"CRYPTOGRAPHY UNVEILED"

Aabha Sharma*

NikhitaUpreti*

Divya Bali*

NikhitaPahuja*

ABSTRACT

In today's scenario security has become a major issue in the society. It is a broad topic that covers a multitude of sins. It is concerned with making sure that nosy people cannot read, or worse yet, secretly modify messages intended for other recipients. In order to adjudicate this problem there are various methods and one of them is cryptography.Cryptography is a technique that enables users to communicate securely over an insecure channel in a way that ensures their transmissions' privacy and authenticity. Central goal for cryptographic protocols is providing privacy and authenticity, but the field has expanded to cover many other techniques, including e-voting, digital coins, and secure auctions. This paper explains what cryptography is about and the purpose of cryptography. It also talks about the type of cryptographic algorithms, trust models and cryptographic algorithms in action.

* Computer Science,MDU,Rohtak

INTRODUCTION

Practise of enciphering and deciphering of messages in secret codes in order to render them unintelligible to all but the intended receiver.Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to conceal its meaning is called encryption. Encryption is used to ensure that information is hidden from anyone. The encrypted or encoded information such that it contains a form of the original plaintext that is unreadable by a human or computer for whom it is not intended is called cipher text. The process of reverting ciphertext to its original plaintext is called decryption.

HISTORY

The word cryptography comes from the Greek words kryptos and graphein, which mean hidden and writing, respectively .

Earlier cryptography was solely concerned with transforming messages into unreadable groups of figures to hide the message's content during the time the message was being sent from one place to another. In the modern era, cryptography has grown from basic message confidentiality to include some phases of message integrity checking, sender/receiver identity authentication, and digital signatures.

The history of cryptography can be broadly divided into three phases:

(a) From ancient civilizations to the nineteenth century and the first part of the twentieth century, with relatively simple algorithms that were designed and implemented by hand.

(b) Extensive use of encrypting through electro-mechanical machines, around the period of the Second World War.The invention of such complex, mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption.

(c) Ever more permeative use of computers, about in the last fifty years, supported by solid mathematical basis.

PURPOSE OF CRYPTOGRAPHY

- **Authentication**. This process to prove the identity of an entity can be based on*something you know*, such as a password; *something you have*, such as an encryption key or card; *something you are*, such as biometric measurements.

- **Data integrity**. This property refers to data that has not been changed, destroyed, or lost in an unauthorized or accidental manner. The need for data integrity is especially evident if data is transmitted across a nonsecure network, such as the Internet.
- **Privacy/confidentiality**: Ensuring that no one can read the message except the intended receiver.
- **Non-repudiation**: A mechanism to prove that the sender really sent this message.

TYPES OF CRYPTOGRAPHY

- **SECRET KEY CRYPTOGRAPHY**

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 1, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called *symmetric encryption* or conventional cryptography .

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

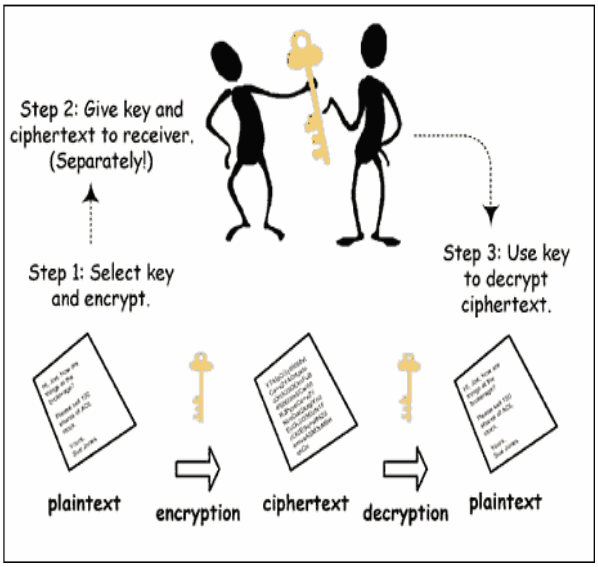


Figure 1

ADVANTAGES:

- **Simple:** This type of encryption is easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages.
- **Uses less computer resources:** Symmetric key algorithms are computationally less intensive than asymmetric key algorithms.
- **Speed:** Symmetric key encryption is much faster than assymetric key encryption.
- **Prevents widespread message security compromise:** A separate secret key is used for communication with every different sender and reciever. If a key is compromised, only the messages between a particular pair of sender and receiver are affected. Communications with other people are still secure.

DISADVANTAGES:

- A big disadvantage of symmetric key algorithms is the requirement of a shared secret key, with one copy at each end.
- Choosing, distributing, and storing keys without error and without loss is difficult to reliably achieve.
- Origin and authenticity of message cannot be guaranteed i.esince both sender and receiver use the same key, messages cannot be verified to have come from a particular user. This may be a problem if there is a dispute.

- If the key becomes known by unauthorized individuals, the key is compromised and must be regenerated and redistributed.

PUBLIC KEY CRYPTOGRAPHY

Public-key cryptography refers to asystem which requires two separate keys, one of which is secret and the other is public as shown in figure. Although different, the two parts of the key pair are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the ciphertext. Neither key can perform both functions by itself. The public key may be known to everyone without compromising security, while the private key must not be revealed to anyone not authorized to read the messages.

Public-key systems, such as Pretty Good Privacy (PGP), are becoming popular for transmitting information via the Internet. They are extremely secure and relatively simple to use. The only difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her.

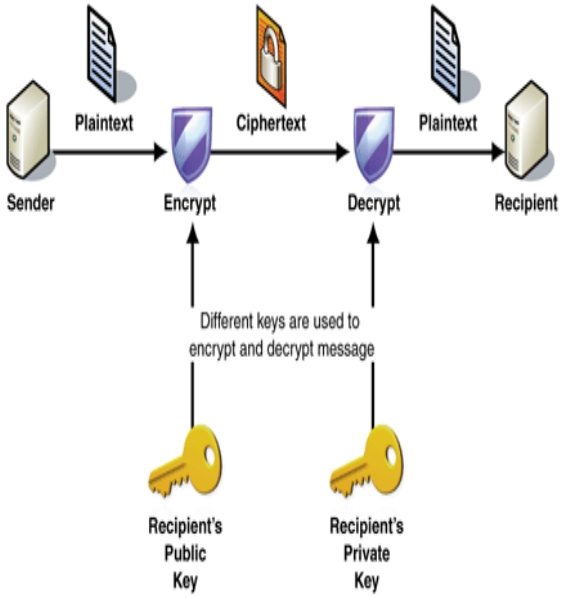


Figure 2

ADVANTAGES

- **Security** : The primary advantage of public-key cryptography is increased security, the private keys do not ever need to be transmitted or revealed to anyone.

- **Convenience:** It solves the problem of distributing the key for encryption.Everyone publishes their public keys and private keys are kept secret.
- **Provide for non-repudiation:** Digitally signing a message is similar to physically signing a document. It is an acknowledgement of the message and thus, the sender cannot deny it.
- **They can provide a method for digital signatures:** A digitally signed message cannot be modified without invalidating the signature.

DISADVANTAGES

- Public key encryption is slow compared to symmetric encryption.
- The key sizes must be significantly larger than symmetric cryptography to achieve the same level of protection.
- The loss of a private key means that all received messages cannot be decrypted.
- If an attacker determines a person's private key, his or her entire messages can be read.
- Requires lots of computer resources.

PROTOCOLS

A cryptographic protocol is a protocol that uses cryptography. A cryptographic protocol involves some cryptographic algorithm, but generally the goal of theprotocol is something beyond simple secrecy. The whole point of using cryptography in a protocol is to prevent or detect eavesdropping and cheating.

Cryptographic protocols are widely used for secure application-level data transport. A cryptographic protocol usually incorporates at least some of these aspects:

- Key agreement or establishment
- Entity authentication
- Symmetric encryption and message authentication material construction
- Secured application-level data transport
- Non-repudiation methods

HASH FUNCTIONS:

A cryptographic hash function is a hash function; that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digest.

Cryptographic hash function are an important tool in cryptography to achieve certain security goals such as authenticity, digital signatures , digital time stamping and entity authentication .They are also strongly related to other important cryptographic tools such as block ciphers and pseudorandom functions.

The ideal cryptographic hash function has four main properties:

- it is easy to compute the hash value for any given message
- it is infeasible to generate a message that has a given hash
- It is infeasible to modify a message without changing the hash
- It is infeasible to find two different messages with the same hash

DIGITAL SIGNATURES IN CRYPTOGRAPHY

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information. These features are every bit as fundamental to cryptography as privacy, if not more.

A digital signature is superior to a handwritten signature in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as the identity of the signer.

TRUST MODELS

Secure use of cryptography requires trust. While secret key cryptography can ensure message confidentiality and hash codes can ensure integrity, none of this works without trust.

There are a number of *trust models* employed by various cryptographic schemes. This section will explore three of them:

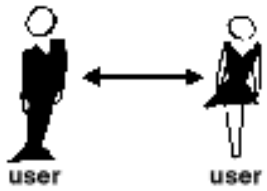
• Direct Trust

• Hierarchical Trust

• A Web of Trust

DIRECT

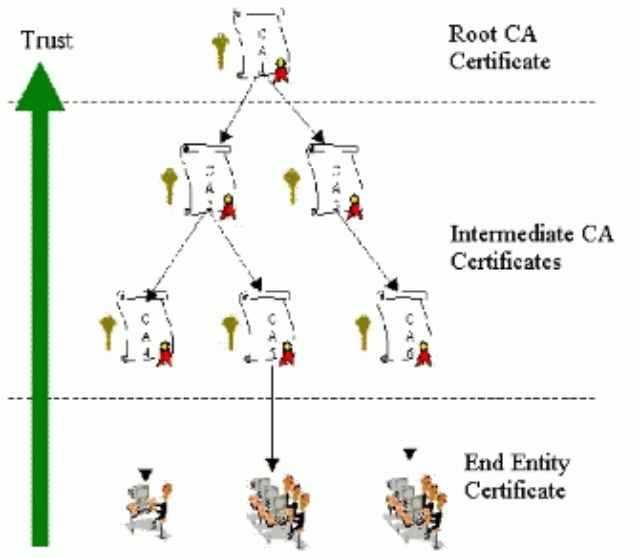
Direct trust is the simplest trust model. In this model, a user trusts that a key is valid because he or she knows where it came from. All cryptosystems use this form of trust in some way. For example, in web browsers, the root Certification Authority keys are directly trusted because they were shipped by the manufacturer. If there is any form of hierarchy, it extends from these directly trusted certificates. In PGP, a user who validates keys herself and never sets another certificate to be a trusted introducer is using direct trust.



Hierarchical Trust

In the hierarchical trust model everybody's certificate is issued by a third party called Certificate Authority (CA). If one trust the CA then he automatically trust the certificates that CA issues. This is a simplified form of hierarchical trust model. In reality there are a number of root certificate authorities from which trust extends. These CAs may issue certificates themselves, or they may issue certificates that are used to issue certificates down some chain.

The whole structure is like a trust tree. End (leaf) certificate is verified by tracing backward from its issuer to the issuer's issuer until a directly trusted root CA is found. Again we see direct trust here. A trusted third party is required to build the trust relationship without direct contacts among communicating parties.

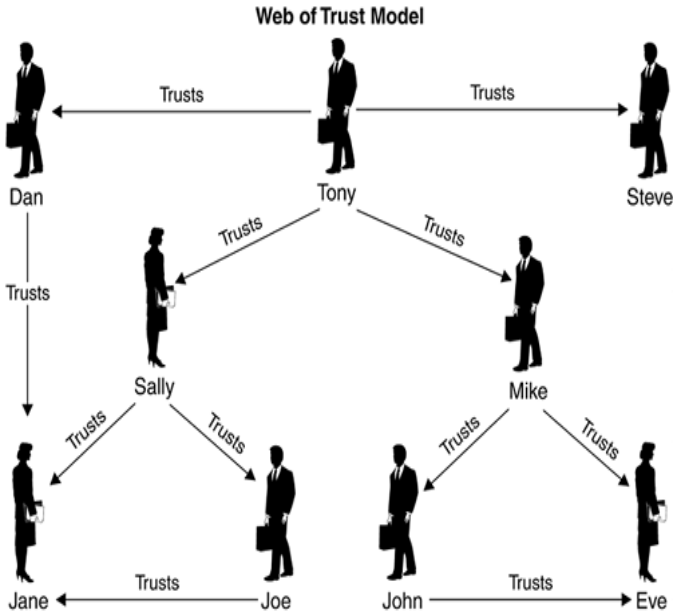


WEB OF TRUST:

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy andauthentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications.

Both when encrypting messages and when verifying signatures, it is critical that the public key used to send messages to someone or some entity actually does 'belong' to the intended recipient. Simply downloading a public key from somewhere is not overwhelming assurance of that association; deliberate (or accidental) impersonation is possible. From its first version, PGP has always included provisions for distributing user's public keys in an 'identity certificate', which is also constructed cryptographically so that any tampering (or accidental garble) is readily detectable but merely making a certificate which is impossible to modify without being detected is insufficient. It can prevent corruption only after the certificate has been created, not before. Users must also ensure by some means that the public key in a certificate actually does belong to the person or entity claiming it. From its first release, PGP products have included an internal certificate 'vetting scheme' to assist with this, a trust model which has been called aweb of trust. A given public key (or more specifically, information binding a user name to a key) may be digitally signed by a third party user to attest to the association between someone (actually a user

name) and the key. There are several levels of confidence which can be included in such signatures. Although many programs read and write this information, few (if any) include this level of certification when calculating whether to trust a key.



1. CONCLUSION

The goal of cryptography is to enable two people (A – sender, B – receiver) to communicate over an insecure medium in a manner whereby a third person (C) cannot comprehend the communication if the message was intercepted. In an age of explosive growth of digital data storage and communication, cryptography plays in integral role in our society. It is a challenge to respect the serious concerns of national security and copyright protection while also safeguarding individual liberties. The main purpose of this report is to disseminate basic cryptographic knowledge and discuss the implications of such knowledge on our society. This paper covers all the aspects of cryptography and various techniques and function used in cryptography.

REFERENCES

[1]http://www.garykessler.net/library/crypto.html

[2]http://www.creativeworld9.com/2011/04/abstract-and-full-paper-on-network_13.html

[3]http://www.studentpulse.com/articles/41/a-brief-history-of-cryptography

[4]http://www.logicalsecurity.com/resources/whitepapers/Cryptography.pdf

[5]http://www.slideshare.net/guest9006ab/a-brief-history-of-cryptography

[6]ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf

[7]http://en.wikipedia.org/wiki/Ciphertext

[8]http://www.divini.net/tlm3/products0708/mathspedia/it/cryptography.pdf

[9]http://i.thiyagaraaj.com/tutorials/introduction-of-cryptography/purpose-of-cryptography

[10]http://www.informit.com/articles/article.aspx?p=170808

[11]http://i.thiyagaraaj.com/tutorials/introduction-of-cryptography/types-of-cryptographic-algorithms#TOC-Secret-Key-Cryptography

[12]http://www.scribd.com/doc/22594424/Types-of-Cryptography

[13]http://vig.prenhall.com/samplechapter/0130614661.pdf

[14]http://en.wikipedia.org/wiki/Public-key_cryptography

[15]http://www.webopedia.com/TERM/P/public_key_cryptography.html

[16]http://voices.yahoo.com/comparing-symmetric-asymmetric-key-encryption-6329400.html

[17]http://www.pierobon.org/ssl/ch1/disad.htm

[18]http://www.ehow.com/info_8738577_advantages-disadvantages-private-key-encryption.html

[19]http://denis.arnaud.free.fr/zds/appendix/node8.html

[20]http://www.prismnet.com/~hcexres/power_tools/hyperweb/website1.PDF