Journal of Engineering and
Technology (JET)
Vol.1, Issue 1 Dec 2011 28-41
© TJPRC Pvt. Ltd.,

CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY

Mr.Kaushal Kishor
Hi-Tech Institute of Engineering College GZB.
Mr.Vihung Garg
Hi-Tech Institute of Engineering College GZB.

ABSTRACT

Cryptography is the only known practical method for protecting information transmitted through potentially hostile environments, where it is either impossible or impractical to protect the information by conventional physical means. Also, damage resulting from message alteration, message insertion, and message deletion can be avoided. Administrative and physical security procedures often can provide adequate protection for offline data transport and storage. However, where file security methods are either nonexistent or weak, encryption may provide the most effective and economical protection.

A basic task in **cryptography** is to enable users to communicate securely over an insecure channel in a way that guarantees their transmissions' privacy and authenticity.

We live in an era of unimaginably rapidly advancing and amazing technologies that enable instantaneous flow of information - anytime, anywhere. The convergence of computers and networks has been the key force behind the development of these awe inspiring technologies. Increasing use of systems built using these information technologies (IT) is having a profound impact on our everyday lives. These technologies are becoming all pervasive and ubiquitous. An illustration of this is provided by the development of mobile communication. There is a flurry of activity in the development of novel applications that run on this infrastructure. Phones have gone from wireless to small to smart to a situation where they can be used as entertainment devices (games, radios, mp3 players, cameras and now television), for serious personal applications(for location services, messaging and authentication, banking) in addition to being used also to talk to people. The fast paced development of these applications has been enabled by the flexibility of the underlying computing platform and the communication infrastructure. The key perquisite for the continued development and successful exploitation of IT is the notion of assurance. Information Assurance involves - Conducting those operations that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

INTRODUCTION

Cryptography is the art of hiding messege related to such aspects of data security as

Authentication: The process of proving one's identity.

Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.

Integrity: Assuring the receiver that the received message has not been altered in any way from the original.

Non-repudiation: A mechanism to prove that the sender really sent this message.

BENEFITS OF CRYPTOGRAPHY

Encryption can protect communications and stored information from unauthorized access and disclosure. Other cryptographic techniques, including methods of authentication and digital signatures, can protect against spoofing and message forgeries.

HISTORY

Cryptography has a long history, actually dating back to the time of Julius Caesar who encrypted messages by substituting each letter in the document by the letter that appears three positions further down the alphabet.

In 1967, the appearance of David Kahn’s best selling book entitled *The Codebreakers* introduced the general public to the secret world of cryptography. Interest continued to develop throughout the 1970s and 1980s much to the chagrin of the National Security Agency (NSA), with improved communication technology, the growing need for access control, electronic payments, and corporate security and the advent of the Internet, cryptography finally became public and world wide.

Prior to the Internet, use of cryptography was structured around symmetric cryptography. Symmetric cryptography uses the same key to both encrypt and decrypt information. That implies that both sender and receiver must possess the same key. Symmetric cryptography provided a great advantage over communication.

With the advent of the Internet, the use of symmetric cryptography proved to be an even greater liability because sender and receiver often never met or even knew each other. Public key cryptography, introduced in 1976 by Whitfield Diffie and Martin Hellman, was developed to accommodate the tremendous risks inherent in any Internet transmission, risks that symmetric cryptography couldn’t overcome. Unlike symmetric cryptography, public key cryptography uses two keys, one public and one private. The private key never has to leave the owner, negating the high risk of transporting keys to each document recipient. The public key can be made public so everyone can have access to it by simply downloading it from the Internet. The risks of safeguarding a highly secret key during distribution to users disappears, making public key cryptography ideally suited for the Internet, large distributed systems, and big corporate networks.

DIFFERENT TYPES OF CRYPTOGRAPHY

➢ QUANTUM CRYPTOGRAPHY

Quantum cryptography, uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

An important and unique property of quantum cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental part of quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavedrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. If the level of eavesdropping is below a certain threshold a key can be produced which is guaranteed as secure otherwise no secure key is possible and communication is aborted.

Quantum cryptography is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad as it is provably secure when used with a secret, random key.

➢ ELLIPTICAL CURVE CRYPTOGRAPHY

ECC is a public key encryption technique based on *elliptic curve theory* that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation. The technology can be used in conjunction with most public key encryption methods, such as RS. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

Elliptic curve cryptography was first proposed in 1985, by Neal Koblitz from the University of Washington, and Victor Miller at IBM. An elliptic curve is not an *ellipse* (oval shape), but is represented as a looping line intersecting two axes (lines on a graph used to indicate the position of a point). ECC is based on properties of a particular type of equation created from the mathematical group (a set of values for which operations can be performed on any two members of the group to produce a third member) derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result. Equations based on elliptic curves have a characteristic that is very valuable for cryptography purposes: they are relatively easy to perform, and extremely difficult to reverse.

➢ VISUAL CRYPTOGRAPHY

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers.

Visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into *n* shares so that only someone with all *n* shares could decrypt the image, while any *n-1* shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all *n* shares were overlaid, the original image would appear.

➢ FINANCIAL CRYPTOGRAPHY

FC is the use of cryptography in applications in which financial loss could result from subversion of the message system.Cryptographers think of the field as originating in the work of Dr David Chaum who invented the blinded signature. This special form of a cryptographic signature permitted a virtual coin to be signed without the signer seeing the actual coin, and permitted a form of digital token money that offered untraceability. This form is sometimes known as Digital Cash.

Financial cryptography includes the mechanisms and algorithms necessary for the protection of financial transfers, in addition to the creation of new forms of money. Proof of work and various auction protocols fall under the umbrella of Financial Cryptography. Hashcash is being used to limit spam.Financial cryptography is frequently seen to have a very broad scope of application. Ian Grigg sees financial cryptograpy in seven layers, being the combination of seven distinct disciplines: cryptography, software engineering, rights, accounting, governance, value, and financial applications. Business failures can often be traced to the absence of one or more of these disciplines, or to poor application of them. This views FC as an appropriately crossdiscipline subject.

➢ MALICIOUS CRYPTOGRAPHY: Kleptographic Aspects

In the last few years we have concentrated our research efforts on new threats to the computing infrastructure that are the result of combining malicious software (malware) technology with modern cryptography. At some point during our investigation we ended up asking ourselves the following question: what if the malware (i.e., Trojan horse) resides within a cryptographic system itself? This led us to realize that in certain scenarios of black box cryptography (namely, when the code is inaccessible to scrutiny as in the case of tamper proof cryptosystems or when no one cares enough to scrutinize the code) there are attacks that employ cryptography itself against cryptographic systems in such a way that the attack possesses unique properties (i.e., special advantages that attackers have such as granting the attacker exclusive access to crucial information where the exclusive access privelege holds even if the Trojan is reverse-engineered). We called the art of designing this set of attacks "kleptography."

CRYPTOGRAPHY IN GAMES

- **Crypto! (TM)** is a Windows version of the popular Cryptogram puzzles found in puzzle books or the Sunday paper. Crypto! selects a quote or phrase from its library of 50, encrypts it, and presents it for you to solve (the registered version includes over 10,000 puzzles). Solving cryptograms is more fun because Crypto! makes it easy to try various letters and undo mistakes. Letter frequencies are provided, and there are various hints and helps to get you started quickly.

Requirements:	Any Windows computer
Release Date:	January 12, 2001
Install Support:	Install and Uninstall
Platforms:	Windows 3.x, Windows NT 4.x, Windows 95, Windows 2000, Windows 98, Windows XP, Windows Me, Windows NT 3.x

Tags:	Cipher, Code, Crypto, Cryptogram, Game, Puzzle, Shareware
Users rating:	0/10

- Crypto-gram online flash word game, this free flash game develops your perception of words for speed reading and slow reading. This game is a Flash version of the cryptogram puzzles. Break the code and reveal the message. Crypto-gram selects a sentence from the list. Then it crypts it, and presents it for solving. This crypto gram game challenges the mind. The object of it is to solve the puzzles by selecting letters and placing them onto the crypto grams map.

CRYPTOGRAPHY NEXT GENERATION

Cryptography Next Generation (CNG) in the Windows Server® 2008 operating system provides a flexible cryptographic development platform that allows IT professionals to create, update, and use custom cryptography algorithms in cryptography-related applications such as Active Directory® Certificate Services (AD CS), Secure Sockets Layer (SSL), and Internet Protocol security (IPsec). CNG implements the U.S. government's Suite B cryptographic algorithms, which include algorithms for encryption, digital signatures, key exchange, and hashing.

A. What does CNG do?

CNG provides a set of APIs that are used to:

Perform operations, such as creating hashes and encrypting and decrypting data.

Create, store, and retrieve cryptographic keys.

Install and use additional cryptographic providers.

CNG has the following capabilities:

CNG allows customers to use their own cryptographic algorithms or implementations of standard cryptographic algorithms. They can also add new algorithms.

CNG complies with Common Criteria requirements by using and storing long-lived keys in a secure process.

CNG provides support for elliptic curve cryptography (ECC) algorithms.

THE FUTURE OF CRYPTOGRAPHY

A few years ago, the phrase crypto anarchy was coined to suggest the impending arrival of a *Brave New World* in which governments disappeared, and been replaced by virtual communities of individuals doing as they wish without interference. Crypto anarchy is the inevitable and highly desirable. With this technology, it will be impossible for governments to control information, compile dossiers, conduct wiretaps, regulate economic arrangements, and even collect taxes i.e.civil society based on a libertarian free market.

A new paradigm of cryptography, key escrow, is emerging and gaining acceptance in industry. Key escrow is a technology that offers tools that would assure no individual absolute privacy or untraceable anonymity in all transactions i.e. allow individuals to choose a civil society over an anarchistic one.

Cryptography's Limitations and Drawbacks

LIMITATIONS

Encryption does nothing to protect against many common methods of attack including those that exploit bad default settings or vulnerabilities in network protocols or software even encryption software.

If the system where the encryption is performed can be penetrated, then the intruder may be able to access plaintext directly from stored files or the contents of memory or modify network protocols in order to get access to keys or plaintext data. For example, PGP could be replaced with a Trojan horse that appears to behave like PGP but creates a secret file of the user's keys for later transmission to the program's owner much like a Trojan horse login program collects passwords

DRAWBACKS

Cryptography also threatens national security by interfering with foreign intelligence operations.

With encryption, an employee of a company can sell proprietary electronic information to a competitor without the need to photocopy and handle physical documents. The keys that unlock a corporation's files may be lost, corrupted, or held hostage for ransom, thus rendering valuable information inaccessible.

The Drift Toward Crypto Anarchy

Crypto anarchy can be viewed as the proliferation of cryptography that provides the benefits of confidentiality protection but does nothing about its harms. It is government-proof encryption which denies access to the government even under a court order or other legal order. It has no safeguards to protect users and their organizations from accidents and abuse. It is like an automobile with no brakes, no seat belts, no pollution controls, no license plate, and no way of getting in after you've locked your keys in the car.

The crypto anarchist position is that cyberspace is on a non-stop drift toward crypto anarchy.

The potential harms of cryptography have already begun to appear as child pornography, customs violations, drugs, espionage, embezzlement, murder, obstruction of justice, tax protestors, and terrorism.

The Emergence of Key Escrow as an Alternative

The benefits of strong cryptography can be realized without following the crypto anarchy path to social disorder. One promising alternative is key escrow encryption. The idea is to combine strong encryption with an emergency decryption capability. This is accomplished by linking encrypted data to a data recovery key which facilitates decryption. This key need not be the one used for normal decryption, but it must provide access to that key. The data recovery key is held by a trusted fiduciary, which could conceivably be a governmental agency, court, or trusted and bonded private organization. As part of this encryption initiative, the government developed an escrowed encryption chip called the **Clipper Chip**.

Each Clipper Chip has a unique key that is programmed onto the chip and used to recover data encrypted by that chip. This key is split into two components, and the two components are held by two separate government agencies: the National Institute of Standards and Technology and the Department of Treasury Automated Systems Division. The general specifications for the Clipper Chip were adopted in February, 1994, as the Escrowed Encryption Standard (EES), which is a voluntary government standard for telephone communications, including voice, fax, and data. The chip and associated key escrow system have been designed with extensive safeguards, including two person control and auditing, to protect against any unauthorized use of keys. Clipper's key escrow system does not provide user data recovery services.

Escrowing is done within the user's organization and serves primarily to protect against data loss.

Under current U.S. export regulations, encryption products with key lengths greater than 40 bits are not generally exportable when used for confidentiality protection. One of the attractions of key escrow encryption is that by providing a mechanism for authorized government decryption, it can enable the export of products with strong encryption.

Some type of escrow facility might be used to control anonymity services as well as encryption. For example, escrow could be used with digital cash and anonymous remailers to ensure traceability when there is a court order or other legal authorization for information about the originator of a transaction.

Alternatives to Key Escrow: Weak encryption

From the user's perspective, key escrow encryption has an advantage over weak encryption of allowing the use of strong encryption algorithms that are not vulnerable to attack. However, for applications where such a high level of security is not needed, weak encryption offers a less costly alternative. A disadvantage of weak encryption is that it can preclude real-time decryption in an emergency situation (e.g., kidnaping).

A third approach is **link encryption**. One major advantage of link encryption is that it allows someone with a cellular phone to protect the over-the-air connection into the phone system without requiring that the other party have a compatible encryption device or, use any encryption at all. Global System for Mobile (GSM), a world-wide standard for mobile radio telecommunications, encrypts communications transmitted over the radio link, but they are decrypted before being transmitted through the rest of the network. The disadvantage of link encryption is that plaintext data are exposed in, potentially, many intermediate nodes. By contrast, key escrow encryption can support secure end-to-end encryption.

CONCLUSION

Crypto anarchy is an international threat which has been stimulated by international communications systems including telephones and the Internet. Addressing this threat requires an international approach that provides for both secure international communications crossing national boundaries and electronic surveillance by governments of criminal and terrorist activity taking place within their jurisdictions. The adoption of an international approach is critical in order to avoid a situation where the use of encryption seriously endangers the ability of law enforcement agencies, worldwide, to fight terrorism and crime. The result will not be worldwide suppression of communications and encryption tools, as May asserts, but rather the responsible use of such tools lest they lead to social disorder. Our information superways require responsible conduct just as our interstate highways require.

Key escrow encryption has emerged as one approach that can meet the confidentiality and data recovery needs of organizations while allowing authorized government access to fight terrorism and crime. It can facilitate the promulgation of standards and products that support the information security requirements of the global information infrastructure. The governments of the OECD nations are working with the international business community to find specific approaches that are mutually agreeable.

REFERENCES

1. Tim May, "Crypto Anarchy and Virtual Communities," *Internet Security*, April 1995,
2. Secure Computing Corporation, "Answers to Frequently Asked Questions About Network Security," Roseville, MN, Oct. 1994.
3. Louis J. Freeh, Keynote talk at International Cryptography Institute, Sept. 1995. Available through http://www.fbi.gov/crypto.htm
4. Dorothy E. Denning and Dennis K. Branstad, "A Taxonomy of Key Escrow Encryption," *Comm. of the ACM*. Dorothy E. Denning, "Key Escrow Encryption: The Third Paradigm," *Computer Security Journal*, Summer,

1995 and Dorothy E. Denning, "Critical Factors of Key Escrow Encryption Systems," *Proc. National Information Systems Security Conf.*, Oct. 1995.

5. Statement by the Press Secretary, The White House, April 16, 1993.

6. John A. Thomas, "Can the F.B.I. Stop Private Cryptography?," *Internet Security*, April 1995, pp. 13-14.

7. Carmi Gressel, Ran Granot, and Itai Dror, "International Cryptographic Communication; KISS: Keep the Invaders (of Privacy) Socially Sane, presented at the International Cryptography Institute 1995: Global Challenges, Sept. 21-22, 1995.

8. Silvio Micali, "Fair Cryptosystems," MIT/LCS/TR-579.c, Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA, August 1994.

9. Thomas Beth, Hans-Joachim Knoblock, Marcus Otten, Gustavus J. Simmons, and Peer Wichmann, "Clipper Repair Kit - Towards Acceptable Key Escrow Systems," *Proc. 2nd ACM Conf. on Communications and Computer Security*, 1994.

10. Nigel Jefferies, Chris Mitchell, and Michael Walker, "A Proposed Architecture for Trusted Third Party Services," Royal Holloway, University of London, 1995.