Chapter 2: Literature Survey

2.1 Introduction

The field of cryptography deals with the techniques for conveying information securely. The goal of cryptography is to allow the intended recipients of a message to receive the message securely. Cryptography tries to prevent the eavesdroppers from understanding the message. The message in its original form is called plaintext. The transmitter of a secure system will encrypt the plaintext in order to hide its meaning. This meaning will be revealed only after the correct recipient tries to access it. This reversible mathematical process produces an encrypted output called cipher-text. The algorithm used to encrypt the message is a cipher. The unauthenticated user can also try to access the information. The analysis is carried out to check if cipher’s security is satisfactory from unauthorised access. Cryptanalysis is the science of breaking ciphers, and cryptanalysts try to defeat the security of cryptographic systems. A cipher-text can be transmitted openly across a communications channel. Because of its encrypted nature, eavesdroppers who may have access to the cipher-text will ideally be unable to uncover the meaning of the message. Only the intended recipient, who has the valid key, can decrypt the message to recover the plaintext and interpret.
Ciphers can be classified using several criteria. According to one criterion, the ciphers are classified as symmetric key and asymmetric key [48]. In symmetric key ciphers, the same key is used for both encryption and decryption. A major problem with such a system is that the sender and receiver must know the key prior to transmission. This requirement makes such a system difficult to use in practice. The key cannot be openly transmitted since that would compromise the security of the system. One possibility is for the two parties to meet and exchange the keys prior to transmitting their messages. However, this exchange becomes more difficult when many parties are involved in a communications network. An asymmetric key cipher uses different keys for encryption and decryption [49]. These two keys are mathematically related, but it is very difficult to obtain one from the other unless one knows the transformation. The key used for encryption is called the public key and the key used for decryption is called the private key. The public key can be revealed without compromising the security of the system. The corresponding private key, however, must not be revealed to any party.

Currently information is electronically processed and conveyed through public networks. The main objective of cryptography is, to conceal the content of messages transmitted through insecure channels such that it guarantees privacy and confidentiality in the communications to the authorized users. Since the early 1960’s, cryptography has no longer been restricted to military or governmental
concerns, that has spurred an unprecedented development of cryptographic technique [50]. This advancement of digital communication technology benefitted the field of cryptography. The efficient encryption schemes were designed.

### 2.2 The Phases of Cryptography

Modern cryptography originates in the works of Feistel at IBM during the late 1960’s and early 1970’s [51]. DES was adopted by the NIST, for encrypting unclassified information in 1977. DES is now replaced by the Advanced Encryption Standard (AES), which is a new standard adopted. Another milestone happened during 1978, marked by the publication of RSA [52]. The RSA is the first full-fledged public-key algorithm. This discovery by and large solved the key exchange problem of cryptography. RSA also proposed the world wide acceptable standard techniques like authentication and electronic signatures in modern cryptography. In the 1980s, elliptic curve cryptography (ECC) [53] became popular due to its superior strength per bit compared to existing public key algorithms such as RSA. ECC is able to produce higher security using a key of small size. This superiority of ECC over RSA resulted into effective usage of bandwidth and quick implementation [54]. This property of ECC made it highly appealing in the field of cryptography. IEEE proposed P1363-2000 standard which recognizes ECC based key agreement and digital signature algorithms [55]. This standard lists the secured curves that can be used for ECC based
cryptosystems. Both these techniques require highly mathematical operations which are power consuming. These systems also have a centralized threat of key compromise.

In 1993, chaotic cryptography is introduced, which takes advantage of the complex behaviour of chaotic dynamical systems to hide or mask information. Since then, many different implementations of this basic idea are proposed. The different methods devised so far for the use of chaotic methods are found [56, 57, 58]. The chaotic behaviour can be distinguished by its extreme sensitivity to initial conditions; it leads to long term unpredictability. The signals resulting from chaotic dynamics are broadband and present random like statistical properties, although they are generated by deterministic systems. There exist a definite connection between the random looking behaviour exhibited by chaotic systems and the properties of confusion and diffusion, required for Shannon cryptosystems [59]. This motivates the use of chaotic systems for secure communications. This system is still questionable as the behaviour of any chaotic function is chaotic for a finite limit.

Another concept of policy-based cryptography was formalized in 2005 [60]. This provides a framework for performing cryptographic operations with respect to policies formalized as monotone Boolean expressions written in standard normal forms. A policy based encryption scheme allows encrypting of the message with respect to a policy in such a way that only the policy compliant users are able to decrypt the
message. A policy consists of conjunctions (logical AND operation) and disjunctions (logical OR operation) of conditions, where each condition is fulfilled by a digital credential representing the signature of a specific credential issuer on a certain assertion. A user is thus compliant with a policy if and only if he has been issued a qualified set of credentials for the policy i.e. a set of credentials fulfilling the combination of conditions defined by the policy. Policy based encryption belongs to an emerging family of cryptographic schemes. Policy based cryptosystems have the ability sharing to integrate encryption with credential based access structures. This ability allows several interesting applications in different contexts but not restricted to oblivious access control [61], trust negotiation, and cryptographic workflow [62].

Another interesting area that is the focus of recent research is quantum cryptography [63]. This arose as a potential solution to the key establishment problem but the scope has broadened considerably. Most of the current research concentrates on experimental physics but the impact of the results could be significant.

Essentially all current experimental activity in quantum cryptography is in quantum key exchange (QKE) [64]. The experiments use photons to create a shared bit string between two parties. The security of QKE relies on the physical law that it is impossible to obtain information about the quantum state of a particle without introducing a disturbance. Any eavesdropping attempt can be detected. The security of
QKE does not depend on any computational assumptions in particular, shared keys established by QKE never become insecure when faster computers or new algorithms are introduced. Photons can be transported either through optical fibres or in free space. Recent experiments in free space have demonstrated QKE over distances of the order of 20 km. A future aim within the reach of current technology is QKE between the ground and a satellite [65]. Current technology limits QKE using optical fibres to distances of less than roughly 100 km. Basic QKE systems using existing telecom optical fibres are commercially available. Current challenges include the development of reliable single photon sources, higher detector efficiencies, better key generation rates, authentication, and the integration of a QKE system into a computer network.

Overall cryptography combines mathematics, computer science, sometimes electrical engineering, and a twisted mindset that can figure out how to get around rules, break systems, and subvert the designers’ intentions.

2.3 Challenges to Develop Secured System

Building cryptography into products is very hard. Most cryptography products on the market are insecure. Some are obviously flawed. Others are more subtly flawed. Sometimes people discover the flaws quickly, while for others it takes years. Sometimes a decade goes by before someone invents new mathematics to break the system. The flaws can be in the trust model, the system design, the algorithms and
protocols, the implementations, the source code, the human computer interface, the procedures, the underlying computer system [66]. Flaws cannot be found through normal beta testing. It has been shown that security has nothing to do with functionality [67]. A cryptographic product can function normally and be completely insecure. Flaws remain undiscovered until someone looks for them explicitly. Most importantly, a single flaw breaks the security of the entire system [68]. If cryptography is a chain then the system is only as secure as its weakest link. This means everything has to be secured. It is not enough to make the algorithms and protocols perfect but the implementation also must be perfect. A great product with a broken algorithm is useless and a great algorithm, protocol, and implementation can be ruined by a flawed random number generator [69]. Under these circumstances the most rational design decision is to use as few links as possible, and as high a percentage of strong links as possible. Since it is impractical for a system designer to analyze a completely new system, a smart designer reuses components that are generally believed to be secure, and only invents new cryptography where absolutely necessary [70,71].

### 2.4 Key management methods and definitions

The data encipherment only cannot provide security to any system. To decrypt the enciphered information the key has to be shared amongst all the legitimate users. The communication involves two or more participants. Hence the importance of secret sharing and management of
the keys is a vital problem. Large numbers of methods have been proposed in the literature to solve this problem. These methods of secret sharing use the cryptographic protocols.

Any cryptographic protocol is also an essential component in security. The protocol consists of following components. A two party cryptographic protocol may be defined as the specification of an agreed set of rules on the computations and communications that need to be performed by two entities A (Alice) and B (Bob), over a communication network, in order to accomplish some mutually desirable goal, which is usually something more than simple secrecy. Several essential properties of cryptographic protocols are as follows. Correctness, guarantees that every trusted party should get the agreed output. The privacy assures about the protection of every party’s secrets. Fairness means if a dishonest party exists, neither will it gain anything valuable, nor honest party may lose anything valuable. In the game theoretical model two new properties regarding dishonest behaviours can be defined exclusiveness, which implies that one or both parties cannot receive their agreed output. Voyeurism is contrary to privacy because it implies that one or both parties may discover the other’s secret [72]. The previous definition of fairness agrees with the rationality concept described in because fairness here is a property which is understood to be more practical than theoretical. In other words, protocols are here defined according to their practical security against any kind of adversaries. In a worst case
analysis of a protocol, one must assume that any party may try to subvert the protocol. While designing a two party cryptographic protocol one of two possible models can be considered. These are

- Semi honest model: when it is assumed that the protocol is cooperative and both parties follow the protocol properly in such a way that they help each other to compute $f_i(M_A, M_B)$, but curious parties may keep a record of all the information received during the execution and use it to make a later attack.

- Malicious model: where it is assumed that parties may deviate from the protocol. In this case, during the interaction, each party acts non-cooperatively and has different choices which may determine the output of the protocol.

But the network supports various types of communications like one to many, many to one, one to one (peer) and many to many communications. The cases of many to many communications are essentially very important to study as all the cases are covered. Hence a detailed study of group communication is done. The many to many communication is like IP broadcast or multicast. Based on various applications the tailor made protocols are designed and presented in the literature [72]. This communication is called as group communication. As IP multicast comes to play a fundamental role in several emerging network applications such as online conferencing, distributed multiparty games, communication of stock quotes to brokers, etc. The security of
group communications is a critical networking issue. However, for this model of communication, the issues and problems of security are complex since group settings involve multiple participants who may join and/or leave dynamically. In order to secure group communications, security mechanisms such as authentication, access control, integrity verification and confidentiality are required. Group communication confidentiality requires that only group members could read multicast data even if the data are broadcast to the entire network. This key is generally called group key and the underlying management problem is called group key management. A group key management protocol must establish and distribute the group key while meeting the following requirements [73]

Group key secrecy: non-group members should not have access to any key that can decrypt any multicast data sent to the group.

Key independence: a user who knows any proper subset of group keys cannot discover any other group key not included in the subset.

Forward secrecy: members who left the group should not have access to any future key. This ensures that a member cannot decrypt data after he leaves the group.

Backward secrecy: a new user who joins the session should not have access to any old key. This ensures that a member cannot decrypt data sent before he joins the group in order to meet the last two requirements; a rekey process should be triggered after each join/leave to/from the
group. Based on various types of frequent actions on joining and leaving groups several protocols were introduced. One such protocol is a group key agreement protocol from pairings is introduced [74]. The protocol is adaptive to the fast changing group, but the protocol is not scalable and the resynchronization overhead is too much. In the group communication there are basically two methodologies one is centralized other is distributed. Group key management protocols received a lot of interest with the proliferation of the Internet and group based applications. Key management protocols play a key role in securing group communications. In real multicast sessions, nodes can fail and messages may be delayed or lost. These conditions affect considerably the performance of key establishment protocols. Most proposed solutions in the literature do not take this parameter into consideration. [75, 76] Failure detectors need a periodic exchange of failure information between members. This creates an overhead, which can be a serious drawback for networks with limited bandwidth or highly traffic. [77] It is possible to reduce considerably this overhead by using an adapted organization of group members.

On the similar grounds a tree based key management framework was also proposed. The scheme proposed Matsuzaki et al [78]. The method suffers badly from retrieval time of the key. This method is distributed in nature. A lot of other modified methods were produced which are the variants of Matsuzaki et al with modification [79, 80].
The authentication and authorization is the first and most critical in the cryptographic protocol. There are various schemes followed to authenticate the user. Some of the schemes are described briefly. The users are treated as subjects and the resources like memory and devices are treated as objects in case of Discretionary Access Control (DAC) [81]. A set of access rights of both of these are created. The conditions are built using predicate logic for the access control. The access rules are the business logic. These predicates are generated using access control matrix. The subjects will be able access the objects if certain permissions are available after evaluation of the predicates.

The basic method followed by mandatory access control (MAC) is the movement of the data in the given system. DAC is used in all the operating systems of computer but the use of MAC can make it better as it looks at the data from the angle of flow in the system which is more composite. In either of the cases maintenance of the data and permissions associated needs to be stored separately. A complex logic has to be developed to meet the changing business needs. The delegation of the access control is the difficult task.

To stand up to the structure that is followed in the industry another authorization model is followed. For the authentication system for the access of the information becomes more difficult if a new user is introduced to the system. The processes of relation this new subject to all the objects has to be carried out. It is not possible to connect the
subject authorization directly. This process will be tedious with respect to time. Further the assignments in the industry demand the dynamic changes in the access control system. It is not only consuming, but it may lead to errors also. As user assignments change over the time mostly the user gets more privileges than necessary. The access control module is separated as a separate mechanism in role based access control model (RBAC) [81]. This model assigns the data access irrespective of the state of the information. The jobs associated with subjects are called as roles. Every subject is a part of role and it is associated with certain permission. The user belonging to each role has definite permissions. This access control mechanism is closer to the administrative demands of the industries. A new layer introduced by RBAC never allows a user to connect directly to the permissions. The mutual authentication happens between the roles and the user. Each user has a role and role has a set of users. This module takes care of the overhead of authorization. The two different tasks need to be managed one is to manage roles and their permissions and the other to manage users and the roles. RABAC is the efficient authorization technique but role resolution and role mapping have numerous combinations which reduces the scalability.

Microsoft has introduced a new service in support of user centric web solutions. This is Microsoft .net invention. These are called as .net my services. This initiative enables the user as a single window
authentication like passport. This password based initiative is called as single sign in (SSI) Microsoft.net passport [82]. The Microsoft .net passport has been a popular as the widespread unique identity across all the applications in the web. This same identity is valid across all the email services DNS services etc. The passport needs the shared secret stored in the Microsoft servers centrally or distributed. This is similar to the technique like trusted third party.

Another authentication technique called Kerberos was invented in MIT. Earlier three variants of Kerberos systems were tested on campus and the forth version was released for the open use. Some websites avail the Kerberos functionality from MIT but some of them provide it on their own. The customizations are made by the users of Kerberos according to the needs [83]. This permit the users not to send the authorizations like user name and passwords to the service provider instead it is done by Kerberos itself. There is a ticketing system available in Kerberos which takes care of this authorization. A third party will authenticate user due to the involvement of a trusted KDC. These tickets are verified by the authentication server and the ticket grant server (TGS) [84]. The authentication server authenticates the legitimate users and sends a request to TGC to grant the ticket grant ticket request. This third party authentication is not best suited for a large scale network. One more authentication scheme called SESAME [85] is also used. The Secure European System for Applications in a Multi-vendor Environment
(SESAME) supports for the development project that aims to develop an arrangement for the security of distributed networked systems. The Kerberos is used as an extension to authorize and authenticate users in the system. The users are attached to certain license. This is issued by the Privilege attribute server (PAS). This PAS further issues Privilege Attribute Certificates (PAC). This PAC contains all the information for the access of the data associated with the user as per the guidelines provided by the PAS. This PAC contains necessary information like identification information of the user, organization and the attribute details. This information is resolved by the application server later and the user having the valid PAC is permitted to access the data for which the attributes are resolved by PAS.

The important aspect in all these methods adopted is secret sharing. Hence this is the most important aspect while designing any key exchange or management system. Secret sharing schemes are multi-party protocols related to key establishment. The motivation for secret sharing is establishing the key without revealing it. To safeguard cryptographic keys from loss, it is desirable to create backup copies. The greater the number of copies made, the greater the risk of security exposure; the smaller the number, the greater the risk that all are lost. Secret sharing schemes address this issue by allowing enhanced reliability without increased risk. Secret sharing also facilitates distributed trust or shared control for critical activities. The idea of secret
sharing is to start with a secret, and divide it into pieces called shares which are distributed amongst users such that the pooled shares of specific subsets of users allow reconstruction of the original secret. This may be viewed as a key pre distribution technique [86], facilitating one-time key establishment, wherein the recovered key is pre determined (static), and in the basic case, the same for all groups. A secret sharing scheme may serve as a shared control scheme if inputs (shares) from two or more users are required to enable a critical action.

If the shared secret is undivided then it becomes symmetric cryptography. If the secret is unequally broken then it becomes asymmetric cryptosystem. The new approaches are made to overcome the drawbacks of symmetric and asymmetric key cryptography. This hybrid cryptosystem [87] is a combination of protocols and algorithms using multiple ciphers of different types together, each to its best advantage. One common approach is to generate a random secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient’s public key. The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient. The recipient decrypts the secret key first, using his/her own private key, and then uses that key to decrypt the message. This is basically the approach used in Pretty Good Privacy [88].
PGP combines some of the best features of both conventional and public key cryptography [89]. PGP is a hybrid cryptosystem. When a user encrypts plaintext with PGP, PGP first compresses the plaintext. Data compression saves modem transmission time and disk space and, more importantly, strengthens cryptographic security. Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher. Compression reduces these patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis.

PGP then creates a session key, which is a one-time-only secret key. This key is a random number generated from the random movements of your mouse and the keystrokes you type. This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient’s public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient. Decryption works in the reverse. The recipient’s copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the conventionally encrypted ciphertext.

2.5 Role of network security

On top of all these the location of the cryptographic algorithms at the proper location in the OSI model is a challenge. The role of network security becomes essential. At the same time added security decreases the network efficiency [90]. The decision making criteria using the
predicates [91] is better and secured and adds to the efficiency of the computer networks.

Another such effort towards the security is Virtual Private Networks (VPN) as private networks are expensive and face the problem of physically securing their lines. VPN offer an economical solution to this problem by establishing a virtually private network while physically sharing the Internet media. Privacy is achieved by creating a cryptographically secure tunnel between authenticated peers, making the traffic virtually invisible to the rest of the Internet but leads to the issue of key management.

The protocols like Diffie-Hellman, Oakley key exchange [92], SKEME and Internet key exchange (IKE) [93] are not presently the universal standards. The Deffie Hillman protocol fails to authenticate the legitimate users. The man in middle is also one such threat to this method. IKE does not provide any management of certificates or long-term keys. Thus, in general, the shared secret should be exchanged offline.

Looking in to the details and the nature of the difficulty a new system design is proposed in this work. The proposed system has its own key management life cycle. This system is proposed after studying all the security aspects including the network layer level security. In this work the consideration is given to a new predicate routing algorithm for the security also. The difficulty involved in the sub-graph problem also is
considered. The numbers generated called keys are also tested for their pseudo-randomness.

**The properties of cryptographic keys**

A method of producing random like digits is called as pseudo random number generator. The digits produced by such method are not completely random. Only some natural processes like noise radioactive decay etc. are actually random. As the computers work on iterative methods which repeat the same set of instructions and algorithms, it is difficult to produce the random sequence. The iterations lead to recurrence relations which make the sequence highly predictable. This leads to a threat that an attacker can reproduce sequence to know all the possible sets of numbers that can be generated using this mechanism. It is also a fact that after some finite time the generator will reproduce the numbers which were generated previously. The algorithms used are responsible for this problem. The techniques like hashing and some cryptographic fundamentals are used in various orders to produce the pseudo-random sequence. It is called as PRNG. It is expected that an excellent pseudo-random generator should generate a sequence which has very low probability of prediction. In the modern cryptography the generators are available in the form of algorithms but still the sequence generated by these is will not be known to the intruder. The generator must have strong statistical properties. It is also
necessary that the computational cost involved in generating these numbers must be less. As stated earlier all the PRNG reproduce the same sequence sooner or later, it is expected that this period must be suitably large to be predicted by intruder. All the PRNG need a seed value which is projected to an impossible value. If this seed value is supplied as an input the PRNG produces an entirely different sequence which is pseudo-random in nature.

The need for random and pseudorandom numbers arises in many cryptographic applications. For example, common cryptosystems employ keys that must be generated in a random fashion. Cryptographic protocols also require random or pseudorandom inputs at various points, e.g., for auxiliary quantities used in generating digital signatures, or for generating challenges in authentication protocols. Security of an algorithm rests in keys. If cryptographically weak process is used to generate keys then the whole system will be weak. Only the key should be secret. Cryptographic mechanisms depend on the confidentiality of keys. Algorithms are in the public domain.

To engage in secure communications there is a need to securely distribute a secret key or public key. Keys should be dynamic. Hence a cryptographically strong key must be generated, and thus the key management becomes the major issue in cryptography. Usually Random numbers are numbers that occur in a sequence such that two conditions
are met: The values are uniformly distributed over a defined interval or set, and it is impossible to predict future values based on past or present ones.

The sequences of this kind are very rare and less in numbers and easily the algorithm can be compromised with this small set. Also cryptanalysis is carried out to know the strength of the key. The uniqueness of the key also supports following properties used in cryptography they perfectly match with each other.

- The important use of randomness is the generation of unique values
- Unique random strings are important in cryptographic protocols to prevent replay attacks, in which an adversary tries to reuse correct values from previous executions of the protocol, hoping that they'll seem correct in the current attempt.
- If a user wants to use an encryption algorithm, it is best that they select a random number as the key. If this is not done properly, security can be compromised.
- Random sequences cannot be reused and must never become available to any attacker, which implies a continuously operable generator.
- Since a requirement in cryptography is unpredictability to an attacker, any published random sequence is a poor choice, as are
such sequences as the digits in an irrational number such as the φ or even in transcendental numbers such as π, or e. Put another way, in cryptography, random bit streams need to be not only random, but also secret and hence unpredictable.

The non availability of the random numbers and increasing demand of cryptographic keys expects a better key generation algorithm that produces many keys that meet the criteria of secure keys. Also the popular RSA algorithm is time consuming and uses session keys for the secured communication. The power used by RSA for generation and management of the keys is very large. The latest handheld devices need better security as well as low power consumption. The solution lies in providing the key management in the symmetric keys. The evolutionary computing based systems that are used to solve the NP problems which have multiple solutions are used for the key generation and management. Various PRNG are tested for their generated key values. These values are tested for randomness.