CHAPTER 1

INTRODUCTION

1.1 GENERAL

Cryptography is defined as the study of mathematical techniques related to some aspects of information security. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce. The goals of Cryptography are Confidentiality, Data integrity, Authentication and Non-repudiation. Confidentiality is a service used to keep the content of information secret from all except the authorized users. Data integrity is a service which addresses the unauthorized alteration (addition, deletion, modification) of data. Authentication is a service related to identification. This function is applied to both entities and information itself. In entity authentication, the claimant must identify himself/herself to the verifier. This can be done with one of the three kinds of witness: something known, something possessed or something in him/her. A secret known only by the claimant for example a password, a PIN comes under something known. Some identification card, a passport or a driving license possessed by the claimant belong to the second kind. Some inherent characteristics like conventional signatures, finger print, voice, facial characteristics, retinal pattern belong to the third kind.

Knowledge of the password is assumed to guarantee that the user is authentic. The weakness in this system for transactions is that passwords can

often be stolen, accidentally revealed, or forgotten. For this reason, Internet business and many other transactions require a more stringent authentication process. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure is likely to become the standard way to perform authentication on the internet. Non-repudiation is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. A procedure involving a trusted third party is needed to resolve the dispute.

Assume a sender Alice (as is commonly used) wants to send a message m to a receiver referred to as Bob. She uses an insecure communication channel. For example, the channel could be a computer network or a telephone line. There is a problem if the message contains confidential information. The message could be intercepted and read by an eavesdropper or even worse, the adversary might be able to modify the message during transmission in such a way that the legitimate recipient Bob does not detect the manipulation.

1.2 ENCRYPTION AND SECRECY

The fundamental and classical task of cryptography is to provide confidentiality by *encryption methods*. The message to be transmitted can be some text, numerical data, an executable program or any other kind of information which is called the *plaintext*. Alice encrypts the plain text m and obtains the *ciphertext* c. The ciphertext c is transmitted to Bob. He then turns the ciphertext back into the plaintext by *decryption*. To decrypt, Bob need some secret information. However, the encryption should guarantee secrecy and prevent anyone from deriving any information about the plaintext from the observed ciphertext without the knowledge of the key.

In classical encryption schemes, encryption and decryption algorithms depend on the same secret key k. These encryption methods are called *symmetric-key encryption schemes*. DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm, AES (Advanced Encryption Standard) etc. are some of the symmetric encryption schemes.

Diffie and Hellman (1976) introduced the concept of public-key cryptography. They provide a solution to the long standing problems of key exchange and pointed the way to *digital signatures*. In public-key encryption scheme, each recipient of messages has his/her personal key $k = (pk, sk)$, consisting of two parts: pk is the encryption key and is made public, sk is the decryption key and is kept secret. If Alice wants to send a message m to Bob, she encrypts m by the Bob's publicly known encryption key pk. Bob decrypts the ciphertext by using his decryption key sk, which is known only to him.

Mathematically speaking, public-key encryption is a one-way function with a trapdoor. Everyone can easily encrypt a plaintext using the public key pk but the other direction is difficult. It is practically impossible to deduce the plaintext from the ciphertext, without knowing the secret key sk which is called the trapdoor information. Public-key encryption methods require more complex computations.

1.3 OBJECTIVES OF CRYPTOGRAPHY

Providing confidentiality is not the only objective of cryptography. Cryptography is also used to provide solutions for other problems like Data Integrity: the receiver of a message should be able to check whether the message was modified during transmission, either accidentally or deliberately. No one should be able to substitute a false message for the original message, or parts of it. Authentication: the receiver of a message should be able to

verify its origin. No one should be able to send a message to Bob and pretend to be Alice (data origin authentication). When initiating a communication, Alice and Bob should be able to identity each other (entity authentication). Non-repudiation: the sender should not be able to later deny that she/he didn't send a message.

If messages are written on paper, the paper provides a certain security against manipulation. Hand written personal signatures are intended to guarantee authentication and non-repudiation. If electronic media are used, the medium itself provides no security at all, since it is easy to replace some bytes in a message during its transmission over a computer network, and it is particularly easy if the network is publicly accessible, like the Internet. So, while encryption has a long history, the need for techniques providing data integrity and authentication is rapidly increasing in electronic communication.

There are symmetric as well as public-key methods to ensure the integrity of message. Classical symmetric methods require a secret key k that is shared by the sender and receiver. The message m is augmented by a *message authentication code* (MAC). The code is generated by a hashing algorithm and depends on the secret key. The augmented message $(m, H_k(m))$ is protected against modification. The receiver may test the integrity of an incoming message (m, md) by checking whether $H_k(m) = md$, where md is the message digest.

1.4 CRYPTOGRAPHIC PROTOCOLS

Encryption and decryption algorithms, cryptographic hash function are the basic building blocks for solving problems involving secrecy, authentication or data integrity. In many cases a single building block is not sufficient to solve the given problem, hence different primitives must be

combined. A series of steps must be executed to accomplish a given task. Such a well-defined series of steps is called a *cryptographic protocol.*

1.5 EVALUATING THE SECURITY OF A CRYPTOSYSTEM

In 1949, Claude Shannon published a paper entitled 'Communication Theory of Secrecy Systems' in the Bell Systems Technical Journal. This paper had a great influence on the scientific study of Cryptography. There are various approaches for evaluating the security of a cryptosystem. Among these, most useful criteria for evaluating the security are computational security, provable security and unconditional security.

1.5.1 Computational Security

This measure concerns the computational effort required to break a cryptosystem. A Cryptosystem is said to be computationally secure if the best algorithm for breaking it requires at least N operations, where N is some specified, very large number. The problem is that no known practical cryptosystem can be proved to be secure under this definition. In practice, people often study the computational security of a cryptosystem with respect to certain types of attacks (eg. exhaustive key search).

1.5.2 Provable Security

Another approach is to provide evidence of security by means of reduction. In other words, if the Cryptosystem can be shown to be 'broken' in some specified way, and then it would be possible to efficiently solve some well-studied problem that is thought to be difficult. For example, it may be possible to prove a statement of the type "a given cryptosystem is secure if a given integer cannot be factored". Cryptosystem of this type are sometimes termed as provably secure. This is a similar situation to proving that a

problem is NP-complete: it proves that the given problem is at least as difficult as any other NP-complete problem.

1.5.3 Unconditional Security

This measure concerns the security of cryptosystem when there is no bound placed on the amount of computation that an attacker is allowed to do. A Cryptosystem is defined to be unconditionally secure if it cannot be broken, even with infinite computational resources.

1.6 DIGITAL SIGNATUARE SCHEMES

A ‘conventional’ hand written signature attached to a document is used to specify the person responsible for it. A signature is used in everyday situations such as writing a letter, withdrawing money from a bank, signing in contract, etc. A signature scheme is a method of signing a message stored in electronic form. As such, a signature scheme can be transmitted over a computer network. With a conventional signature, a signature is a part of the physical document being signed. However, a digital signature is not attached physically to the message that is signed, so the algorithm that is used must somehow binds the signature to the message. A conventional signature is verified by comparing it to other, authentic signatures. Digital signatures, on the other hand, can be verified using a publicly known verification algorithm. Thus, anyone can verify a digital signature. The use of a secure signature scheme will prevent the possibility of forgeries.

Another fundamental difference between conventional and digital signatures is that a copy of a singed digital message is identical to the original. On the other hand, a copy of a signed paper document can usually be distinguished from an original. This feature means that care must be taken to prevent a signed digital message from being reused. For example, if Alice

signs a digital message authorizing Bob to withdraw Rs.1000 from her bank account, she wants Bob to be able to do so only once. So message itself should contain information, such as a date that prevent it from being reused..

A signature scheme consists of two components: a signature algorithm and a verification algorithm. Alice can sign a message m using a secret signing algorithm $sign_k$ which depends on a secret key sk. The resulting signature $sign_{sk}(m) = s$ can be subsequently be verified using a public verification algorithm $veri_{pk}(m,s)$. Given a pair (m,s), where m is the message and s is a purported signature on m, the verification algorithm returns an answer 'true' or 'false' depending on whether s is a valid signature for the message m. These ideas are described formally using the following mathematical notation. A digital signature scheme is a quintuple (P, A, K, S, V), where the following conditions are satisfied.

1. P is a finite set of possible messages
2. A is a finite set of possible signatures
3. K, the keyspace, is a finite set of possible keys
4. For each $sk \in K$, there is a singing algorithm $sign_k \in S$ and a corresponding verification algorithm $veri_{pk} \in V$. Each $sign_{sk} : P \to A$ and $veri_{pk} : P \times A \to \{0,1\}$ are functions such that the following equation is satisfied for every message $m \in P$ and for every signature $s \in A$:

$$veri_{pk}(m,s) = \begin{cases} 1; s = sign_{sk}(m) \\ 0; s \neq sign_{sk}(m) \end{cases}$$

A pair (m,s) with $m \in P$ and $s \in A$ is called a signed message. For every $sk \in K$, the function $sign_k \in S$ and $veri_{pk} \in V$ should be polynomial-time

functions. $veri_{pk} \in V$ will be a public function and $sign_k \in S$ will be private/secret. Given a message m, it should be computationally infeasible for anyone other than Alice to compute a signature s such that $veri_{pk}(m, s) = true$. If Charlie can compute a pair (m, s) such that $veri_{pk}(m, s) = true$ and m was not previously signed by Alice, then the signature s is called a forgery. Informally, a forged signature is a valid signature produced by someone other than Alice.

It is common not to sign the message itself, but to apply a cryptographic hash function first and then sign the hash value. In schemes like the RSA (Rivest, Shamir and Adleman), the decryption algorithm is used to generate signatures and the encryption algorithm is used to verify them. This approach to digital signatures is therefore referred to as the "hash-then-decrypt" paradigms. A digital signature depends on the message.

1.7 DIGITAL CERTIFICATES

A certificate is a collection of information that binds an identity (user, computer, service or device) to the public key of a public/private key pair. The typical certificate includes information about the identity and specifies the purposes for which the certificate may be used, a serial number, and location where more information about the authority that issued the certificate may be found. The certificate is digitally signed by the issuing authority called, the certificate authority (CA). The infrastructure used to support certificates in an organization is called the Public Key Infrastructure (PKI). The certificate, in addition to being stored by the identity it belongs to, may itself be broadly available. It may be exchanged in e-mail, distributed as a part of some application's initialization, or stored in a central database of some sort from where those who need a copy can retrieve one. Each certificate's public key has its associated private key, which is kept secret,

usually only stored locally by the identity. Some implementations provide private key archiving, but often it is the security of the private key that provides the guarantee of identity.

When certificates are used for authentication, the private key is used to encrypt or digitally sign some request or challenge. The related public key available on the certificate can be used by the server or a central authentication server to decrypt the request. If the result matches what is expected, then proof of identity is obtained. These authentication step are as follows:

1. The client issues an authentication request. In this step, the client browser will load the CA digital certificate which contains the public key of the client.
2. A challenge is issued by the server. In this step the server extract the digital certificate of the client and obtain the public key of the client.
3. The workstation uses its private key to encrypt the challenge.
4. The response is returned to the server.
5. The server uses the public key to decrypt the response.
6. The result is compared to the challenge. In this step the verification is done for the correctness.
7. If there is a match, the client is authenticated

The original sets of keys are generated by the client, and only the pubic key is sent to the CA. The CA generates the certificate and signs it using its private key, and then returns a copy of the certificate to the user and to its database. It is the digital signing of the certificate that enables other systems to evaluate the certificate for its authenticity. If they can obtain a

copy of the CA's certificate, they can verify the signature on the client certificate and thus be assured that the certificate is valid.

1.8 ELLIPTIC CURVES

Elliptic curves as algebraic/geometric entities have been studied extensively for the past 150 years, and these studies contributed a rich and deep theory. Elliptic curve systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz from the University of Washington, and Victor Miller, who was then at IBM, Yorktown Heights.

Many cryptosystems often require the use of algebraic groups. Elliptic curves may be used to form elliptic curve groups. A group is a set of elements with custom-defined arithmetic operations on those elements satisfying some conditions. For elliptic curve groups, these specific operations are defined geometrically. Introducing more stringent properties to the elements of a group, such as limiting the number of points on such a curve, creates an underlying field for an elliptic curve group. Elliptic curves are first examined over real numbers in order to illustrate the geometrical properties of elliptic curve groups. Thereafter, elliptic curve groups are examined with the underlying fields of F_p (*where p is a prime*) and F_{2^m} (*a binary representation with* 2^m *elements*).

1.8.1 Elliptic Curve Groups over Real Numbers

An elliptic curve over real numbers may be defined as the set of points (x, y) which satisfy an elliptic curve equation of the form $y^2 = x^3 + ax + b$, where x, y, a and b are real numbers. Each choice of the numbers a and b yields a different elliptic curve. For example, $a = -4, b = 0.67$ gives the elliptic curve with equation $y^2 = x^3 - 4x + 0.67$; the

graph of this curve is shown in Figure 1.1. If $x^3 + ax + b$ contains no repeated factors, or equivalently if $4a^3 + 27b^2 \neq 0$, then the elliptic curve $y^2 = x^3 + ax + b$ can be used to form a group. An elliptic curve group over real numbers consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity.

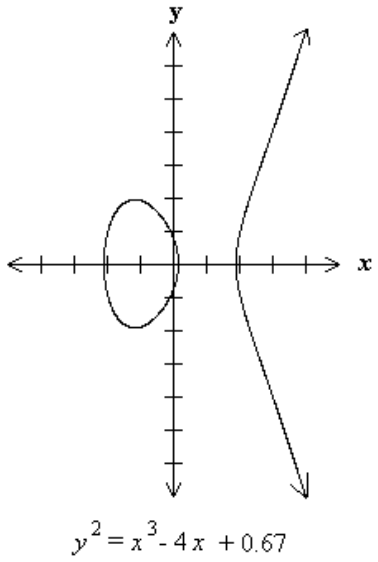

Figure 1.1 Graph of the elliptic curve $y^2 = x^3 - 4x + 0.67$

1.8.2 Elliptic Curve Addition

Elliptic curve groups are additive groups; that is, their basic operation is addition. The addition of two points in an elliptic curve is defined geometrically. The negative of a point $P = (x, y)$ is its reflection on the x-axis that is $-P = (x, -y)$. For each point $P = (x, y)$ on an elliptic curve, the point $-P = (x, -y)$ is also on the curve under modular arithmetic.

1.8.2.1 Adding two distinct points

Suppose that P and Q are two distinct points on an elliptic curve, and P is not $-Q$. To add the points P and Q, a line is drawn through the two points. This line will intersect the elliptic curve at another point $-R$. The reflection of the point $-R$ on the x-axis is the point R. The law for addition in an elliptic curve group is $P + Q = R$ which is illustrated in Figure 1.2.

The algebraic formula for the sum of two distinct points $P(x_1, y_1)$ and $Q(x_2, y_2)$ over F_p, $p > 3$ is $R = (x_3, y_3)$ where $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ and $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.

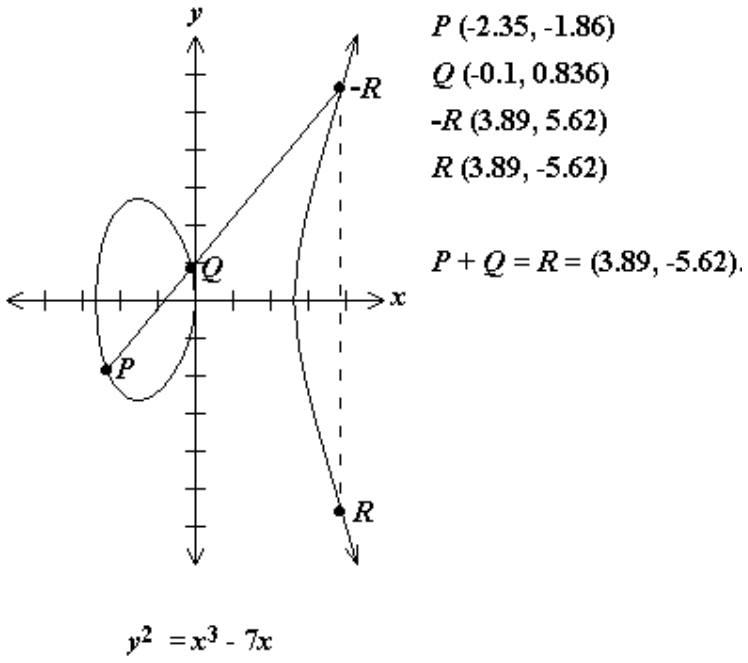

Figure 1.2 Elliptic curve point addition

1.8.2.2 Adding the point P and -P

The line through P and $-P$ is a vertical line which does not intersect the elliptic curve at a third point; thus the points P and $-P$ cannot be added as previously. It is for this reason that the elliptic curve group includes the point at infinity O, and $P+(-P)=O$. As a result of this equation, $P+O=P$ in the elliptic curve group. O is called the additive identity of the elliptic curve group; all elliptic curves have an additive identity. Figure 1.3 shows the addition of the points P and –P.

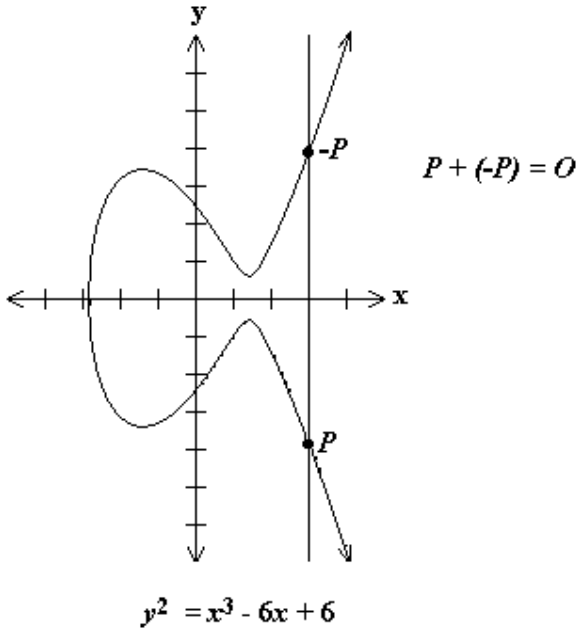

Figure 1.3 Adding P and –P

1.8.2.3 Doubling the point P

To add a point $P(x, y)$ to it, a tangent line to the curve is drawn at the point P. If $y \neq 0$, then the tangent line intersects the elliptic curve at

exactly one other point, $-R$. $-R$ is reflected on the x-axis to get R. The law for doubling a point on an elliptic curve group is defined by $P+P=2P=R$. This is shown in Figure 1.4. The algebraic formula for doubling the point $P(x_1, y_1)$ where $P \neq -P$ then $2P=(x_3, y_3)$ where $x_3=\left(\frac{3x_1^{\,2}+a}{2y_1}\right)^2-2x_1$ and $y_3=\left(\frac{3x_1^{\,2}+a}{2y_1}\right)(x_1-x_3)-y_1$

If the point $P(x, y)$ is such that $y=0$ then the tangent line to the elliptic curve at P is vertical and does not intersect the elliptic curve at any other point. By definition, $2P=O$ for such a point P. To find 3P add $2P+P$. This becomes $P+O=P$. This is shown in Figure 1.5.

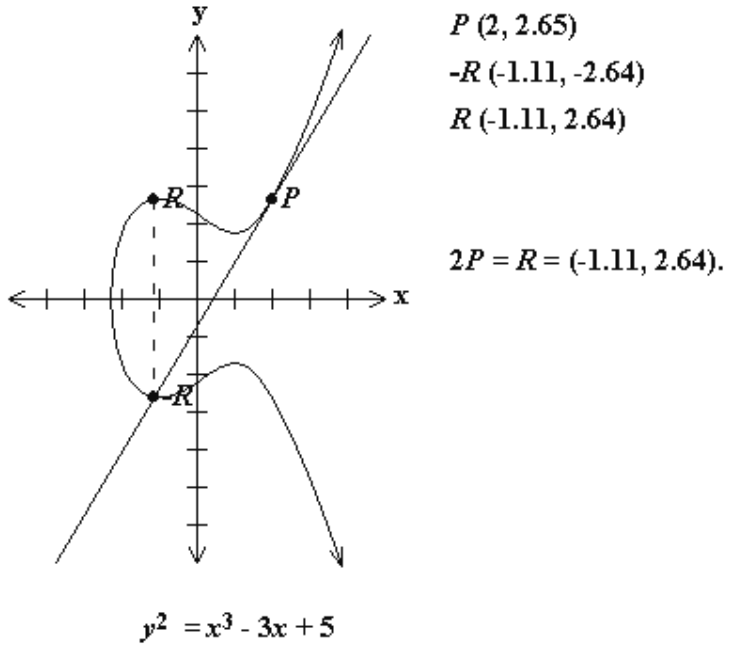

Figure 1.4 Doubling the point P

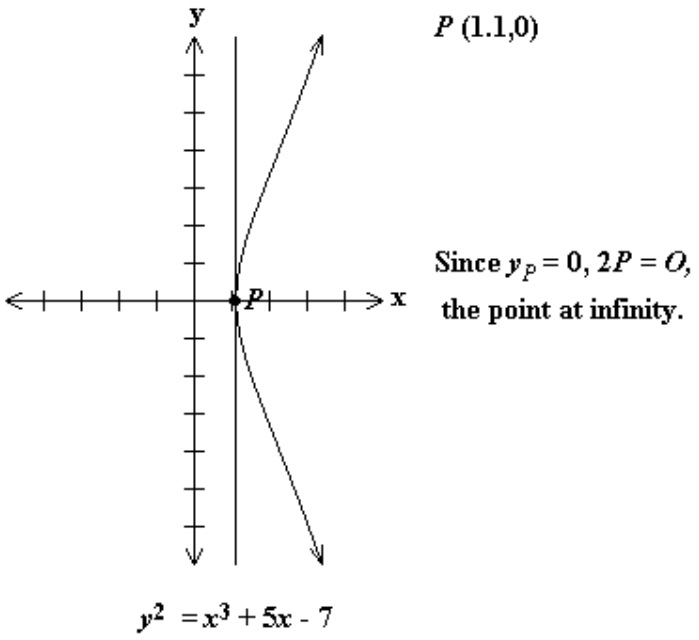

Figure 1.5 Doubling the point P with 2P=O

1.9 MATHEMATICALLY HARD PROBLEMS

In practice there are three approaches for evaluating the security of a cryptosystem, they are (i) computational security, (ii) provable security and (iii) unconditional security. In this section some of the mathematically hard problems used for the digital signature scheme have been discussed. It is assumed that the following problems are intractable.

1.9.1 Discrete Logarithm Problem (DLP)

The discrete logarithm is the inverse of discrete exponentiation in a finite cyclic group. Given a cyclic group G with group multiplication $\times$ and a generator g of order n, exponentiation in G is defined by

$$g^x = \overbrace{g \times g \times \ldots \times g}^{x-times} (\mathrm{mod}\, n)$$

Suppose $y = g^x$, then the discrete logarithm of y is x and is written as

$$\log_g y = x(\mathrm{mod}\, n)$$

The discrete logarithm problem is, given two group elements $g, y \in G$ and n (order of the generator g), find an integer x such that $y = g^x (\mathrm{mod}\, n)$. Discrete exponentiation within a group can be performed quickly by doing only $O(\log x)$ group operations. However discrete logarithms appear to be much harder to compute. All methods for computing discrete logarithms designed to work in all cyclic groups require a long time. The best known algorithm for computing the discrete logarithms is by means of index calculus method. Predicted size of problems that can be solved using the index calculus method is given the Table 1.1.

Table 1.1 Predicted sizes of problems that can be solved using the index calculus method

Time Available	Problem Size	
	In Bits	In Digits
1 hour	117	35
1 day	154	46
1 week	179	53
1 month	198	59
1 year	234	70

1.9.2 Elliptic Curve Discrete Logarithm Problem

Let E be the elliptic curve defined over a finite field F_p. Let $G =< P >$ be a cyclic subgroup of E where $P \in E$. Let $Q \in G$. ECDLP is the problem of finding an integer n such that $Q = nP$, whenever such an integer exists.

1.9.3 Decision Diffie-Hellman Problem

The Decision Diffie-Hellman assumption (DDH) is a gold mine. It enables one to construct efficient cryptographic systems with strong security properties. The DDHP is that for $a, b \in Z_q^*$, given P, aP, bP, cP, decide whether $c \equiv ab \bmod q$.

1.9.4 Computational Diffie-Hellman Problem

For $a, b \in Z_q^*$, given P, aP, bP, compute abP.

1.9.5 Gap Diffie-Hellman Problem

A class of problems where DDHP is easy while CDHP is hard on a group E. This group E is called Gap Diffie-Hellman group.

These mathematically hard problems play a vital role in providing provable security in cryptography.

1.10 LITERATURE SURVEY

Hellman (1979) gave the foundation to the mathematics of public key cryptography. Then various digital signature schemes were introduced. Goldwasser et al (1983) presented the strong signature scheme. Itakura and Nakamura (1983) introduced a public key cryptosystem, suitable

for digital multisignatures. Goldwasser et al (1985) introduced the concept of paradoxical signature scheme. Harn and Kiesler (1989) introduced the new scheme for digital multi-signature scheme. Frankal and Desmedt (1992) introduced the parallel reliable threshold multi-signature. Hard Jono and Zheng (1992) presented the practical digital multi-signature scheme based on discrete logarithm. Harn and Yang (1992) introduced the concept of group oriented undeniable signature scheme without the assistance of a mutually trusted party. Goldwasser et al (1998) presented a digital signature which is secure against adaptive chosen message attacks. Hwang and Chen (2001) introduced the new proxy multi-signature signature scheme.

Harn (1993) introduced the (t,n) threshold signature and digital multi-signature. Hwang et al (1993) gave the remarks on the threshold RSA signature scheme. Harn (1994) presented the group oriented (t, n) threshold signature scheme and digital multi-signature. Hwang et al (1995) introduced the (t, n) threshold signature scheme based on discrete logarithm. Lim and Lee (1996) presented the directed signature scheme and its applications to threshold cryptosystems. Lanford (1995) made a differential linear cryptanalysis on the threshold signatures. Langford (1996), pointed the weaknesses in some threshold cryptosystems.

Gennaro et al (1996) presented the generation of robust threshold signature scheme. Mambo et al (1996) introduced the concept of proxy signatures for delegating signing operation. Zhang (1997) introduced the concept of threshold proxy signature schemes. Guillou and Quisquater (1988) gave a paradoxical identity based on signature scheme resulting from zero knowledge. Guillou and Quisquater (1988) presented a practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory.

Hwang et al (2000) presented a secure nonrepudiable threshold signature scheme with known signers. Kim and Kim (2001) presented an efficient and provably secure threshold blind signature scheme. Jac and Jung (2002) introduced an identity based signature from gap Diffie Hellman groups. Ivan Damgård and Mads Jurik (2003) gave a length-flexible threshold cryptosystem with applications. Giuseppe Ateniese and Cristina Nita-Rotaru (2002) gave the stateless-recipient of certified e-mail system based on verifiable encryption. Zhang and Kim (2003) gave an efficient ID-based blind signature and proxy signature from pairings.

Lal and Awasthi (2003) presented a new way for proxy blind signature scheme. Ji-Hye Park et al (2007) introduced the proxy blind signature scheme with proxy revocation. Lal and Awasthi (2003) introduced a scheme for obtaining warrant message from the digital proxy signature scheme. Jan Camenish and Victor Shoup (2003) presented a practical verifiable encryption and decryption of discrete logarithms. Ming Yang and Yumin Wang (2008) gave a new efficient ID-based proxy blind signature scheme.

Chaum (1982) introduced the concept of blind signature scheme. Using the blind scheme a user A can obtain the signature of any given message, without revealing any information about the message. His further works (Chaum 1989, 1991, 1995) devoted to the significant development of the digital signature schemes. Mambo et al (1996) introduced the concept of proxy signature scheme. In a proxy signature scheme, a potential signer delegates his signing capability to a proxy entity, who signs a message on behalf of the original signer. Yi and Xiao (2001) introduced the concept of proxy blind signature scheme. Further extension was done by Tan et al (2002) using DLP and Elliptic Curve Discrete Log Problem (ECDLP). This scheme is useful in several applications such as e-voting, e-payment and mobile agent

environments. In a proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer.

Stinson and Stroble (2001) propose a distributed version of Schnorr's signature scheme, which is as secure as the non-distributed one. Pointcheval and Stern (2002) proved that this distributed signature scheme is unforgeable. Shamir (1984) proposed ID-based encryption and signature scheme to simplify key management procedures in certificate-based public key setting. Since then many ID-based encryption and signature schemes have been proposed. The main idea of ID-based cryptosystems is that the identity information of each user works as his/her public key. Bellare and Michali (1998), Chaum et al (2000) proposed the construction of digital signatures using trapdoor function.

Bilinear pairings, namely the Weil pairing and the Tate pairing of algebraic curves, are important tools for study on algebraic geometry. Their usage in cryptography is due to Victor Miller's (1986) unpublished paper and in particular the results of Menezes-Okamoto-Vanstone (1993) and Frey-Ruck (1994). However, most of the initial applications were to attack elliptic curve cryptosystems by transforming the ECDLP to DLP using bilinear pairings in the multiplicative group of a finite field. In the recent years, the bilinear pairings have been found various applications in cryptography. They are the basic tools for construction of ID-based cryptographic schemes, many ID-based cryptographic schemes have been proposed using them. They are Boneh and Franklin's (2001) ID-based encryption scheme, Smart's (2002) ID-based authentication key agreement protocol and several ID-based signature schemes like Cha and Cheon (2003), Hess (2002), Paterson (2002), Sakai et al (2000), Zhang and Kim (2002) etc.

Fiat and Shamir (1986) gave the practical solution to identification and signature problem. Frankal and Desmedt (1992) proposed parallel reliable

threshold multi-signature scheme. Gennaro et al (1996) introduced the robust threshold signature. Gnanaguruparan and Kak (2002) studied the recursive hiding of the secrets in the visual cryptography. Goldrich (1986) gave a remarks concerning the digital signature scheme. Goldwasser et al (1983) proposed the concept of strong signature scheme. Goldwasser et al (1985) introduced paradoxical signature scheme. Goldwasser et al (1998) proved that his digital signature is secured against the adaptive chosen message attacks. Guillou and Quisquater (1988) introduced a paradoxical identity based on signature scheme resulting from zero knowledge. Guillou and Quisquater (1988) gave the application to practical zero-knowledge protocol. It can be fitted to security microprocessors minimizing both transmission and memory.

Giuseppe Ateniese and Cristina Nita-Rotaru (2002), proposed stateless-recipient certified e-mail system based on Verifiable Encryption. Hard Jono and Zheng (1992) gave a practical digital multi-signature scheme based on discrete logarithm. Harn and Kiesler (1989) introduced a new scheme for digital multi-signature. Harn and Yang (1992), proposed the group oriented undeniable signature scheme without the assistance of a mutually trusted party.

Harn (1993) gave a new approach to (t, n) threshold signature and digital multi-signature. Harn (1994), proposed Group oriented (t, n) threshold signature scheme and digital multi-signature. Hwang et al (2000) gave a secure nonrepudiable threshold signature scheme with known signers. Hwang and Chen (2001), proposed a new proxy multi-signature signature scheme. Hwang et al (1995), introduced (t, n) Threshold signature scheme based on discrete logarithm.

Giuseppe Ateniese (2004) presented the Verifiable Encryption of RSA signature scheme, Cramer-Shoup signature scheme and Schnorr signature scheme which is used for the certified electronic mail protocols.

There have been several approaches to solve the fair exchange problem which are based on different definitions of fairness. Fairness is interpreted as *equal computational effort* by Even et al (1985). In this paper, it is assumed that two parties, Alice and Bob, have equal computational power and they exchange their items bit-by-bit by taking turn. This approach does not require the intervention of a trusted third party but it involves many rounds of interactions. A probabilistic approach is adopted by Ben-Or et al (1990), in this paper, the probability of successfully completing the protocol is gradually increased after every round of interaction. Asokan et al (2000) introduced the *optimistic* approach. It relies on the existence of a trusted third party which is invoked only in case of an exception. As long as the two parties follow the exchange protocol, there is no need for the trusted party's intervention, but if one deviates from the protocol then the trusted party can easily restore fairness. This approach results in particularly efficient fair exchange protocols for generic items. Asokan et al (1998) and Bao et al (1998) have built fair exchange protocols by means of *verifiable encryption* of digital signatures. Camenisch and Damgard (2000) generalized the schemes given by Asokan et al (1998) to achieve more efficient schemes that can be proved secure without relying on random oracles.

Proprietary certificates were introduced by Jakobsson et al (2002) to discourage sharing of access rights to subscription-based resources. A proprietary certificate is a certificate that contains some information related to another certificate called collateral certificate. In Boldyreva and Jakobsson (2002) an additional property called theft protection was given as a solution. The core of their solution is based on the concept of time delay (T) for deriving the secret key so that the proprietor can do the necessary steps to change the secret key during this stipulated time T.

1.11 OBJECTIVES OF THE WORK

The main objective of this research is to develop digital signature schemes and cryptographic protocols based on various mathematical hard problems to obtain efficient and robust signature generation and to solve the fairness problems which occur in the internet. These signature schemes and cryptographic protocols can be used to provide intrinsic authentication applications like Electronic Voting, Health Care Insurance Claims, Contract Signing and Proprietary certificates. All the digital signature models and cryptographic protocols are implemented using Java programming language and performance evaluation had been made.

In this thesis, two new type of digital signature schemes and two cryptographic protocol schemes were presented for providing intrinsic authentication applications like electronic voting, health care insurance claim module, contract signing and theft protected proprietary certificates. The digital signature schemes are:

- Proxy Blind Distributed Signature Scheme which is based on Discrete Log Problem (DLP)
- Identity Based Proxy Blind Distributed Signature Scheme based on Bilinear Pairing.

Signatures alone will not solve some specific problems like contract problem, certified electronic mail, etc. instead; the right approach is to use cryptographic tools to build protocols. That is explicitly specified processes are required for solving such problems. This thesis proposed two cryptographic protocol schemes. They are:

- Verifiable Encryption of Elliptic Curve Digital Signature Algorithm. This protocol is an adjudicated protocol, that is,

the Trusted Third Party (TTP) takes part in the protocol only when there is a dispute.

- Verifiable encryption scheme based on Elliptic Curve Discrete Log Problem. This protocol does not require the intervention of the third party.

The proposed digital signature schemes are theoretically developed and numerically justified. Main objectives of this research are, to develop the theoretical framework for various digital signature schemes, to implement the digital signature schemes in real time intrinsic authentication applications and to analyze the performance measures with numerical illustration.

1.12 THESIS ORGANIZATION

The chapters of this thesis are organized as follows:

Chapter 2 addresses a new type of digital signature scheme named as Proxy Blind Distributed Signature Scheme which is based on Discrete Log Problem (DLP). The need for Proxy Blind Distributed Digital Scheme arises by considering the factor that whenever a person delegating his signing authority to the intended person, there is no guarantee that the proxy signer will be in the position to do the work (signing process). The proxy signing system may be engaged with some other work or the system may be corrupted due to some malicious programs at that time. In this case if the system is modeled with proxy signature scheme then the original signer cannot achieve his goal. Hence the signing delegation is distributed into a group of persons with a threshold version. This technique will overcome the problem of unavailability of the system in a proxy signature scheme. Furthermore, this distributed concept will increase the robustness of the signature scheme.

Chapter 3 discusses a new type of digital signature scheme named as Identity Based Proxy Blind Distributed Signature Scheme. The identity of a person plays a vital role in the verification process of a signed electronic document or message. In many real time applications like Automated Health Insurance Policies, the claims for the insurance holder need the identity of the person when the digitally signed bill was verified. Secondly by distributing the signing power to the group of servers will make the signing process more trusted while compared to delegation of signing power to a single person. For example a dishonest hospital may issue a forged claim bill to the client who has not undergone any treatment. In this chapter the signing delegation is distributed into a group of persons with a threshold version and Identity based signature scheme is employed.

Chapter 4 addresses the Verifiable Encryption of Elliptic Curve Digital Signature. The protocol presented is an Adjudicated protocol, that is, the Trusted Third Party (TTP) takes part in the protocol only when there is a dispute. This scheme provides the solution to the *Fair Exchange Problem* that occurs in the Internet. This scheme can be used to build efficient fair exchanges and certified e-mail protocols.

Chapter 5 concerns with the digital certificate based authentication scheme. A new simple scheme for theft-protected proprietary certificate problem is presented by introducing a mobile phone as an additional requirement for the proprietor. Also this chapter presents the proprietary certification process using Elliptic Curve Discrete Log Problem (ECDLP) instead of Discrete Log Problem (DLP) for defining the relation R. Implementation results shows that by introducing ECDLP the certification process is more efficient than DLP.

Chapter 6 concerns about the application of the proposed digital signature scheme in a polling station based automated electronic voting

scheme and Health Care Insurance service management system for the secured and robust signature generation for the customer health insurance claim module.

Chapter 7 concludes the thesis by presenting an overview of all the proposed digital signatures and their scope for future enhancements.