Cryptography: Algorithms and Security Applications

Alfredo Cruz, Ph.D.
Associate Professor
Department of Electrical Engineering
Polytechnic University of Puerto Rico
across@coqui.net

Maxime Fernández (mfernandez@hispaniapr.com), Gloria Díaz (gloriat@coqui.net), Alberto Cosme (acosme@omppr.jnj.com), Irtalis Negrón (talo_11@hotmail.com) and Priscilla Negrón (pris@coqui.net)
Polytechnic University of Puerto Rico
Hato Rey, PR

ABSTRACT

Cryptography in Computer Science and Information Systems are broad. It is based in a sequence of steps, and its premise is only one: security. One of the latest developments in cryptography is Steganography, which is the art of transmitting information in such a way that the very existence of the message is unknown. The purpose of steganography is to elude drawing suspicion to the transmission of a hidden message. If suspicion is developed, then the goal is overcome. Steganalysis is the art of assembling and rendering useless such concealed messages. This paper will give an overview of Cryptography. We will focus on the algorithms mostly used and the different techniques available for encryption. We will also explain the Digital Signature, Digital I.D process, Certification Authentication, X.509 Certificate Format, Certificate distribution, Digital Time-Stamping (DTS), and finally discuss the attacks and security features obtained through the Cryptography.

SINOPSIS

La criptografía es un concepto amplio en las ciencias computacionales y en los sistemas de información. Está basada en una secuencia de pasos y su premisa es la seguridad. Uno de los últimos desarrollos dentro de la criptografía es la steganografía, la cual es el arte de transmitir información de tal modo que la sola existencia del mensaje es desconocida. El propósito de la steganografía es el de eludir la atracción de sospechas en la transmisión de un mensaje oculto. Si se desarrolla alguna sospecha sobre dicho mensaje, entonces este objetivo no ha sido logrado. Steganálisis es el arte de ensamblar y convertir en inservible este tipo de mensajes ocultos. Este artículo dará una ojeada a la criptografía. Se enfocará en los algoritmos más usados y en las diferentes técnicas de codificación disponibles. También se explicarán los conceptos de firma digital, proceso digital de identificación, autenticación de certificados, formato de certificado X.509, distribución de certificados, estampado digital de tiempo (DTS) y finalmente se discutirán los ataques y las características de seguridad obtenidas a través de la criptografía.

I- INTRODUCTION

What is Cryptography? A formal definition describe Cryptography as the art of creating and using methods of disguising messages, using codes, ciphers, and other methods, so that only certain people can see the real message [1].

Cryptography is one of the oldest fields known to man. It dates back to 2,000 years BC when the Egyptians used it to tell the history of their kings. The jeroglyphics on the tombs narrated the greatest acts and life of the kings. Julius Caesar used it to send messages to his troops because he did not trust his messengers [2].

Throughout the years many developments have transformed this field, specially the invention of the telegraph and radio. These inventions accelerated the development of cryptography because the information or messages were not delivered in person and was no physical security of the message [2].

The fast growing pace of the e-commerce has influenced the development of new techniques and has blossomed the interest of more people in this field. Until recently, the government was the one which had the most cryptographic capabilities. They used it to protect the confidentiality of military and diplomatic information.

With the emerging of the electronic commerce as an integral component of the global economy, the use of cryptography has increased dramatically. The

government has been studying the impact this could have because it sees that the availability of strong cryptographic systems could be a threat to national security and to the ability to control crime. They are evaluating the possibility of controlling the use and export of cryptography software.

Stenography, another form of cryptography, encompasses methods of carrying across secret messages through safe cover carriers in such a way that the very existence of the embedded messages is undetectable. Creative methods have been devise in the concealing process to reduce the visible detection of the embedded messages.

Having defined the Cryptography, it is now pertinent to define some of the parameters is it composed of. *Plaintext* is any text. When plaintext is coded, it is converted into *ciphertex*t. The process by which plaintext is converted into ciphertext, is called *Encryption*. On the other hand, the process of converting ciphertext into plaintext is known as a *Decryption*.

A- *New Developments*

As mentioned above, this new interest on cryptography has brought new developments. On January 1999, an Irish girl named Sarah Flannery (16 years old) developed a much faster algorithm [3]. She used 2 x 2 matrices multiplication to speed up the encryption of data, which is 22 times faster than the battle tested RSA encryption algorithm. This poses enormous benefits to the electronic commerce development. Although it is a great advance, scientist says that this new algorithm will have to be tested thoroughly before it could be put in practice [4].

Cryptography allows people to keep their electronic records in a form that is easily accessible to you but inaccessible to snoops, whether siblings or government.

Part of the art of cryptography consists of choosing an appropriate level of security. The strength of a cryptography system is usually measured by the amount of effort that would be required to crack it by an enemy who knows the algorithm.

There are three ways for a third person (outsider) to crack a cipher where the algorithm is known but the key is not. First, an enemy can simply steal the key or suborn a keyholder. Second, if the enemy knows the algorithm but does not have the key, he/she can try to analyze the cipher, hoping to find a weakness in the algorithm. Third, the attacker(s) can mount a "brute-force" attack using computers with large numbers of chips running in parallel, to try to decrypt the message. Exactly how long an encrypted message would be vulnerable to an economical brute-force attack is a matter of debate. Advances in computer power continue to make longer and longer keys vulnerable.

II- *TYPES OF CRYPTOGRAPHY*

Surely, computer crime is going to continue. The purpose of computer security must be to institute controls that preserve and protect confidentiality, integrity, and availability of information and systems. The most powerful tool in providing this security is *encryption*. Transforming data so that it become unintelligible to the outsider can virtually nullify the interception, modification, or fabrication of sensible information. Even though encryption is a very important tool in computer security, we should overrate its importance. If encryption is not used properly, it could make security problems worse. Weak encryption can give the users an unwanted sense of security that enemies could exploit and gain access to unwanted data or information.

All cryptosystems are based on three basic types of algorithms: secret key (symmetric), public key (asymmetric) and message digest [5].

Secret key cryptography uses the same key or password for encryption and decryption (Figure 1). This means that the encryption and decryption formulas are the same. For this reason, secret key cryptography is also called symmetric cryptography or conventional cryptography. The classic example used to explain this type of cryptography is the message sent between Alice and Bob. Alice uses a secret key to encrypt her message to Bob, using any algorithm. Bob needs to know this key to be able to

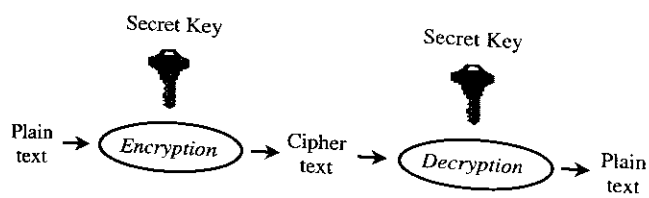

Figure 1: *Secret key Cryptography*

decrypt the message. It is very important for them to agree on the secret key and to keep it as a secret to maintain the message secure. To share this secret key, public key cryptography is used.

Symmetric algorithms can be divided into two types: stream ciphers and block ciphers. A block cipher processes the input, one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output, one element at a time, as it goes along.

Several algorithms use secret key cryptography. DES (Data Encryption Standard) is the most common [6]. It was developed in 1970's and is the standard in the US government. It is also used widely in the financial industry. DES is a block cipher with 64-bit block size and 56-bit keys. This algorithm is still strong but new versions, like 3DES, have been developed to make it more secure.

IDEA (International Data Encryption Algorithm) is an algorithm which uses a 128 bit key and is considered very secure. RC4 is a very fast cipher. It accepts keys of variable length. SAFER provides secure encryption with fast software implementation.

Public key cryptography permits the encryption key to be public, but the recipient is the only one that can decrypt the message by using a private key. Because two different keys are used, public key cryptography is also known as asymmetric key (Figure 2). The public key and the private key are mathematically related but it is infeasible to derive the private key from the public key. Using Alice and Bob example, Alice uses Bob's public key to encrypt her message. Bob uses his private key to decrypt the ciphertext and recover the original message. Any eavesdropper can intercept the ciphertext message but cannot decrypt it because he will not have Bob's private key.

Public key algorithms are about 100 to 1000 times slower than secret key algorithms. They are rarely used to encrypt large amounts of data.

RSA is the most popular public key algorithm. It was created by Rivest, Shamir and Adleman. RSA is used for confidentiality, digital signatures and key exchange. The key length is variable, between 512 and 2048 bits. The security of this algorithm relies on the difficulty of factoring large integers.

The message digest algorithm does not use any key. It takes a variable-length message as input and produces a fixed-length digest as output. This output is called the message digest, digest or hash. This algorithm is also referred as one way hash algorithm or hash algorithm. This method needs three properties to be cryptographically secure. It must not be feasible to determine the input message based on its digest. It must not be possible to find an arbitrary message that has a particular, desired digest. Also, it should be infeasible to find two messages with the same digest.

III- CONVENTIONAL ENCRYPTION: CLASSICAL TECHNIQUES

The art of encryption includes several methods to transform or change a message from plaintext to ciphertext. All the existing methods can be classified in one way or another within substitution techniques and transposition techniques.

A- SUBSTITUTION TECHNIQUE

In this method, the letters of the plaintext are substituted by other letters, numbers or symbols to create the ciphertext. This is basically the principle of cryptography in where the goal is to decode a message by substituting letters by symbols. Examples of substitution techniques are the *Caesar Cipher* and the *Vigenere Cipher*. The following paragraphs briefly discuss these methods.

The Caesar Cipher is one of the simplest monoalphabetic substitution one may use, and it's also one of the easiest to break. The Caesar Cipher replaces the letter on the plaintext by the letter that is three steps below in the 26 alphabet.

$$C = (p + 3) \bmod 26$$
$$P = \text{letter number}$$

Plain:
a b c d e f g h I j k l m n o p q r s t u v w x y z

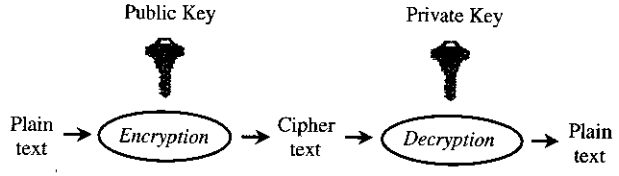

Figure 2: *Public key Cryptography*

Cipher:
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

The Vigenere Cipher is a polyalphabetic substitution. It is reasonably secure requiring more work than a simple monoalphabetic substitution. It consists of the 26 Caesar cipher, with shifts of 0 through 25 forming a 26X26 matrix. Each cipher is represented by a key letter, which is the ciphertext letter that substitutes for the plaintext letter.

Different from the Caesar Cipher method, Vigenere requires a *key* to decode the message. In other words it would be impossible to decode the cipher without a key that guides to the solution. For example:

Key: *IngenieriaIngenieriaIn*
Plaintext: *Universidad Politecnica*
Ciphertext: *CAOZRZWZLALCUPVBITVIKIN*

On this example the word "Ingenieria" serves as the decoding key for the cipher. Each letter of the cipher is matched with a letter of the key and as a coordinate system it is pointed in the Vigenere Table.

B- TRANSPOSITION TECHNIQUE

All the techniques examined so far involve the substitution of ciphertext symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.

The simplest cipher is the Rail Fence Technique, in which the plaintext is written down as matrix of four rows and for each column formed a number is assigned, then these number are rearranged to form the cipher. To decode the cipher it is written down in columns of four letters assigning the corresponding number of the key to each column. Once the matrix is formed, the columns are arranged in the correct number sequence and finally the message is displayed. The following example shows this technique:

Order:	*1*	*2*	*3*	*4*	*5*	*6*
Plaintext:	u	n	i	v	e	r
	s	i	d	a	d	p
	o	l	i	t	e	c
	n	i	c	a	x	y
Key	*5*	*3*	*2*	*1*	*6*	*4*

Cipher: **edexidicniliusonrpcyvata**

In some other more complex techniques the substitution method and the transposition method can be used as the same time.

C- STEGANOGRAPHY

Concealing information, where electronic media are used as such carriers, requires alterations of the media properties which may introduce some form of degradation. If utilized to images that degradation, may sometimes, be visible to the human eye [7] and tip to signatures of the steganographic methods and tools used. These signatures may actually announce the existence of the inserted message, thus frustrating the purpose of steganography, which is concealing the existence of a message.

A message is the information concealed and may be plaintext, ciphertext, images, or anything that can be inserted into a bit stream [10]. Together, the cover carrier and the inserted message originate a stego-carrier. Hiding information may require a stegokey which is additional secret information such as a password essential for embedding the information. For example, when a secret message is concealed within a cover image, the resulting product has a stego-image.

A possible formula of the process [9] may be represented as:

Cover medium + embedded message + stegokey = stego-medium

Two aspects of attacks on steganography are detection and eradication of the embedded message. Any image can be rearranged with the object of destroying some hidden information, [10] whether an inserted message exists or not.

Terminology with respect to attacks and cracking steganography schemes is similar to cryptographic terminology; however, there are some significant differences. Just as a cryptanalyst utilize cryptanalysis in an attempt to decipher or break encrypted messages, the steganalyst is one who utilize steganalysis in an attempt to discover the existence of hidden information. With cryptography, comparison is made between portions of the plaintext (possibly none) and portions of the ciphertext. In steganography, comparisons may be made between the cover-media, the stego-media, and possible portions of the message. The end result in cryptography is the ciphertext, while the end result in steganography is the stego-media. The message in steganography may or may not be encrypted. If it is encrypted, then if the message is extracted, the cryptanalysis techniques may be applied.

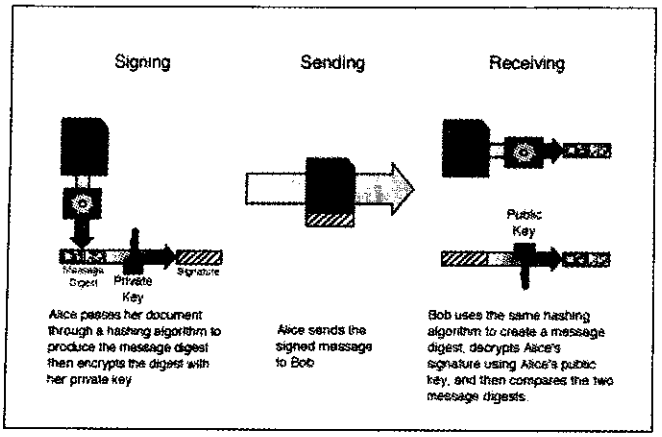

Figure 3: *Digital signature process*

The Internet is an infinite channel for the broadcast of information that includes publications and images to divulge ideas for mass communication. Images provide excellent carriers for concealed information and many different techniques [11] have been attempted. Development in the area of covert communication and steganography will continue. Research in building more robust digital watermarks [12] that can survive image manipulation and attacks continue to grow.

However, a stego-image which seems innocent enough may, upon further investigation, actually broadcast the existence of embedded information.

IV- DIGITAL SIGNATURE AND DIGITAL I.D.

A digital signature and digital I.D. are security applications that use the message digest algorithm (hash functions).

A- DIGITAL SIGNATURE

What is a digital signature? A digital signature is, as you might expect, the equivalent to a handwritten signature in a digital document. The purpose it serves is the same one as your daily hand written signature, but it is achieved in a very different way. The objective is to let someone know that the letter you sent him via any electronic way is really what you said and not a falsification. Next, we explain how this is done.

First, the document is passed through what is known as a hash function. This hash function compresses your document and gives it a value in such a way that if you change anything in the document, this value will also change. Hash functions are used in order to save time and memory space, because instead of checking the whole document (as large as it might be) people are able to check the hash output only.

The next step is to take the output of the hash function, which is known as the message digest, and encrypt it with your private key. After doing this, the next step is to send this encrypted message digest along with the entire document. This is all the sender has to do.

When the message is received, the receiver has to pass the document through the same hash function and get a message digest. The receiver also has to take the encrypted message digest and decrypt it with his or her public key. Upon decrypting the message digest, the receiver can be sure that the message was encrypted with the private key of the person she or he is dealing with. To make sure that the received document is legitimate, the receiver must go on and compare the result of their message digest with the result of the decrypted message digest. If the two hash values are the same, then it can be assumed that the person who wrote it is the same person that signed it.

The security of this procedure depends on the secrecy of the sender's private key. Anyone that has the sender's private key can impersonate him and there is no way of knowing the difference. The whole process is illustrated in Figure 3.

B- DIGITAL I.D.

When you decrypt the message digest using your public key, you can say that the message was encrypted with the corresponding private key. If you know who the owner of the private key is, then you can be sure that only him could be the sender given that his key wasn't stolen. In many cases you are dealing with a company or with someone you have never met. In these cases you have no way of knowing that the person you are dealing with is the person he or she claims to be because the public key is sent along with the message.

This is where the digital I.D comes in handy. The digital I.D is that person's public key signed trustworthy entity such as the Verisign company. Refer to Figure 4.

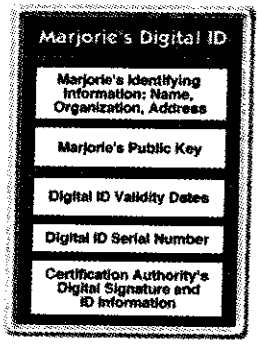

Figure 4: Digital I.D example

This way you are guaranteed by this company that the sender is who he or she claims to be. The only thing you need to know is the company's public key in order to verify the legitimacy of the I.D.

C- *Subject Authentication*

Obviously, it is critical that the CA confirms the identity of the person, device, or entity that requests a certificate. This is typically accomplished through a combination of the following, depending on the level of security required:

1- ***Personal presence***: The person may physically appear before a trusted entity.

2- ***Identification documents***: A CA can make use of ID documents such as a passport, a driver's license, or an employee badge.

D- *The X.509 Certificate*

The most widely recognized public-key certificate format is that defined in the ISO X.509 standard, as shown below. The X.509 certificate format provides for certificate extensions, including standard extensions and private or community-defined extensions. Standard extensions are defined for various purposes including key and policy information, subject and issuer attributes, and certification path constraints.

E- *Certification Distribution*

Digital certificates may be distributed online - even through unsecured networks - because the certificates are self-protecting. Typical means of distributing certificates include:

1- ***Certificate accompanying signature***: The signer has a copy of its own certificate and can attach a copy of that certificate to the digital signature. If this is done, anyone who wants to verify a signature will have the certificate in hand.

2- ***Directory service***: When using public-key technology, the message originators must first obtain the certificates of the intended recipients. When multiple parties are involved, this can be a complex task. Directories provide an easy way to search for and find certificates on the Web.

F- *Certification Revocation*

Under some circumstances, digital certificate revocation may be required (for example, an employee terminates employment with the organization).

The decision to revoke a certificate is the responsibility of the issuing company, generally in response to a request from an authorized person. For added security, the CA will generally authenticate the source of any revocation request.

G- *Control of Certification*

Digital certificates must be issued by a trusted entity known as a Certificate Authority. A CA's role is analogous to that of a Department of Motor Vehicle, which issues driver's licenses and is broadly acknowledged and accepted as a trustworthy means of personal identification. Certificate Authorities typically offer a combination of cryptography technology, an infrastructure of highly secure facilities, and a specification of practices and liability that establish its ability to operate as a trusted third party.

In today's dynamic business climate, many companies want to take advantage of the peace of mind of working with a CA, but also want to maintain strict control over the issuance and revocation of digital certificates. That is why leading CAs, such as VeriSign, now offer choices in certificate programs. Customers may contract with the CA to handle routine certificate administration tasks, or they may elect to assume responsibility for certificate issuance and revocation themselves, thereby maintaining a higher level of control.

H- *How Long It Will Remain Valid?*

Normally, a key expires after some period of time, such as one year, and a document signed with an expired key should not be accepted. However, there are many cases where it is necessary for

signed documents to be regarded as legally valid for much longer than two years; long-term leases and contracts are examples. By registering the contract with a *digital time stamping service* at the time it is signed, the signature can be validated even after the key expires.

If all parties to the contract keep a copy of the time stamp, each can prove that the contract was signed with valid keys. In fact, the time-stamp can prove the validity of a contract even if *one signer' key gets* compromised at some point after the contract was signed. Any digitally signed document can be time-stamp, assuring that the validity of the signature can be verified after the key expires.

I- DIGITAL TIME-STAMPING

A *digital time-stamping service* (DTS) issues time-stamps, which associated a date and time with a digital document in a cryptographically strong way. The digital time-stamp can be used at a later date to prove that an electronic document existed at the time stated on its time-stamp. For example, a physicist who has a brilliant idea can write about it with a word processor and have the document time-stamped. The time-stamp and document together can later prove that the scientist deserves the Nobel Prize, even though an archrival may have been the first to publish.

Following is an overview of the major regulatory initiatives on digital signatures in the United States and Europe.

I- U.S.

Congress is considering two bills to enhance the electronic commerce through the use of digital signatures. The first addresses the general use of digital signatures in commerce, while the other focuses on electronic communications in the government.

The first bill, introduced by Rep. Richard H. Baker (R-LA), would recognize electronic transmissions --including digital signatures-- as a legal alternative to current paper-based practices. The bill, which applies to both electronic signatures and digital signatures, establishes that--unless otherwise prohibited by state law--all forms of electronic authentication that meet the bill's standards would be given the same status afforded a written signature.

The bill would also establish the National Association of Certification Authorities to help define and standardize methods of electronic authentication. The association would in turn set up an Electronic Authentication's Standards Review Committee to develop criteria for electronic communications and adopt "guidelines, standards, and codes of conduct regarding the use of electronic authentication by members of the association." Any private or public entity could become a certification authority as long as it registers with the national association established under the bill.

The second bill, introduced by Rep. Anna Eshoo (D-CA), would require federal agencies to use digital signatures when communicating with one another. According to the bill, the government would issue guidelines governing the acceptance of digital signatures.

Federal agencies would also be required to establish systems allowing citizens to submit federal forms electronically.

States. In the absence of federal law, several states have enacted their own legislation clarifying the legal status of digital signatures, and others are in the process.

The first digital signature statute, the Utah Digital Signature Act, was passed in February 1995.

The law establishes a system for state licensing of certification authorities (CA). These authorities serve as trusted third parties and provide public/private key pairs to persons after verifying their identity. The CA then safeguards a copy of the certificate, which serves as a record verifying the key owner's identity. The law basically requires that digital signatures conform to technological norms.

If a company sells goods on the basis of a contractual agreement sealed with a digital signature and later learns that the digital signature was not that of the presumed purchaser, who therefore refuses to pay, the law provides recourse for the seller only against the person using the key unlawfully. The person whose key was illegally used is not liable, but the person taking the key can be criminally charged.

The Utah law states that the CAs is to be licensed by the Utah Department of Commerce. The law also details certification requirements such as procedures and duties; control of private keys; suspension, revocation, and expiration of certificates; and the obligations of the certification authority.

The subscriber's private key is protected as property, and therefore its theft or unauthorized use is subject to criminal and civil liability. The person listed in the certificate is legally responsible for the certificate and must provide proof if claiming that he or she did not sign a document that bears the certificate. The law does not explain the extent to which the certification authority is responsible for identifying the person applying for a certificate.

However, the law states that when issuing licenses for certification authorities, the Utah Department of Commerce may consider an authority's procedures.

The Utah bill was based on digital signature guidelines drafted by the American Bar Association (ABA). According to Tom Smedinghoff, an attorney with McBride, Baker, and Coles in Chicago, who helped write the document, the guidelines were meant to serve as an explanation of digital signature issues for the courts and a model for states addressing the topic.

Other digital signature acts, which all assert the legal validity of such signatures, have been passed or are pending in California, Minnesota, New Jersey, New Mexico, Oregon, Vermont, Washington and Mississippi. Some states have passed legislation with respect to the broader concepts of digital and electronic signatures. Examples include the Florida Electronic Signature Act of 1996 and the Massachusetts Electronic Records and Signatures Act. However, the terminology is not always used consistently. For instance, the definition of an electronic signature in the Georgia Electronic Records and Signatures Bill seems to refer to digital signatures.

Some states have not taken Utah's approach to certification authorities. A New Jersey law stipulates that the state perform the role of the certifying authority. This law also suggests that an office of electronic documentation be established under the Secretary of State to maintain a register of public keys.

According to Smedinghoff, such laws could serve to stifle the use of digital signatures because they stipulate different rules for conducting business in different states. Consequently, a contract might be legally binding in Utah but not in New Jersey.

As an alternative to this approach, the ABA is currently working on accreditation guidelines that could be adopted among U.S. states and around the world. Instead of forcing businesses to seek licensing as CAs in various jurisdictions, the guidelines suggest that a single international body be recognized as an accreditation authority. States or governments could then grant licenses to those entities that meet the standardized accreditation requirements.

In many states, legislation has been issued or is pending on specific uses of digital signatures, such as for government communications and tax filing. For example, California's digital signature law only applies to the use of digital signatures for communications among public entities. Similarly, Louisiana's law applies only to medical records; Nebraska's to architects and engineers; Wisconsin's to state construction contracts; and Hawaii's to court documents.

In general, limiting digital signatures to specific applications actually hinders the technology, says Smedinghoff.

2- Europe

European telecommunications ministers meeting in Luxembourg approved legislation that is expected to be key in establishing a legal framework for electronic signatures and promoting the development of electronic commerce in the European Union.

The directive approved today requires all EU countries to introduce legislation that recognizes digital signatures as the legal equivalent to hand signatures, provided they have been certified by a third party and the technology used to make them respects a series of conditions.

The directive was designed to promote consumer confidence in electronic transactions by providing them with guarantees regarding the authenticity of the data.

V- CRIPTANALYSIS AND ATTACKS ON CRYPTOSYSTEMS

Criptanalysis is the art of deciphering encrypted communications without knowing the proper keys. There are many criptoanalytic techniques or attacks. These techniques may be used by cryptanalysts to challenge the established or new cryptosystems. In the other part, adversaries may be use bribery or torture to obtain a secret key or the plaintext associated with a ciphertext message. Some of the more important attacks are described below [5].

1- Ciphertext-only attack

This situation occurs when the attacker (criptanalyst) does not know anything about the contents of the message. The criptanalyst intercepts some ciphertext and wishes to obtain the corresponding plaintext or recover key. One way to obtain the plaintext message is to launch a brute force attack in which the analyst tries each possible key of the key space until the ciphertext decrypts to some meaningful message.

2- Known-plaintext attack

The criptanalyst has access to a ciphertext message and its corresponding plaintext message. The pair of ciphertext and plaintext messages is extremely valuable; it may allow the analyst to

narrow down the key space or obtain statics that can be subsequently be used to deduced some information about another ciphertext message.

3- Chosen-plaintext attack

The analyst can select a plaintext, with a plaintext; the analyst can avoid duplicating data and may be able to target an attack toward the weaker points of an algorithm. The analyst is able to have any text he likes encrypted with the unknown key. The task is to determine the key used for encryption.

4- Man-in-the-middle-attack

This occurs when two parties are exchanging keys for secure communication but, an adversary puts himself between parties on the communication line. The parties will think that they are communicating securely, but the adversary is interfering and altering the communication. One way to prevent man-in-the-middle-attack is that both sides compute cryptographic hash function of the key exchange, sign it using digital signature algorithm, and send the signature to the other side.

There are many other cryptographic attacks but these are the most commonly used by cryptanalyts.

VI- SECURITY AND CRYPTOGRAPHY TECHNOLOGIES

Security can be defined as a mean for ensuring that the operations of a communication system is not compromised due to unauthorized tampering. There are some key elements of the security process that are described next [13, 14].

1- Authentication
Authentication deals with verifying the identity of a person – it verifies that you are who you claim you are.

2- Authorization
Authorization establishes the level of information that a person has access to, after the authentication process has been completed.

3- Confidentiality
Confidentiality ensures that the data is not revealed or disclosed to unauthorized people.

4- Integrity
Integrity of the data deals with assuring that it was not tampered during the transport. The integrity mechanism assures that the data received is exactly the same as the data transmitted from its source.

5- Reliability
Reliability assures that the data always remain available in its true form, no matter when it was transmitted or received.

6- Non-repudiation
Non-repudiation deals with assuring that any action carried out by a person cannot be denied in the future.

The different cryptographic technologies address the security requirements. Table I describes the cryptographic technologies in compliance with the different security requirements.

Table 1: Cryptographic Enabling Technologies

Security Requirement	Cryptographic Technology
Confidentiality	Encryption
Integrity	Hash function, Digital Signatures
Authentication	Digital Signature Digital Certificates
Non-repudiation	Digital Signatures

VII-CONCLUSIONS

This article describes the cryptographic technologies (cryptosystems) and applications. The cryptosystems are a collection of cryptographic algorithms, keys, plaintexts, and the associated ciphertexts. The cryptosystems are used as security means to protect the communication transactions. This article presents the enabling cryptographic technologies that address the major security requirements. To obtain a secure communication we must use a combination of cryptographic technologies to assure that all the major security requirement are included. Although cryptosystems has been increasingly and new cryptosystems has been created, our recommendation is to use a validated published cryptosystems. By this way we assure that the cryptographic algorithm had been attempted to break it without success, therefore we can assume that the algorithm is secure.

VIII-REFERENCES

[1] Froomkin, A. Michael: The Metaphor is the key: Cryptography, The ClipperChip, and the Constitution.

http://www.law.miami.edu/~froomkin/articles/clipper.htm

[2] Fred Cohen, "A Short History of Cryptography", http://all.net/books/ip/chap2-1.html

[3] "Irish Girl Hailed a Genius", http://www.zdnet.co.uk/news/1999/1/ns-6631.html, January 1999.

[4] Niall McKay, "Teen Devises New Crypto Cipher", http://wired.com/news/technology/story/1/330.html

[5] Feghhhi, Williams, Digital Certificates Applied Internet Security, p. 3 - 58, 1999

[6] "Cryptography A-Z - Cryptographic Algorithms", http://www.ssh.fi/tech/crypto/algorithms.html

[7] Kurak, C., McHugh, J: A Cautonary Note On Image Downgrading, IEEE Eight Annual Computer security Application Conference (1992) pp. 153-159.

[8] Cole, E.: Steganography. Information System Security paper, George Mason University, 1997.

[9] Johnson, N. F., Jajodia, S.: Exploring Steganography: Seen the Unseen, IEEE Computer, February 1998.

[10] Anderson, R., Peticoas, F.: On the Limits of steganography, IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, May 1998, pp. 474-481

[11] Bender, W., Gruhl, D., Morimoto, N., Lu, A.: Techniques for Data hiding, IBM Systems journal, Vol. 35, No. 3 & 4, MIT Media Lab, 1996 pp. 313-336

[12] Upham, D.: Jpeg-Jsteg, Modification of the independent JPEG Group's JPEG (software release 4) for 1-bit steganography in JFIF output files. ftp://ftp.funet.fi/pub/cryp/steganography.

[13] Basit Hussaion Ph.D., Saeed Ahmad Rajput Ph.D., "Internet and Secure Messaging", http://www.chowk.com/UniversityAve/basit_aug0797.html

[14] "Encryption for Secure Messaging," http://www.tda.ecrc.ctc.com/kbase/encryption/encrypt.htm