General View on the Aspects of Cryptography

Amit Kumar*
Sonia Kumari**

Abstract

This paper provides the summary of cryptography & the areas where it is used or applied. Information Security is the method or the process to secure the information or data from unauthorized access. Cryptography is one of the methods to protect the data by making the data unreadable from all except users belongs to the category of sender or receiver. Cryptography is the process of secret writing that is hides the content of information from all except the sender and the receiver. As the use of technology increase, the probability of cyber-attack may be increase. So cryptography is kind of process that make sure about the data authentication, unauthorized access of data, confidentiality of data and integrity of data.

Keywords: Cryptography, Electronic Signature, Hashes, Virtual Private Network

Introduction

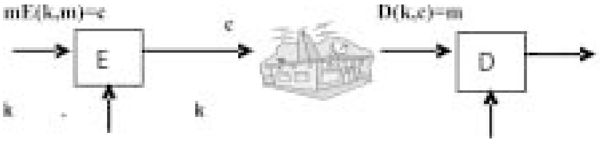
Information security plays a vital role during internet communication. When the sender send the data via internet communication channel, there is a probability of loss of data, stealing of data etc. So to protect the data, there are no of methods and cryptography is one of the methods that have a capability to protect the data. Data Security is absolutely essential when communication is carried between lacs of people daily on the internet. There are various cryptography methods that provide the way for secure e-commerce and e-payment on the unsecure channel of internet and protecting passwords. Cryptography is the necessary for protecting the information or in other word for secure communication. This paper provides the types of cryptography and their application.

Cryptography

The word cryptography comes from the Greek words êñõðôï (hidden or secret) and ãñáöç (writing)[1].The basic service provided by cryptography is the capability to send information between sender and receiver in a way that prevents the information by making it unreadable from others except sender and receiver. It also provides other services, such as

- Integrity checking—reassuring the recipient of a message that the message has not been altered since it was generated by a legitimate source
- Authentication—verifying someone's (or something's) identity But back to the traditional use of cryptography.
- Non-Repudiation—particularly important for financial or e-commerce applications.
- Confidentiality—the biggest concern will be to keep information private.

Original form of message is known as plaintext or cleartext. The meaningless information is known as ciphertext. The process for producing ciphertext from plaintext is known as encryption. The reverse of encryption is called decryption.



E, D: cipher k: secret key (e.g. 128 bits)
m, c: plaintext, ciphertext

Figure 1. Process of encryption & decryption

Encryption is the transformation of data into some unreadable or meaningless form. Its purpose is to

Amit Kumar*
Scientific Assistant (Adhoc)
IGIPESS, B-Block, Vikaspuri, Delhi

Sonia Kumari**
Assistant Professor (Adhoc)
IGIPESS, B-Block, Vikaspuri, Delhi

ensure privacy by keeping the data hidden from all except sender and receiver. Decryption is the reverse of encryption. It is the transformation of encrypted data back into some intelligible and meaningful form. Encryption and decryption require the use of some secret information, which is a key. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different.In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes about *any* network, particularly the Internet.

Various Types of Cryptography

Public Key Cryptography

Public-key cryptography has been said to be the most significant new development in cryptography. Modern PKC was first described publicly by Stanford University professor Martin Hellman in 1976 [2]. PKC is also called *asymmetric encryption*, uses a pair of keys for encryption and decryption as shown in figure 2.

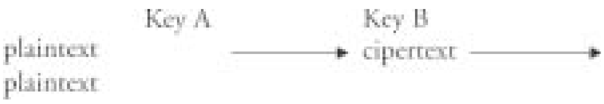


Figure 2: PKC Figure

PKC uses two keys, one for encryption and the other for decryption.

With public key cryptography, keys work in pairs of matched public and private keys.The major advantage asymmetric encryption offers over symmetric key cryptography is that senders and receivers do not have to communicate keys up front. Provided the private key is kept secret, confidential communication is possible using the public keys.Encryption and decryption are two mathematical functions that are inverses of each other.

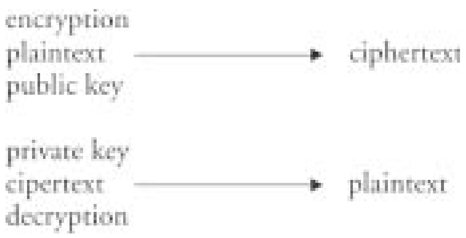


Figure 3: PKC using two keys

There is an another thing one can do with public key technology, which is to generate a digital signature on a message. A digital signature is a additional number associated with a message.

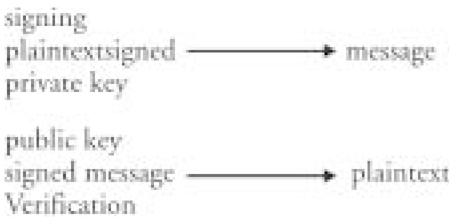


Figure 4: PKC using digital signature

Translucent Cryptography

In this scheme the government can decrypt some of the messages, but not all. Only p fraction of message can be decrypted and 1-p cannot be decrypted.

Symmetric Key Cryptography

Symmetric key cryptography is also known as Secret key cryptography. In this method of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the key that are used by sender and decrypted by the same key that is used by the receiver. Key must be shared between the sender and receiver as shown in figure 5.

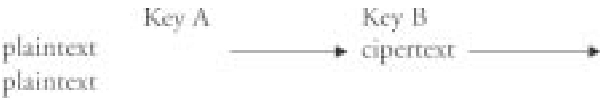


Figure 5: Symmetric key

SKC uses a single key "key A" both encryption and decryption.

This method works well if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers of people.

Secret key cryptography schemes are categorized in 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.

Hashes

Hash functions take data of an arbitrary length (and possibly a key or password) and generate a fixed-length hash based on this input. Hash functions used in cryptography have the property that it is easy to calculate the hash, but difficult or impossible to re-generate the original input if only the hash value is known. In addition, hash functions useful for cryptography have the property that it is difficult to craft an initial input such that the hash will match a specific desired value.

MD5 and SHA-1 are common hashing algorithms used today. These algorithms are considered weak (see below) and are likely to be replaced after a process similar to the AES selection. New applications should consider using SHA-256 instead of these weaker algorithms [3].

Application of Cryptography

There are number of cryptographic algorithms available that are used to solve the problem related to data confidentiality, data integrity, data secrecy and authentication of data and user. User uses the various algorithms according to the requirement of the work.

Privacy in Transmission

Current privacy systems for transmission of data use a private key for transforming the data because it is the quicker method with overhead and reasonable assurance.

In case of the number of communicating parties is small, key distribution is done periodically and maintenance of key is based on physical security of the keys.

In case of the number of parties is large, electronic key distribution is used. Usually, key distribution was done with a special key-distribution-key (also known as a master-key) maintained by all parties in secrecy over a longer period of time than the keys used for a particular transaction. The "session-key" is generated at random either by one of the parties or by a trusted third party and distributed using the master-key.

The problem with master-key systems is that if the master-key is successfully attacked, the entire system collapses. Similarly, if any of the parties under a given master-key decides to attack the system, they can forge all messages throughout the entire system.

With the advent of public-key systems, privacy can be maintained without a common master-key or a large number of keys. Instead, if B wants to communicate with A, Bsends Aa session-key encrypted with A's public key. A decrypts the session-key and uses that over the period of the transaction.

Privacy in Storage

Privacy in storage is basically maintained by a one-key system where the user provides the key to the computer at the beginning of a session, and the system then takes care of encryption and decryption throughout the course of normal use. For an example, numbers of hardware devices are available for personal computers to automatically encrypt all information that stored on disk. When the computer is turned on, the user must enter a secret key to the encryption& decryption the hardware. The information cannot be meaningful without key, so even if the disk is stolen, the information on it will not be readable or useable because it is meaningless without the secret key [5].

But there is also a problem in privacy of storage. If the user forgets a key, all information that is encrypted with that key becomes permanently unusable. The information is encrypted while in storage, not when in use. If the encryption and decryption are done in software, or if the key is stored anywhere in the file of system, the system may be circumvented by an attacker [6].

Integrity in Transmission

Mainly users of communication systems are not as much concerned about secrecy as about integrity. In an electronic funds transfer, the amount sent from one account to another in public domain. How bank is managed and maintained about proper transfers can be made in a proper way. If an active tapper could introduce a false transfer, funds would be moved any other account. Cryptographic techniques are widely used to assure that intentional or accidental modification of transmitted information does not cause erroneous actions to take place.

A technique for assuring integrity is to perform a checksum of the information being transmitted and also transmit the checksum in encrypted form. Once the information and encrypted checksum are received, the information is again checksummed and compared to the transmitted checksum after decryption. If the checksums agree, there is a high possibility that the message is unaltered. Unfortunately, this scheme is too simple to be of practical value as it is easily forged. So designing strong cryptographic checksums is therefore important to the assurance of integrity.

Integrity in Storage

The mean of assuring integrity of stored information has been access control. Access control means locks and keys, guards, and other mechanisms of a physical or logical. The spread of computer viruses has changed this to a significantly, and the use of cryptographic checksums for assuring the integrity of stored information is becoming widespread.

Authentication of Identity

Simple passwords have been used for hundreds of years to prove identity. More complex protocols such as sequences of secret keys exchanged between sets of end users.Cryptography is the theory and practice of using passwords, and modern systems also use strong cryptographic transforms in conjunction with physical properties of individuals and shared secrets to provide highly reliable authentication of identity.

Practice of Using good passwords falls into the field known as key selection. In essence, a password is a secret key for any cryptosystem that allows encryption and decryption of everything that the password allows access to.

The selection of keys has historically been a cause of cryptosystem failure. Although we know from Shannon that H(K) is maximized for a key chosen with an equal probability of each possible value (i.e. at random), in practice when people choose keys, they choose easy password that easy to remember, and therefore not at random. This is most dramatically demonstrated in the poor selection that people make of passwords.

On many systems, passwords are stored in encrypted form with read access available to all so that programs wishing to check passwords needn't be run by privileged users. A side benefit is that the plaintext passwords don't appear anywhere in the system, so an accidental leak of information doesn't compromise system wide protection.

For passwords allowing numbers, lower case letters and special symbols, this goes up considerably. Studies over the years have consistently indicated that key selection by those without knowledge of protection is very poor. In a recent study, 21% of the users on a computer system had 1 character passwords, with up to 85% having passwords of 1/2 the maximum allowable length, and 92% having passwords of 4 characters or less. These results are quite typical, and dramatically demonstrate that 92% of all passwords could be guessed on a typical system in just over an hour.

Credential Systems

A credential is a document that introduces one party to another by referencing a commonly known trusted party. For example, when credit is applied for, references are usually requested. The credit of the references is checked and they are contacted to determine the creditworthiness of the applicant. A driver's license is a form of credential, as is a passport.

Electronic credentials are designed to allow the credence of a claim to be verified electronically. Although no purely electronic credentialing systems are in widespread use at this time, many such systems are being integrated into the smart-card systems in widespread use in Europe. A smart-card is simply a credit-card shaped computer that performs cryptographic functions and stores secret information.

Electronic Signatures

Electronic signatures, like their physical counterparts, are a means of providing a legally binding transaction between two or more parties. To be as useful as a physical signature, electronic signatures must be at least as hard to forge, at least as easy to use, and accepted in a court of law as binding upon all parties to the transaction.

Electronic Cash

There are patents under force throughout the world today to allow electronic information to replace cash money for financial transactions between individual accounts. Such a system involves using cryptography to keep the assets of nations in electronic form. Clearly the ability to forge such a system would allow national economies to be destroyed in an instant. The pressure for integrity in such a system is staggering.

Threshold Systems

Threshold systems are systems designed to allow use only if a minimal number of parties agree to said use. For example, in a nuclear arms situation, you might want a system wherein three out of five members of the Joint Chiefs of Staff agree. Almost threshold systems are based on encryption with keys which are distributed in parts. The most common technique for partitioning a key into parts is to form the key as the solution to N equations in N unknowns. If N independent equations are known, the key can be determined by solving the simultaneous equations. If less than N equations are known, the key can be any value since there is still an independent variable in the equations. Any number can be chosen for N and equations can be held by separate individuals. The same general concept can be used to form arbitrary combinations of key requirements by forming ORs and ANDs of encryptions using different sets of keys for different combinations of key holders. The major difficulties with such a system lie in the key distribution problem and the large number of keys necessary to achieve arbitrary key holder combinations [6].

Systems Using Changing Keys

Shannon has shown to us that given enough reuse of a key, it can eventually be determined. It is common practice to regularly change keys to limit the exposure due to successful attack on any given key. A common misconception is that changing a key much more often than the average time required for break the cryptosystem, provides an increased margin of safety.

If we chose the key at random, and that the attacker can check a given percentage of the keys before a key change are made, it is only a matter of time before one of the keys checked by the attacker happens to correspond to one of the random keys. If the attacker chooses keys to attack at random without replacement over the period of key usage, and begins again at the beginning of each period, it is 50% likely that a currently valid key will be found by the time required to try 50% of the total number of keys, regardless of key changes. Thus if a PC could try all the DES keys in 10 years, it would be 50% likely that a successful attack could be launched in 5 years of effort. The real benefit of key changes is that the time over which a broken key is useful is limited to the time till the next key change. This is called limiting the exposure from a stolen key [7].

Hardware to Support Cryptography

Basically in history, cryptography has been carried out through the use of cryptographic devices. The use of these devices derives from the difficulty in performing cryptographic transforms manually, the severe nature of errors that result from the lack of redundancy in many cryptographic systems, and the need to make the breaking of codes computationally difficult.

In WWII, the ENIGMA machine was used by the Germans to encode messages, and one of the first computers ever built was the BOMB, which was designed to break ENIGMA cryptograms. Modern supercomputers are used primarily by the NSA to achieve the computational advantage necessary to break many modern cryptosystems. The CRAY could be easily used to break most password enciphering systems, RSA systems with keys of length under about 80 are seriously threatened by the CRAY, and even the DES can be attacked by using special purpose computer hardware. Many devices have emerged in the marketplace for the use of cryptography to encrypt transmissions, act as cryptographic keys for authentication of identification, protect so called debit cards and smart cards, and implementing electronic cash money systems [8].

Cryptography in Daily Life

Emails

Today, we live in a modern world with the technology. We send emails for general communication with friends, business communication within the companies or with the person whose email address we have. Normally people send billions of emails daily either for the business communication or friendly communication. We deliver the emails through the internet that is a huge big network consisting of a thousands of computers, nodes etc. A number of people like to steal data from others, sometimes it may be for fun, but the data is the main important thing of any organization. Loss of data is very dangerous for any organization. The first three countries in the highest number of internet users list [8]:

1. China
2. USA
3. JAPAN

There is millions of user who use email service on internet. So the question comes, how do emails get protected while they are being sent?

We all need secure communication. To secure the email service that can be possible if the all connections between routers and routers need to be secured. That is done by using the technique data encryption. There are two methods for this security [9].

1. Use PGP (Pretty Good Privacy). It is a method to secure email, a standard in cryptographically secure emails. It is used with MIME Security.
2. Sender secure their website self, recipient has a username and password. Recipient read the data after logging into the website.

Usually, ISPs can encrypt the process of communication between the sender and receiver by using TLS and SASL protocol. Email server is also using this kind of protection between each other.

TLS is used in different circumstances. TLS is used with POP3 & IMAP services. If HTTP is protected by TLS, it provides more security then simple HTTP.

TLS (Transport Layer Security) and SSL (Secure Layer Security) are very same. Basically TLS is the successor of SSL. They are used for messages, emails, browsing etc. These protocols are used by everyone who use the internet. TLS plays a very important role on the internet. HTTP, FTP, SMTP, NNTP are protocols with TLS protection. TLS uses protocol which is known as reliable connection (like TCP). TLS is commonly used with HTTP to create HTTPS.

In case of VPN, TLS is used to tunneling an entire network. Thereis number of users use FTP (File Transfer Protocol) for transfer of data between two nodes. There are no of FTP servers and clients available on the Internet. These tools ease our work. If we use the client side, we can manage or organize our download. If we use the server side, manage the user who can download. FTP use usernames and passwords for the protection but it is vulnerable. FTP is built in a way which provides ability for users on the same network as the transfer is being processed to sniff data including: username, password and files. There is no built-in security or data encryption. A well-known solution for this security problem is to use either SFTP OR FTPS [10].

VPN

VPN (Virtual Private Network) is a virtual computer network. It used virtual circuits or open connections to have the network together. It has a special security system. Authentication is required before connecting with VPN. If we are a trusted user, have a right to access to resources.

Secure VPNs are designed to provide privacy for the users. The essentiality of this consists in cryptographic tunneling protocols. Secure Virtual private Network ensures message integrity, confidentiality and sender authentication.

We use cell phone and telephone to communicate each other. Telephones transmit electric signals over a communication channel that is telephone network. But the problem is that it can easily be eavesdropped. Eavesdroppers require only three things [10] [11] [12]

a. a pickup device,
b. a transmission channel
c. Listening device.

The pickup device is commonly a microphone or a video camera. These devices are used to record sound or to capture video images which later to be converted to electric signals. Data transmit through a link which may be a wire or a radio transmission. A listening device allows monitoring, recording or retransmitting signals.

Mobile phones are used by almost every second man on the earth. Through mobile phones, we use no of services like SMS, MMS, EMAIL, INTERNET, and GAMING AND BLUETOOTH. To protect our self against eavesdropping, we can use the cell phone encrypting devices [13].

Conclusion

In this research paper we have analyzed of different areas where cryptography is used in our daily activities.

As a normaluser, we can easily find cryptography everywhere around us. Emails and Internet are used by more and more people every day. We cannot feel or imagine our lives without it. And all of these work and services are secured based on different types of algorithms of cryptography. The use of technology is increase in great percentage for daily activities. As the use of technology increase, the probability of steal of data over the untrusted communication channel is also increase. So to prevent the data, different types of encryption & decryption techniques are used.

References

1. Spenciner, mike, Perlman,r, and aufman.c. "*Network Security:Private Communications in a Public World*", chapter 2, accessed on December, 23, 2014 on internet.
2. Goyal, Shivangi, "*A survey on the Applications of Cryptography*, in International Journal of Science and Technology Vol. 1 No. 3, March, 2012, pp. 137-140.
3. Marwaha, Mohit, Bedi Rajeev and Singh, t., *"Comparative Analysis of Cryptographic Algorithm "*, in International Journal of Advanced Engineering Technology, Int J Adv Engg Tech/iv/iii/July-Sep., 2013 pp. 16-18.
4. Gupta, V., and Singh, G., *Advanced Cryptography algorithm for improving data security*, in International Journal of Advanced Research in Computer Science and Software Enginering, volume 2, Issue 1, January, 2012.
5. Panday, L. N., and Shukla, N., *"Visual Cryptography Scheme using Compressed Random Shares"*, in International Journal of Advanced Research in Computer Science and Management Studies, 2013, IJARCSMS, Vol. 1, Issue 4, Sep. 2013, pp. 62-66.
6. http://nptel.ac.in/courses/106105031/ accessed on December 05,2014 on Internet.
7. http://williamstallings.com/Cryptography/accessed on Dec,05, 2014 on Internet.
8. http://en.wikipedia.org/wiki/Cryptography accessed on Dec, 10, 2014 on Internet.
9. https://technet.microsoft.com/en-us/library/cc962027.aspx accessed on Dec. 21, 2014 on Internet.
10. http://freevideolectures.com/Course/3027/Cryptography-and-Network-Security accessed on January, 02 , 2015 on Internet.
11. http://people.eecs.ku.edu/~saiedian/teaching/Fa10/710/Readings/An-Overview-Cryptography.pdf accessed on January, 13, 2015 on Internet.
12. Aameer Nadeem, Dr. M.Younus Javed, *"A performance comparison of data Encryption Algorithm"*, in Global Telecommunication Workshops, 2004 GlobeCom Workshops 2004, IEEE.
13. Elkamchouchi, H.M; Emarah, A.-A.M; Hagras, E.A.A, "*A New Secure Hash Dynamic Structure Algorithm (SHDSA) for Public Key Digital Signature Schemes"*, in the 23rd National Radio Science Conference (NRSC 2006).