merged both RSA and Diffie-Hellman algorithms and a comparison has been conducted between the proposed technique, AES (Rijndael), DES, 3DES, RC2 and Blowfish.\(^{[162]}\) Two different cryptographic schemes based on DNA binary strands were discussed.\(^{[163]}\) In one of the approaches DNA based
cryptography itself used to encrypt and decrypt the message and in another approach DNA strands were used to generate key for encryption and decryption. Rafik et al introduced a different security protocol based on stateful public key encryption (StPKE) which addresses both security services for wireless sensor networks (WSNs) and where only the base station can verify the individual data and identify the malicious node. A new method has been proposed for processing halftone images that improved the quality of the share images and the recovered secret image in an extended visual cryptography scheme for which the size of the share images and the recovered image is the same as for the original halftone secret image. The concept of area optimization discussed for the most critical and computationally-intensive operation in lattice-based cryptography using polynomial multiplication with the Number Theoretic Transform (NTT). The proposed hardware architectures reduce slice usage, number of utilized memory blocks and total memory accesses by using a simplified address generation, improved memory organization and on-the-fly operand generations.

Number of cryptographic techniques are proposed each of which has some advantages and disadvantages. There is no algorithm exists as universal solutions. So there is a dearth of searching new techniques as the scenario of computing world is changing continuously with a high rate of gradients.

1.5 Objectives

The objective of modern cryptosystem is not only to provide near perfect or near risk-free security. Rather the objective of cryptography based security is to protect information by making unauthorized acquisition of the information or tampering with the information more costly than the potential value that might be gained.

In the present scenario, existing cryptographic systems depend on the exchange of keys which are used to encrypt and decrypt the information exchange. Using these key sender and receiver perform reasonably complex mathematical operations on the data stream. So it is essential to find some cryptographic techniques which are less complex but provide very
high degree of security with respect to existing cryptographic techniques along with energy awareness.

The current generation users are moving from high power personal computers, laptops and workstations to light, low-power handheld computing devices such as Windows CE, Palm™ and Handsprings. These devices provide for high connectivity with other users through the Internet. For example, the Palm™ VIIx connects to the Internet via a wireless connection relying on Cellular Digital Packet (CDPD) technology, while the Palm™ Mobile Internet Kit provides a mechanism by which Palm™ devices can connect to the Internet through a modem or cellular phone. Windows CE devices provide a similar wide range of network access technologies. So it is essential requirement for this group of users to secure their communication in terms of security as well as energy awareness.

The objectives of this thesis are to

- develop and implement cryptographic techniques which are very simple and easy to implement but provide good security
- compare the proposed techniques with the existing and industrially accepted techniques with respect to parameters like encryption and decryption times, frequency distribution, Avalanche and Strict Avalanche Effects, Bit Independence criterion, Non-homogeneity test with respect to Chi-square values
- trade-off between security and performance of light weight devices having very low processing capabilities or limited computing power

1.6 Organization of the Thesis

The thesis consists of seven chapters. Chapter 1 contains the introductory discussion of the problem and solution domain. An introductory interface about cryptography and some well known encryption techniques, Literature Survey, Objective and Organization of the thesis, metrics for evaluation and salient features of the proposed techniques have been discussed briefly.

Chapter 2 of this thesis deals with two variant of session based symmetric key cryptographic techniques. These techniques are termed as Matrix Based Bit Orientation Technique (MBBOT) and Matrix Based Bit Shuffle Technique (MBBST). Proposed MBBOT is
analyzed and compared with AES, Triple DES (TDES) and RSA whereas MBBST is compared with MBBOT, AES and TDES.

In Chapter 3, a novel symmetric key encryption technique based on the rules of Magic Square termed as Magic Square Based Bit Orientation Technique (MSBBOT) has been proposed. Analysis and comparison has been done among MSBBOT, MBBST, MBBOT, AES and TDES for their relative performances.

A session based bit level symmetric key cryptographic technique based on the concept of Spiral Matrix has been proposed in chapter 4. This technique is termed as Spiral Matrix Based Bit Orientation Technique (SMBBOT). The SMBBOT is analyzed and compared with the MSBBOT, MBBST, MBBOT, AES and TDES for comparative characteristics.

A session oriented symmetric key cryptographic technique at bit level termed as Permutative Cipher Technique (PCT) has been proposed in fifth chapter. Comparative study among PCT, SMBBOT, MSBBOT, MBBST, MBBOT, AES and TDES has been made in terms of various parameters.

Chapter 6 consists of a novel cryptographic technique based on session oriented symmetric key termed as Session Based Symmetric Key Cryptographic Technique (SBSKCT). In this chapter, a brief comparison has been done between the techniques SBSKCT, PCT, SMBBOT, MSBBOT, MBBST, MBBOT, AES and TDES.

Chapter 7 proposed a model through cascaded implementation of the devised cryptographic techniques of this thesis.

At the end list of references is given.

1.7 Metrics for Evaluation

An indicator conform the evidence that a particular condition exists or certain results have or have not been achieved. It can be either quantitative or qualitative. A metric refers to a unit of measurement that is quantitative. Several kinds of metrics have been used for evaluating the quality of the proposed cryptographic systems. The measures are encryption and decryption time, Avalanche and Strict Avalanche effects, Bit Independence criterion,
frequency distribution and Chi-square test which are described in section 1.7.1 to section 1.7.5 respectively.

1.7.1 Encryption and Decryption Time

All the test programs for the proposed techniques are equipped to calculate and display total encryption time and decryption time at the end of execution. Time taken is the difference between processor clock ticks between the starting and end of the algorithm. All times are measured in milliseconds (ms). The lower processing time means the higher speed which sometimes better for a typical end user. Since the CPU clock ticks are taken as time, there might be a slight variation with actual time. This variation is very insignificant and may be ignored.

1.7.2 Avalanche and Strict Avalanche Effects

In cryptography, the Avalanche Effect (AVAL) is a desirable property of block ciphers. Avalanche effect means that a very small number of bit changes in the plaintext will lead to a very large number of bit changes in the ciphertext. In case of high quality block ciphers, a small change in either the key or the plain text should cause a drastic change in the ciphertext. The actual term was first used by Horst Feistel in 1973. More formally, a function \( f : \{0,1\}^n \rightarrow \{0,1\}^n \) satisfies AVAL if whenever one input bit is changed, on the average half of the output bits change, where \( i \) and \( j \) (1, 2, 3, …., n) are input and output bits respectively.

The Strict Avalanche Effect (SAE) is a generalized of the avalanche effect. SAE is said to be satisfy if, whenever a single input bit is complemented, each of the output bits changes with a 50% probability. It builds on the combined concept of completeness and avalanche effect. It was first introduced by Webster and Tavares in 1985. A function \( f : \{0,1\}^n \rightarrow \{0,1\}^n \) satisfies SAE if for all \( i \) and \( j \in (1, 2, 3, \ldots, n) \), flipping input bit i changes the output bit j with the probability of exactly one half. In 1990, the notion of strict avalanche criterion was extended by R. Forre. He considered sub-functions obtained from the original function by keeping one or more input bits constant.
1.7.3 Bit Independence Criterion

In 1986, Webster and Tavares introduced another cryptographic property Bit Independence Criterion (BIC) for s-boxes.\cite{168} A function $f: \{0,1\}^n \rightarrow \{0,1\}^n$ satisfies BIC if for all $i, j, k \in \{1, 2, 3, \ldots, n\}$, with $j \neq k$, inverting input bit $i$ causes output bits $j$ and $k$ to change independently. To measure BIC, the correlation coefficient between $j$'th and $k$'th components of the output difference string is needed, which is called the Avalanche vector $A^{\text{Av}}$.

1.7.4 Frequency Distribution

Frequency distribution analyzes both the original and encrypted files. The occurrence of each character on both the files is measured. Graphs are generated where ASCII value of each character plotted along X-axis and frequency or number of occurrences of characters along Y-axis. The smoother curve in the spectrum of frequency distribution indicates that it is harder for a cryptanalyst to detect the original message bytes.

1.7.5 Chi-square Test

Chi-square value is calculated from the character frequencies using the formula devised by Karl Pearson.\cite{169}

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i}$$

where,

$O_i$ (Occurred) is the frequency of occurrence of character $i$ in the encrypted message

$E_i$ (Expected) is the frequency of occurrence of character $i$ in the original message

Chi-square test is used to determine whether the observed sample frequencies differ significantly from the expected frequencies. The higher the Chi-square values the more deviation from the original message. The large Chi-square values confirm the heterogeneity of the source file and the encrypted file. Larger Chi-square value compare to tabulated Chi-square value ensure the higher degree of heterogeneity.
1.8 Salient Features of the Proposed Techniques

In this thesis, the logic of the proposed cryptographic techniques is simple to understand and implementation is easy using any high level programming language. Since keys are session based which varies session to session and key size is variable in length, the security of the proposed techniques is good. All the proposed techniques can handle any sort of input file of any size. There is no alteration of input file size i.e. after encryption file size remains unchanged. The salient features of all the proposed techniques are summarized as follows:

- Provide good security
- Adopted session based symmetric keys
- Keys are variable in length
- Manage to encrypt bit stream of any size
- No space overhead
- Logics are simple to understand and easy to implement
- Introduced Variable Cipher Block Chaining (VCBC)