Overview of Cryptography

Article *in* SSRN Electronic Journal · January 2011

DOI: 10.2139/ssrn.2741776

1 author:

Anthony-Claret Onwutalobi
Lahden ammattikorkeakoulu
8 PUBLICATIONS **13** CITATIONS

Overview of Cryptography

Onwutalobi Anthony Claret, *Member, IEEE*

Abstract— **The widespread use of cryptography is a necessary consequence of the information revolution. With the coming of electronic communications on computer networks, people need a way to ensure that conversations and transactions remain confidential. Cryptography provides a solution to this problem, but it has spawned a heated policy debate. Some government agencies want to restrict the use of data encryption because they fear that criminals and spies may use the technology to their own advantage. However, Encryption Techniques so far has both advantages and disadvantages to the society and issues about abuse required a formularized policy.**

.

***Index Terms*— Cryptography, Encryption, Encoding, privacy.**

I. INTRODUCTION

In the world where information and communication is the indispensable composition of human activities, where men and technology must communicate or share information in order to make decisions; it therefore behooves that this composite essence of humans should be protected and managed to ensure its sustainability, integrity, accuracy.

Encryption techniques have become the immediate solution to protect information against third parties. These techniques required that data and information should be encrypted with some sort of mathematical algorithm where only the party that shares the information could possible decrypt to use the information. This phenomenon has long existed and is not fully reliable which pose danger to the information sharing. However, many method of encryption emerge to serve the need of the emergent trend of rapid technological advancement. These emergent techniques were more reliable and are fast in operation and performance wise.

However, as this new trend of fast and reliable cryptography emerged, there is a very big concern on that issue of using to hide proof of violent scheme as many government authorities see it as impending danger. Since Cryptography has become so powerful that messages scrambled with so-called strong cryptography are virtually undecipherable. Like many powerful technologies, this is a double-edged sword. For good, we know that Encryption can keep email and financial transactions over the Internet secure and private, but law enforcement officials worry that criminals and terrorists could use the same tools to conceal incriminating evidence and violent plots. This concern has convoked many viewpoint and argument, which has alert the formation of policies by some law enforcement agencies to regulate the encryption techniques.

In this view, we will be discussing popular encryption system, types of cryptography, issues of regulating Encryption technology, social and legal implication, computer ciphers and encryption and other cryptosystems which will aid the understanding of Encryption Techniques and its advantages and challenges in the electronic age.

II. DEFINITON AND ORIGIN OF ENCRYPTION TECHNIQUE

Encryption is process of converting messages or data into a form that cannot be read without decrypting or deciphering it. Encryption is derived from a root word —crypt—which comes from the Greek word kryptos, meaning “hidden” or “secret.”[1]

The study and practice of encryption and decryption is called the science of cryptography. Scientists who study different ways to protect and ensure the confidentiality, integrity, and authenticity of information are called cryptologists. Cryptologists also engage in cryptanalysis to find ways to break encryption methods.

For centuries before the age of electronic communication and computers, individuals, militaries, and other groups coded written information. As electronic forms of communication and information storage and processing have developed, the opportunities to intercept, modify, use, disclose, and read confidential information has grown, and the need for powerful encryption techniques has increased.

Government agencies, banks, and many corporations now routinely send a great deal of confidential information from one computer to another. Such data are usually transmitted via telephone lines or other non-private channels, such as the Internet. Continuing development of secure computer systems and networks will ensure that confidential information can be securely transferred across computer networks.

In the early 1970s, Horst Feistel, a scientist at International Business Machines Corporation (IBM Corporation), developed LUCIFER, a computerized cryptosystem that used both substitution and transposition.

In 1977, the United States National Bureau of Standards (now the National Institute of Standards and Technology [NIST]) developed a cryptographic technique called the Data Encryption Standard (DES). DES was based on LUCIFER and made use of the computer binary code (converting plaintext to bits, or binary digits of 1s and 0s). DES transformed 64-bit segments of information into 64-bit segments of ciphertext

using a key that was 56 bits in size. Each user randomly selected a key and revealed it only to those persons authorized to see the protected data. DES was broken in 1998.

In 1978 three American computer scientists, Ronald L. Rivest, Adi Shamir, and Leonard Adleman, who later founded the company RSA Data Security, created the Rivest-Shamir-Adleman (RSA) system. The RSA system uses two large prime numbers, p and q, multiplied to form a composite, n. The formula n = pq, capitalizes on the very difficult problem of factoring prime numbers.

III. Number Theory

As more and more information is transferred over computer networks, computer scientists continue to develop more secure, complex algorithms. In 1997, the NIST began coordinating development of a replacement for DES called Advanced Encryption Standard (AES). AES will use a more complex algorithm, based on a 128-bit encryption standard instead of the 64-bit standard of DES. This 128-bit algorithm will make AES impossible to decrypt with current technology.

Another encryption system based on 128-bit segments is called International Data Encryption Algorithm, or IDEA. The Swiss Federal Institute of Technology developed the IDEA standard in the 1990s. Computer scientists have also proposed alternatives such as public-key cryptosystems (PKCs), which use two types of keys, a public key and a private key. The public key encrypts data, and a corresponding private key decrypts it. The user gives the public key out to other users, and they can use the public key for encrypting messages to be sent to the user. The user keeps the private key secret and uses it to decrypt received messages. An example of a PKC is the RSA system, described above.

IV. How Encryption Works

Encryption uses a systematic or step-by-step procedure called an algorithm to convert data or the text of an original message, known as plaintext, into ciphertext, its encrypted form.[2] Cryptographic algorithms normally require a string of characters called a key to encrypt or decrypt data. Those who possess the key and the algorithm can encrypt the plaintext into ciphertext and then decrypt the ciphertext back into plaintext. [3]

Cryptologists engage in an unending competition to create stronger cryptographic techniques and to break them. Many recent cryptography techniques are nearly unbreakable even with the most powerful computers. These systems produce ciphertext that appears to be random characters. These systems resist most existing methods for deciphering back into plaintext. The many different types of new cryptosystems use highly complex mathematical language and resist breaking even though cryptologists may know the techniques used in creating them.

Pretty Good Privacy (PGP)

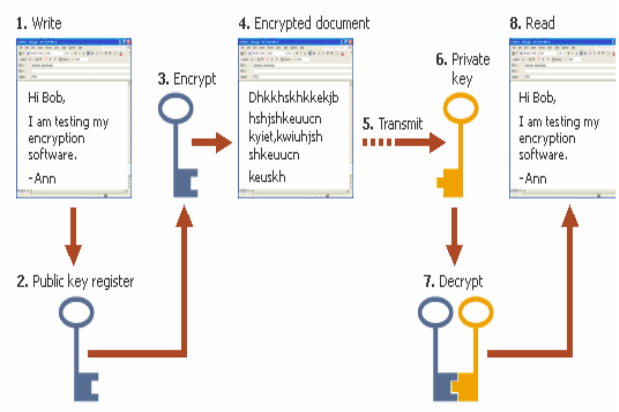

Fig. 1. Pretty Good Privacy (PGP) helps users of e-mail to keep their communications private.

Pretty Good Privacy (PGP) helps users of e-mail keep their communications private. In this two-key system, also known as the public key system, the computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. All computers authorized to receive and decrypt the message are given the matching public key. This method also establishes who sent the message. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key. Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message. The use of the keys is done

V. Popular Encryption System

Three of the most popular cryptography systems used are the Data Encryption Standard (DES), Pretty Good Privacy (PGP), and the Rivest, Shamir, Adleman (RSA) system. Most of this has been shortly described above; however, we will elaborate it below.

DES uses a single key for both encrypting and decrypting. It was developed by International Business Machines Corporation (IBM) and approved by the United States National Institute of Standards and Technology in 1976.

In private-key cryptography,. A secret key may be held by one person or exchanged between the sender and the receiver of a message. For example, if you encrypt data for storage on a hard drive, you remember the key and usually do not give it to another person. But if you want to send secure messages to a business partner using symmetric cryptography, you need to make sure your partner knows the key that will decrypt the messages The secret (or private) key in a public-key cryptographic system is never transmitted or shared. For example, when using this method for client-side authentication, the server sends some data to your client program. The client uses your private key to encrypt that data. Using your public key, the server will attempt to decrypt the

returned data, and, if successful, know that it has established communication with you. [4]

If private -key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key. However, the key may be compromised during transit. If you know the party you are exchanging messages with, you can give them the key in advance. However, if you need to send an encrypted message to someone, you have never met; you will need to figure out a way to exchange keys in a secure way. One method is to send it via another secure channel.

The Rivest, Shamir, Adleman (RSA) algorithm is a popular encryption method that uses two keys. It was developed for general use in 1977 and was named for the three computer scientists—Ronald L. Rivest, Adi Shamir, and Leonard Adleman—who originated it. The RSA Data Security Company has been highly successful in licensing its algorithm for others to use.

Unlike symmetric cryptography, the keys are mathematically related, yet it is computationally infeasible to deduce one from the other. Anyone with the public key can encrypt a message but not decrypt it. Only the person with the private key can decrypt the message. One of the most common uses of public-key technology is to provide a secure communication channel between computer programs, although private-key techniques can be used for this, too. Public key infrastructure also provides the foundation for secure emails because public key cryptography is used to distribute symmetric keys, which are then used to encrypt and decrypt actual messages. For example, in using a public-key system for personal authentication or secure messaging, you keep one key secret. The second (public) key can then be distributed to anyone.

The typical example of public key infrastructure is SSL (Secure Socket Layer) protocol. SSL is often used to protect information sent between Web browsers and web servers; this is commonly used in e-commerce systems.

PGP is an encryption system as demonstrated above it also uses two keys. It is based on the RSA algorithm. PGP was invented by software developer Philip Zimmerman and is one of the most common cryptosystems used on the Internet because it is effective, free, and simple to use. PGP is such an effective encryption tool that the United States government sued Zimmerman for releasing it to the public, alleging that making PGP available to enemies of the United States would endanger national security. [5] The lawsuit was dropped, but it is still illegal in some countries to use PGP to communicate with people in other countries.

In the two-key system, also known as the public key system, one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. All computers authorized to receive and decrypt the message are given the matching public key. This method also establishes who sent the message. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key. [6] Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message. Single key methods, in contrast, require great secrecy in conveying a key from sender to recipient

VI. OTHER CRYPTOSYSTEMS

Secure Sockets Layer (SSL), a protocol developed by Netscape Communications Corporation for transmitting private documents via the Internet, and Secure Hypertext Transfer Protocol (S-HTTP), designed to transmit individual messages, also use encryption methods.

The length or complexity of the key (along with the difficulty of the algorithm) usually indicates the effectiveness of the encryption. DES, for example, uses 56 bits in its key to change 8-character message segments into 64-bit segments of ciphertext. In 1997 the National Institute of Standards and Technology began coordinating development of a new encryption system called Advanced Encryption Standard (AES). AES is to replace DES, as it will use a stronger algorithm, based on a 128-bit encryption standard instead of the 64-bit standard that DES now uses. Another advanced encryption system employs the International Data Encryption Algorithm, or IDEA, based on 128-bit segments. The Swiss Federal Institute of Technology developed the IDEA standard in the 1990s. Banks in the United States and several countries in Europe use the IDEA standard

VII. KERBEROS

Kerberos is another secure encryption method. It was developed at MIT in the mid 1980. Kerberos is available as open source or in supported commercial software. Kerberos employs client/server architecture and provides user-to-server authentication rather than host-to-host authentication. In this model, security and authentication will be based on secret key technology where every host on the network has its own secret key. It would clearly be unmanageable if every host had to know the keys of all other hosts so a secure, trusted host somewhere on the network, known as a Key Distribution Center (KDC), knows the keys for all of the hosts (or at least some of the hosts within a portion of the network, called a realm). In this way, when a new node is brought online, only the KDC and the new node need to be configured with the node's key; keys can be distributed physically or by some other secure means.

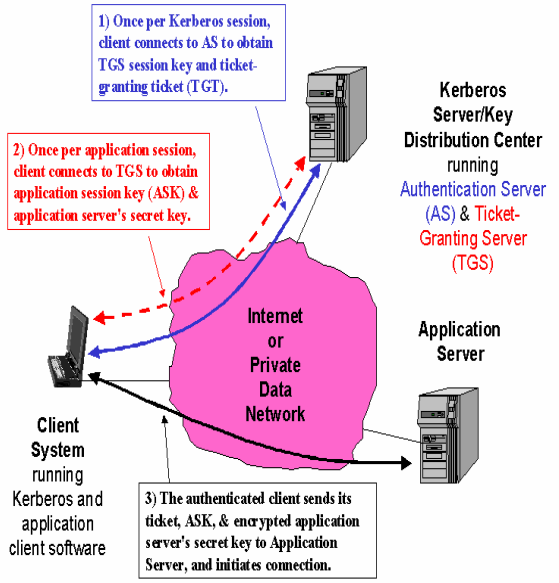

Fig. 2. The Kerberos Server/KDC has two main functions known as the Authentication Server (AS) and Ticket-Granting Server (TGS).

The Kerberos Server/KDC has two main functions known as the Authentication Server (AS) and Ticket-Granting Server (TGS). The steps in establishing an authenticated session between an application client and the application server are:
The Kerberos client software establishes a connection with the Kerberos server's AS function. The AS first authenticates that the client is who it purports to be. The AS then provides the client with a secret key for this login session (the TGS session key) and a ticket-granting ticket (TGT), which gives the client permission to talk to the TGS. The ticket has a finite lifetime so that the authentication process is repeated periodically.
The client now communicates with the TGS to obtain the Application Server's key so that it (the client) can establish a connection to the service it wants. The client supplies the TGS with the TGS session key and TGT; the TGS responds with an application session key (ASK) and an encrypted form of the Application Server's secret key; this secret key is never sent on the network in any other form.
The client has now authenticated itself and can prove its identity to the Application Server by supplying the Kerberos ticket, application session key, and encrypted Application Server secret key. The Application Server responds with similarly encrypted information to authenticate itself to the client. At this point, the client can initiate the intended service requests (e.g., Telnet, FTP, HTTP, or e-commerce transaction session establishment).[6]

A. *Weakness*

Because the KDC's store secret keys for every user and server on the network, they must be kept completely secure. If an attacker were to obtain administrative access to the KDC, he would have access to the complete resources of the Kerberos realm.

Kerberos tickets are cached on the client systems. If an attacker gains administrative access to a Kerberos client system, he can impersonate the authenticated users of that system. This will cause harm to the users of the software. Moreover, it could be disastrous if TGT is stolen, it can be used to access network Services although this problem is huge but it might cause little or no harm as the ticket can expire in few hours and the attacker will be left helpless.

VIII. TYPES OF CRYTOGRAPHY

There are many types of cryptography, including codes, Steganography (hidden or secret writing), and ciphers. Codes rely on codebooks. Steganography relies on different ways to hide or disguise writing. Ciphers include both computer-generated ciphers and those created by encryption methods. The different types of ciphers depend on alphabetical, numerical, computer-based, or other scrambling methods.

A. *Codes and Codebooks*

A well-constructed code can represent phrases and entire sentences with symbols, such as five-letter groups, and is often used more for economy than for secrecy. A properly constructed code can give a high degree of security, but the difficulty of printing and distributing codebooks—books of known codes—under conditions of absolute secrecy limits their use to places in which the books can be effectively guarded. In addition, the more a codebook is used, the less secure it becomes.
Imagine a codebook with two columns. In the first column is a list of all the words that a military commander could possibly need to use to communicate. For example, it contains all the possible geographic areas in a region, all possible times, and all military terms. In the other column is a list of plain words. To create a coded message, the encoder writes down the actual message. He then substitutes words in the codebook by finding matches in the second column for the words in the message and using the new words instead. For example, suppose the message is Attack the hill at dawn and the codebook contains the following word pairs: attack = bear, the = juice, hill = orange, at = calendar and dawn = open. The encoded message would read Bear juice orange calendar open.
If the coded message fell into enemy hands, the enemy would know it was in code, but without the codebook the enemy would have no way to decrypt the message. Codebooks lose some of their value over time, however. For example, if the coded message fell into enemy hands and the next day the hill was attacked at dawn, the enemy could link the event to the coded message. If another message containing the word orange was captured, and the following day, something else happened on the hill, the enemy could assume that orange = hill is in the codebook. Over time, the enemy could put together more and more code word pairs, and eventually crack the code. For this reason, it is common to change codes often. [7]

B. *Steganography*

Steganography is a method of hiding the existence of a

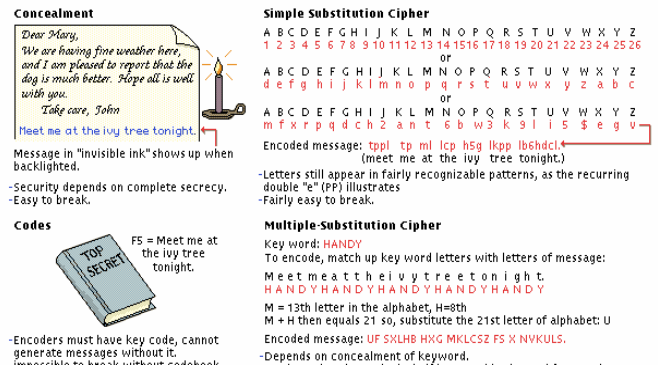

Fig. 3. Sample picture of a codebook (source of the Picture1)

message using tools such as invisible ink, microscopic writing, or hiding code words within sentences of a message (such as making every fifth word in a text part of the message). Cryptographers may apply Steganography to electronic communications. This application is called transmission security.

Steganography, or secret writing, seems to have originated almost as early as writing itself did. Even in ancient Egypt, where writing itself was a mystery to the average person, two distinct forms of writing were used. The priests used hieratic or sacred writing for secret communication, and other literate people used demotic writing. The ancient Greeks and Romans, as well as other civilizations that flourished at around the same time used forms of Steganography. The invention of the first shorthand system was presumably intended as a form of secret writing. Shorthand first came into wide use in ancient Rome, with notae Tironianae ("Tironian notes"), a system invented by Marcus Tullius Tiro in 63 bc.[8]

C. *Ciphers*

Ease of use makes ciphers popular. There are two general types of ciphers. Substitution ciphers require a cipher alphabet to replace plaintext with other letters or symbols. Transposition ciphers use the shuffling of letters in a word to make the word incomprehensible.

Ciphers are the secret codes used to encrypt plaintext messages. Ciphers of various types have been devised, but all of them are either substitution or transposition ciphers. Computer ciphers are ciphers that are used for digital messages. Computer ciphers differ from ordinary substitution and transposition ciphers in that a computer application performs the encryption of data. The term cryptography is sometimes restricted to the use of ciphers or to methods involving the substitution of other letters or symbols for the original letters of a message

D. *Substitution Ciphers*

In simple substitution ciphers, a particular letter or symbol is substituted for each letter. The letters are substituted in their normal order, usually with normal word divisions. Such ciphers are recognized by the occurrence of a set of normal letter frequencies attached to the wrong letters. They are solved by using frequency analysis and by noting the characteristics of particular letters, such as the tendency to form doubles, common word prefixes and suffixes, common first and last letters in words, and common combinations, such as qu, th, er, and re.

A substitution cipher is performed by reordering the letters in the alphabet. For example, a cipher devised long ago by Julius Caesar shifts all the letters in the alphabet by three places. Thus, when the letter a is needed, a d is used, and when a b is to be written, an e is used. The letters wrap around at the end of the alphabet. So, if a person wants to encipher a z, it is written as a c. Similarly, a y is written as a b. The entire cipher is represented by two rows of letters. These rows are called a lookup table.

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
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

When someone wants to encrypt a word, he or she looks up the original letter in the top row and uses the corresponding ciphertext letter in the bottom row. So, for example, the word HELLO would be written as KHOOR. To decrypt the coded word, a person would search for the letter in the bottom row and write down the corresponding letter in the top row. So, KHOOR decrypts back to HELLO.

While the above substitution cipher is easy to remember, it is also easy to break. To make a substitution cipher more complex, multiple substitutions and sometimes even numbers are added to the cipher.

In multiple-substitution (polyalphabetic) ciphers, a keyword or number is employed. The first message letter might be enciphered by adding to it the numerical value of the first letter of the keyword; the second message letter is enciphered similarly, using the second letter of the keyword, and so on, repeating the keyword as often as necessary to encipher the whole message. When adding the numerical value of a keyword letter to a message letter, one starts counting with the message letter. Thus, to encipher the word TODAY by the code word DIG, t becomes w, as d is the fourth letter of the alphabet (count t, u, v, w); o becomes w, as i is the ninth letter of the alphabet; and d becomes j, as g is the seventh letter of the alphabet. For the rest of the message the code word is repeated, and thus TODAY is coded WWJDG.

By using combinations of the basic types of ciphers, ciphers can be created to various degrees of complexity. The key, however, should be easy to remember or reproduce, for without it the cipher is no longer a message but a puzzle. Given sufficient time and material, most ciphers can be solved and their keys discovered, but for a particular purpose, the complexity need be only so great as to obtain the level of security desired. Military orders that must be kept secret for only a few hours, for example, can be encrypted in a cipher that would be entirely unsuited for diplomatic reports using a cipher over an extended period of time.

Transposition Cipher

In a transposition cipher, the order of plaintext letters is changed to derive the ciphertext. The message is usually written without word divisions in rows of letters arranged in a rectangular block. The letters are then transposed in a prearranged order, such as by vertical columns, diagonals, or spirals, or by more complicated systems, such as the knight's tour, which is based on the move of the knight in chess. The arrangement of the letters in the enciphered message depends upon the size of the block of code words used and upon the route followed in inscribing and transposing the letters.
A cipher in which every pair of letters is swapped is an example of a transposition cipher. In this case, for example, the ciphertext for elephant would be lepeahtn. The first and second letters are swapped, then the third and fourth letters are swapped, and so on. Transposition ciphers may be combined with substitution ciphers to produce a more complex encoded message.

Breaking Simple Ciphers

Substitution and transposition ciphers appear to be difficult to break. However, if enough messages are encrypted with any cipher, the cipher is easily broken. Repetition of a series of letters may lead code breakers to the key of any cipher system. In a substitution cipher, once a letter is associated with another letter, a pattern emerges and the cipher is easily decrypted. [10]

In order to make a cipher even more secure, a key word or number may be used. Transposition ciphers might be recognized by the letter frequencies (the number of times a common letter, such as e, is used compared to the number of times a less frequently used letter, such as q, appears) for the language used. Solution of such ciphers without the key is possible by rearranging the letters in various geometric designs and at the same time forming a new word by reordering the letters of the coded word or phrase (such as from satin to stain) until the method of encipherment is discovered.
Computers may be used to break simple ciphers. Techniques for encrypting data naturally took advantage of the power of computers. Today’s modern cryptographic techniques are based entirely on a cryptographic key that is kept secret. The plaintext that is to be encrypted is converted to bits, or binary digits of 1s and 0s (see Bit). Then complex substitutions and transpositions are performed on the plaintext, using the key as a guide. The transformation of the plaintext to ciphertext is entirely dependent on the key.

Cryptographic Authentication

Providing a way to authenticate yourself to a computer system without publicly sending your password is very essential in achieving your security goal. Passwords sent without encryption may be discoverable by others if sent through or to insecure network segments or systems.
Below are the approaches used to avoid unencrypted password problems?
Shared network segments are gradually being replaced by "switched" network segments. The newer, switched network technology greatly reduces the opportunity for "sniffing" or eavesdropping on people's conversations.
Adoption of methods for sending passwords through secure (encrypted) channels.

There is a Cryptographic authentication system, which do not rely on transmitting passwords.

Key Management

One of the big challenges in using cryptography on a widespread basis especially public-key encryption--is the management of private and public keys. Key management deals with the secure generation, distribution, and storage of keys. Secure methods of key management are extremely important. Once a key is randomly generated, it must remain secret to avoid unfortunate mishaps. Most attacks on public-key systems will probably be aimed at the key management level, rather than at the cryptographic algorithm itself.
Users must be able to securely obtain a key pair suited to their efficiency and security needs. There must be a way to look up other people's public keys and to publicize one's own public key. Users must be able to legitimately obtain others' public keys; otherwise, an intruder can either change public keys listed in a directory, or impersonate another user.
If someone's private key is lost or compromised, others must be made aware of this, so they will no longer encrypt messages under the invalid public key nor accept messages signed with the invalid private key. Users must be able to store their private keys securely, so no intruder can obtain them, yet the keys must be readily accessible for legitimate user. Keys need to be valid only until a specified expiration date but the expiration date must be chosen properly and publicized in an authenticated channel.

Certificates

A digital certificate is an attachment to an electronic message used for security purposes. It is commonly used to verify that a user is who he/she claims to be and to provide the receiver with the means to encode a reply.
When you obtain a certificate by applying to a certificate authority (CA); once the CA verifies you are who you say you are, it creates a certificate--a digital document--for you. The certificate contains:
A name that is unique to you
The length of time the certificate is valid
Your public key
Your key's purpose: to sign messages or to encrypt data

Certificates do the following for your system:
Backed up and recoverable
Protected against theft
Matched with encrypted data
Accessible from many systems
Accessible only to the authorized user

In order for you to manage your certificate to be used with applications, you will need to do the followings:
Production and maintenance of a very large standards-based directory

Support for a highly distributed computing environment
Methodologies supporting transparent access by applications
Private and public key storage and access issues
Incompatibility of browser vendors' certificate formats
Issues that Certificate Authority deals with are as follows:
Maintenance of a certificate repository
Methodology for verifying individuals and departments
Management of certificate revocation lists (CRLs)
Renewal of key pairs and certificates
Support for trust relationships with other certificate authorities
Secure messaging is the principal driver for using personal certificates. Other alternatives can be used to address security problems in online systems, including Web-based transaction systems. However, the technical, policy, and management issues mentioned previously must be resolved before any wide scale deployment of a public-key infrastructure is reasonable.

Digital Signatures

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority (CA) so that anyone can verify that the certificate is real.

How It Works

Assume you were going to send the draft of your business data to your close business partner in another place. You want to give your partner the assurance that it was unchanged from what you sent and that it is really from you.

The sender

You copy-and-paste the data into an e-mail note.
Using special software, you obtain a message hash (mathematical summary) of the data.

You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
The encrypted hash becomes your digital signature of the message which will be different each time you send a message
At the other end, your business partner receives the message

The receiver

To make sure it's intact and from you, your business partner makes a hash of the received message.
He then uses your public key to decrypt the message hash or summary.
If the hashes match, the received message is valid.

How a digital certificate looks like

-------BEGIN SIGNATURE------

IQB1AwUBMVSiA5QYCuMfgNYjAQFAKgL/
ZkBfbeNEsbthba4Blrcnjaqbc KgNv+a5kr4537y8RCd+RHm
75yYh5xxA1ojELwNhhb7cltrp2V7LlOnAelws4S87UX80cL
BtBcN6AACf11qymC2h+Rb2j5SSU+rmXWru+=QFMx
-------END SIGNATURE------

IX. PROBLEMS OF ENCRYPTION TECHNIQUES

Although, encryption mechanisms make information unreadable. Therefore, no third parties, including server administrators and others, have access to plain text version of transmitted information through public networks such as internet, but the following are the problems encountered or associated with encryption techniques.
Symmetric Encryption

In symmetric encryption also known as the Private Key Method or encryption, a single key is used for encrypting and decrypting the data. This type of encryption is quite fast, but has a severe problem. The inherent weakness of this method is mostly the requirement of a key exchange between communications partners. In other words, in order to share a secret with someone, they have to know your key. This implies a very high level of trust between people sharing secrets, if an unscrupulous person has your key or if your key is intercepted by a spy they can decrypt all the messages you send using that key. However, Asymmetric encryption solves the trust problem inherent in symmetric encryption by using two different keys: a public key for encrypting messages, and a private key for decrypting messages. This makes it possible to communicate in secrecy with people you don't fully trust. If an unscrupulous person has your public key, who cares? The public key is only good for encryption; it's useless for decryption. They can't decrypt any of your messages! However, asymmetric encryption is very slow. It's not recommended for use on more than roughly 1 kilobyte of data.
Asymmetric Methods

In Asymmetric encryption also known as the Public Key Method, it uses two different keys: the private key and public key. The public key is distributed freely and the private key is known only to the owner of a key. The two keys have a (mathematical) relationship. However, for obvious reasons, calculation of a private key on the basis of the public key must be impossible or at least not feasible.

Both keys have different functions depending on the application at hand. In the case of data encryption, data is encoded using the public key. The private key is required in order to decrypt the message. The private key can also be used to generate digital signatures which can later be verified using the public key.

The disadvantage or problem of this method compared to symmetric encryption is the greater amount of processing time required for the calculation or a process. This is why usually the so called hybrid technology which is a mix of both asymmetric and symmetric encryption is used when dealing with a greater amount of data. In this case, symmetric encryption is used to encode the data but the symmetric key is communicated on a previously determined frequency using asymmetric encryption.

X. SECURITY ISSUES AND LEGAL IMPLICATION

Data encryption is regarded by the U.S. government as a national-security issue because it can interfere with intelligence gathering—therefore, it is subject to export controls, which in turn make it difficult for U.S. companies to function competitively in the international marketplace. To resolve this dilemma, the federal government in 1993 proposed key escrow encryption, an approach, embodied in an electronic device called a "Clipper chip," that makes broadly available a purportedly unbreakable encryption technique (although the code was broken by researchers in 1995) with keys to unlock the information held in escrow for national security and law-enforcement purposes by the federal government. [12] This approach, however, has been unacceptable to civil libertarians and to the international community. In 1994, the Clipper algorithm (called Skipjack) was specified in the Escrow Encryption Standard (EES), a voluntary federal standard for encryption of voice, facsimile (fax), and data communications over ordinary telephone lines. A subsequent compromise escrow scheme intended to create a standard for data encryption that balanced the needs of national security, law enforcement, and personal freedom was rejected in 1995; a compromise proposed in 1999 was also controversial. [13]

XI. CRYPTANALYSIS

Cryptanalysis is the art of analyzing ciphertext to extract the plaintext or the key. In other words, cryptanalysis is the opposite of cryptography. It is the breaking of ciphers. Understanding the process of code breaking is very important when designing any encryption system. The science of cryptography has kept up with the technological explosion of the last half of the 20th century. Current systems require very powerful computer systems to encrypt and decrypt data. While cryptanalysis has improved as well, some systems may exist that are unbreakable by today's standards.

Today's cryptanalysis is measured by the number and speed of computers available to the code breaker. Some cryptographers believe that the National Security Agency (NSA) of the United States has enormous, extremely powerful computers that are entirely devoted to cryptanalysis. [14]

The substitution ciphers described above are easy to break. Before computers were available, expert cryptanalysts would look at ciphertext and make guesses as to which letters were substituted for which other letters. Early cryptanalysis techniques included computing the frequency with which letters occur in the language that is being intercepted. For example, in the English language, the letters e, s, t, a, m, and n occur much more frequently than do q, z, x, y, and w. So, cryptanalysts look at the ciphertext for the most frequently occurring letters and assign them as candidates to be e, s, t, a, m, and n. Cryptanalysts also know that certain combinations of letters are more common in the English language than others are. For example, q and u occur together, and so do t and h. The frequency and combinations of letters help cryptanalysts build a table of possible solution letters. The more ciphertext that is available, the better the chances of breaking the code.

In modern cryptographic systems, too, the more ciphertext that is available to the code breaker, the better. For this reason, all systems require frequent changing of the key. Once the key is changed, no more ciphertext will be produced using the former key. Ciphertext that is produced using different keys—and frequently changed keys—makes the cryptanalyst's task of code breaking difficult.

XII. RECOMMENDATION

It is apparent how important encryption can be in our daily lives. As we transfer data anyone can intercept it. Encryption can protect any sort of data from "eavesdroppers" on the internet. "We want to know that our information travels safely, without alteration and that there is neither information theft nor identity fraud." [14]

Encryption is very important when it comes to private data or information. In this technological age, where all computers on the internet are connected, it is important to encrypt private data before it is sent to another party online.

Making transactions online are also one major reason for encrypting data. When credit card information is sent online without encoding it, it can be intercepted by a malicious user. With the credit card information, the cracker or the hacker will have access to the account of the victim and use it as he/she wishes.

Other hackers might also take advantage of unencrypted data. This might bring rise to social engineering (the act of disguising oneself to be someone else).

With this, we can confidently conclude that encryption is very important aspect of data protection in today's highly technological

XIII. CONCLUSION

Encryption techniques have come to stay in the electronic world. Since every information, that passes through computer network is not protected. This method is there to protect information and to allow safe and secure communication. Although more and more advanced algorithm has emerge in the market. Some of this method has raise some concern to the law enforcement agency as they pose threat to the security and civil protection

REFERENCES

[1] http://www.washington.edu/computing/windows/issue22/encryption.html Date accessed 25/07/06
[2] R. E. Frazier, 2004, data encryption techniques, [online]: http://catalog.com/sft/encrypt.html, date accessed: 23/07/06
Gary C. Kessler, 1998, an overview of cryptography, [online]: http://www.garykessler.net/library/crypto.html, date accessed: 23/07/06
[3] Jennifer Tauser, 2005, Encryption is the most important tool for Internet security and privacy,
[4] http://www.washington.edu/computing/windows/issue22/encryption.html
[5] http://www.rsasecurity.com/rsalabs/node.asp?id=2262
[6] http://www.garykessler.net/library/crypto.html
[6]http://searchsecurity.techtarget.com/sDefinition/0sid14_gci21195300.html
[7]http://www.linktionary.com/p/priv_key_cryp.htmhttp://web.mit.edu/rhel-doc/3/rhel-rg-en-3/s1-kerberos-works.html
[8] http://www.tech-faq.com/kerberos.shtml
[9] http://www.encyclopedia.com/html/d1/dataencr.asp
[10] http://www.ficora.fi/englanti/tietoturva/asymmetrinen.htm
[11]http://www.dsg.cs.tcd.ie/~reynoldv/project_reports/ModernEncryption.htm
[12] http://www.phptr.com/articles/article.asp?p=102212&rl=1
[13]http://filebox.vt.edu/users/jtauser/debate1/importance.htm, date accessed: 23/07/06
[14] http://filebox.vt.edu/users/jtauser/debate1/importance.htm