Cryptography: An Art of Writing a Secret Code

Samiksha Sharma
DAV Institute of Engineering and Technology, Jalandhar, Punjab, India

Abstract

In present era the requirement of internet for wireless communication is rising day by day and thus there is a need of security to guard such communication by users on insecure wireless channels. Data sent over the communication channels is susceptible to attacks because of sensitive information it contain. Cryptography is an art of writing a secret code that defend the data getting exchanged between two communicating parties from external attack. Cryptography is used to hide the confidential details so that the information can be sent securely over the timid network. In this paper a brief review of cryptography is presented along with the study of various cryptography techniques which are widely used to protect data from intruder attack. Various security threats to data over an insecure network are studied. In this paper different cryptography methods are discussed along with the data threats and how that data can be protected through different cryptography techniques.

Keywords

Asymmetric Encryption, Hashing, Symmetric Encryption, Security Threats

I. Introduction

In present era the requirement of internet for wireless communication is rising day by day and thus there is a need of security to guard such communication by users on unsecure wireless channels. Data sent over the communication channels is susceptible to attacks because of sensitive information it contain. To defend the data from external threat the concept of Cryptography is emerged. Cryptography is defined as "An art of writing a secret code" [1], Methodology of Writing that code is cipher and the text is then converted into cipher text which is commonly called Encryption whereas the reverse practice of converting a cipher text into normal text is known as Decryption. Cryptography can be categorized as classical and modern, classical cryptography techniques were used to foil eavesdropping and message interception problems whereas the modern cryptography techniques are more secure and useful for high speed communications. Modern cryptography techniques are more secure than the classical ones and are widely used such as DES, 3DES, AES, ECC, ECDH, RSA etc. From [2] we can see difference between code and cipher. Cipher deals with transformation whereas code deals with replacement of words. We need a key or a pair of keys to perform encryption and decryption on the data, after encrypting the data two kinds of ciphers will be generated one is called transposition cipher and another is commonly known as substitution cipher. Whenever there is rearrangement of character in a word it is termed as Transposition cipher because in the resultant output, letters are interchanged. Another is called Substitution cipher where different substitutes of the original characters in the input data are generated [1]. A simple kind of substitution method takes all the characters and forward them by some position say we have N, where N is cipher key and if N=3 then each letter will be shifted to third value from current state.

II. Aim of Cryptography

Core purpose of cryptography is to prevent any kind of thievery or stealing of private information, along with this it helps in providing authentication. So for this purpose we use various kinds of techniques to foil data from theft. Cryptography must ensure four basic data protection requirements and those are authentication, privacy, integrity and non–repudiation. Following requirements are described in [3] as:-

- **Authentication**- Where we have to verify user's identity involved in communication.
- **Privacy-** To ensure no third person can intercept the message.
- **Integrity -** Ensures that original message and received are same i.e. no alteration of data.
- **Non-repudiation-** Here we need to verify the sender's identity.

So two groups will be involved in this process where one will be the sender and another receiver. Sender will send the data by encrypting it with the key generally called encryption process and receiver will decrypt the message with the help of key known as Decryption process. The purpose of cryptography is to provide authentication of data, privacy so that the sensitive information cannot be used by third party for false means, correctness of data without any modification to the original data and non-repudiation where the identity of sender will be confirmed whether that data is coming from the intended user or not. Cryptography ensures all these requirements for data security. These are necessary requirements which are to be fulfilled by any kind of security algorithm in order to posse's high level of security to the data.

III. Data Security

Data security deals with the data stored in computer and transmitted in communication i.e. it is a study of various procedures and science of securing the data kept in the database or data transferred over network. We can see from [1] the four types of control covered under data security and those are cryptography controls, inference controls, information flow controls and access controls. Data security also covers the procedures of backup and recovery. Also [4] states the following advantages of having data security:-

- **To know what kind of data it is and to classify it -** To check the relationship between data kept in the database and to define rules and policies for that.
- **To get rid of damages which can be there -** To check the vulnerabilities and solidify repositories.
- **Continuous monitoring and auditing-** Data will be monitored on regular intervals In order to know about the chances of threat or any kind of damage to the stored data.
- **To secure data from unauthorized access -** To avoid the content or to block the content which violates policies set by data security procedures.
- **To secure data which is sensitive-** To protect sensitive data we need proper encryption and decryption mechanisms which are essentials of data security.
- **How to manage access**- User can access data to some extent or only authenticate users can have access to data and also privileges are managed.

So cryptography ensures data security and provides diverse set of algorithms to protect data. Let's have a look at modern cryptography data security techniques.

IV. Modern Cryptography

There are number of different cryptography techniques that prevent data from various kinds of intruder attacks. From the past we can see evolution from classical cryptography towards modern cryptography techniques which are proven more significant impact wise in various fields to foil data that has been sent over insecure channel. Among all, the common cryptography techniques are Public key cryptography, Private Key cryptography and Hashing. All these techniques covers enormous range of algorithms that have different architectures and fundamentals principles to provide data security using basic set of rules.

Let's start with the general study about modern cryptography techniques, how they work to guard data from external threat. Given fig. 1 shows all the modern cryptography techniques.

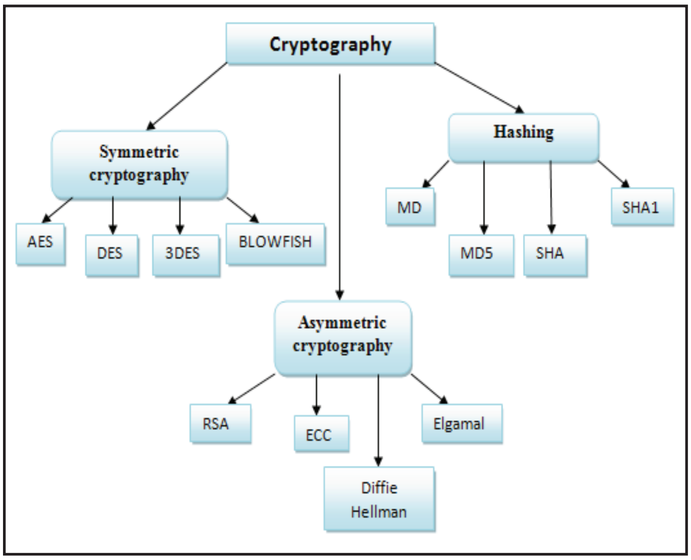

Fig. 1: Modern Cryptography Techniques

As discussed above while sending data to another user, sender will encrypt the original text with the help of the key after that a cipher text will be formed and transferred over the network to another user. On receiving data, user will decrypt the cipher with the help of the key to get the original text back which was originally sent by the sender. Fig. 2 depicts the general terminology of encryption and decryption process.

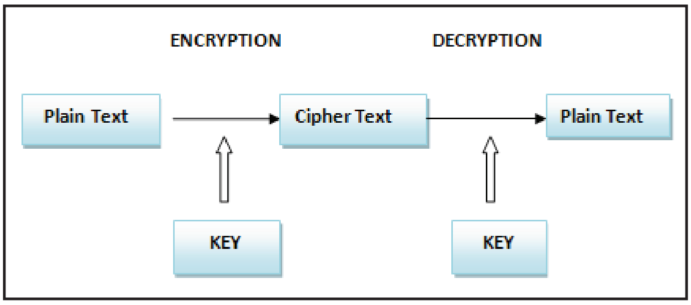

Fig. 2: Encryption/Decryption Terminology

This forms the basic principle of other modern cryptography algorithms where key plays an important role in securing the authentication and integrity of the message sent over an insecure network. If a third party want to extract sensitive information from the data, they have to search for the valid key.

A. Secret Key Cryptography

Secret key encryption is also known as symmetric key encryption scheme. Here only one key will be used by the sender and receiver of message to encrypt and decrypt i.e. the secret key will be same in between them for the entire communication. As discussed [5] sender will encrypt the message using secret key and on the other side receiver will decrypt the same message with same secret key, if that key is intercepted by anyone within the communication link then that person can change the message or can use it for illegal means by reading it. From [2] we can say that in symmetric encryption it's all about secrecy about the key which is shared among the sender and receiver not the algorithm. Symmetric encryption is much faster and makes less use of the resources also we can say that this encryption algorithm supports high computation speed [6-7]. On the other hand there are some disadvantages such that authentication is not guaranteed and key distribution is a major problem because of which this algorithm is not suitable for client server system [6,8]. There are different types of symmetric algorithms available and are widely used such as DES (Data encrypt standard), 3DES, AES (Advanced encrypt standard) and Blowfish. Sender will input the plaintext, using shared secret key sender will encrypt the plain text. After encryption cipher text will be formed which is not easy to understand. Receiver will accept that cipher text and decrypt that cipher using the same shared key to obtain the original text back. For symmetric encryption the shared secret key will be same for the entire communicating session, if that key is compromised than the security can be easily breached.

Fig. 3 demonstrate the methodology of the symmetric encryption and decryption.

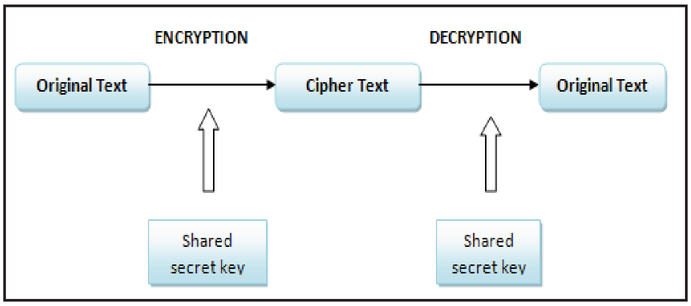

Fig. 3: Symmetric Encryption/Decryption

B. Public Key Cryptography

Public key cryptography is also known as asymmetric encryption scheme [5] and here different keys are used for encryption and decryption of message. Two keys one private key and another public key are used to protect conversations. We declare public key as public to every sender who wants to communicate and private key is kept secret with the receiver of the message. So here for encryption process we need public key and for decryption process we need a private key. While providing privacy it also ensures authentication through digital signature. From [9] self certification is not needed as we have digital certificates for authentication. No need to compromise security as public key is shared among all users [6]. So public key cryptography is much better than secret and is widely used for systems like client and server. Say if different clients want to communicate with the server then in that case key pairs are generated on server's end, one private key and another public. Server will declare public key and pass it to different clients that want to participate in the communication with the server and server will keep secret key or private key with itself without letting other know about that secret key. Client will encrypt the message using the public key and send it to the server, on the other hand side server after receiving the message which is a cipher decrypt that cipher using the private key owned by it. Major advantage of using an asymmetric algorithm is key distribution problem is solved; better key management is there as different communicating parties have their own key pairs through which they can encrypt and decrypt. Better authentication guaranteed using digital signatures which provide non-repudiation by signing message [6-7], on the other side there's a disadvantage of speed which is thousand fold slower than symmetric algorithm as large number of key pairs have to be generated for different sessions where key management will be there on both sides of sender and receiver and it makes much use of resources [10]. Some of asymmetric algorithms are RSA, Elliptic curve cryptography, Diffie-hellman and Elgamal. So if in any case receiver has as doubt whether public key is compromised then receiver will not decrypt the message as private key will be with the receiver. With security perspective if one can see asymmetric encryption is much efficient and is widely adopted for securing large data sets but symmetric holds good speed for encryption and decryption of messages and should be used for fast communicating systems with lesser amount of data sets. Given below fig. 4 illustrate the process of encryption and decryption using different key pairs in asymmetric cryptography.

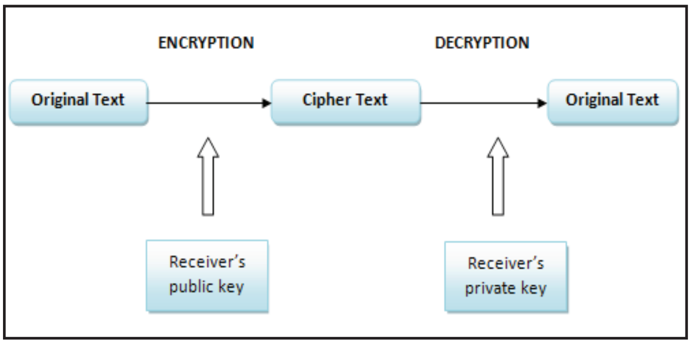

Fig. 4: Asymmetric Encryption/Decryption

C. Hashing

Third well known method is cryptography hashing after symmetric and asymmetric encryption. Whenever a data block of variable length is entered as input to this cryptographic system fixed hash value will be obtained [6]. So there is no use of key it will convert the input to the smaller length output value [5] so the thing is if there's a change even of 1 bit in the original input the output will be completely different or changed. From [3] if we take the file's data, hash algorithm helps to provide digital fingerprint ensuring that the contents of file are not changed or altered also passwords can be securely encrypted through hash functions. We can detect collision possibilities in the hash function with the help of birthday attack [2]. There are different hash algorithms used the common ones are:-

- MD (Message Digest Algorithm)
- SHA(Secure Hash Algorithm)

Once we obtain the output i.e. hash value it is difficult for intruder to get the original text and for same input value there are different hash values so it is difficult to derive the original value. Multiple hash values can be obtained from the original input by making certain changes to it. Fig. 5 demonstrate hashing process where a variable length message is taken as input to the hash algorithm to obtain a fixed length output hash.

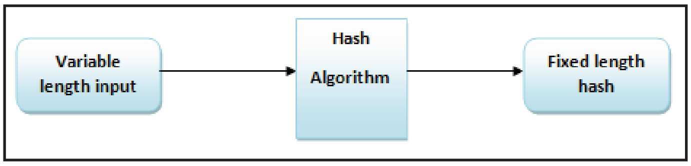

Fig. 5: Hashing Terminology

V. Cryptography Algorithms

Here in the given Table 1, we can see various algorithms which comes under asymmetric and symmetric encryption algorithm along with their features which covers DES (Data encrypt standard) [5][11], AES (Advance encrypt standard) [12], RSA [13], Blowfish [14], Elliptic curve cryptography [15], MD (Message digest) [16], MD5 [17], SHA1 [18] and SHA (Secure hash family algorithm) [17].

Table 1: Different Algorithms with Features

Algorithm	Feature
DES	• It was developed by IBM and consists of 16 cycles of round for operations like swapping, permutation and combination. • Major operations are permutation and other extension.
AES	• NIST announced AES in 2000 as algorithm by rijndael. • Basic operations are adding round key, byte substitution and finally diffusion which is shifting of rows and column mixing.
RSA	• Developed by Leonard Adleman, Adi Shamir and Ron Rivest. • This method is totally based on assumption of finding factors of integers which are too large.
Blowfish	• Consist of fiestal network where encryption and decryption iterated 16 times.
ECC	• This cryptography algorithm was developed by Koblitz and miller based on discrete logarithm problem, Consists of elliptic curves where we use variables and some constants over finite field. • In ECC the key size is less as compared to RSA 1024 bit key of RSA is similar to have a 160 bit key in ECC, so it is preferred over RSA.
MD	• Used in digital signatures where a digest is digitally signed.
MD5	• Developed by Professor Ronald. L Rivest, MD5 for a file is considered as checksum with a value of 128 bit. • Because of this algorithm there are less chances of getting the duplicate values corresponding to two different files. • Length of hash depends upon the algorithm not on the file size. Supports irreversibility and repeatability.
SHA	• Takes as input message of variable length and produce hash of desired length.
SHA1	• It takes any kind of code or text as input and generates large bits of output which serve as fingerprint for the given input. • if there's a slight change in the input like addition or deletion of a symbol or character in an email whole output will be changed.

Above mentioned algorithms are widely used for data protection each has its own advantage and disadvantage. Irrespective of the fact that these algorithms provide high level of data security there are still some threats that can harm the data. Let's have a brief preface to some of well known security threats.

VI. Security Threats

Strong need for data security comes from the fact that there are malicious attacks to the data kept in database or data which is shared among various users. While data is sent over the communication links over network there are more chances of attacks to the data so there is strong need for data security or cryptography. There are number of threats discussed in [6], [20-24] and [7]. Table 2 covers all the discovered security threats to data over the insecure medium.

Table 2: Different Security Threats to Data

Attacks	Meaning
Eavesdropping	When intruder is listening to the communication and try to extract some information from it
Replay Attack	Here the intruder will check the message first if it is of his use he will modify it then send that modified copy to the receiver
Exhaustive Search Attack	Here a checking is done for all inputs to the hash unless original hash value is determined
Burn Attack	Here the attacker will send countless number of request message's to the server to which server will try to decrypt and suffer from burn attack
Insider Threat	Insider attack can be done by the person belonging to the organization who has knowledge of data policies and procedures
Physical Attack	Physical attack refers to attack to hardware, a kind of threat to maintenance and electrical threat like failure of server
Birthday Attack	Collisions between all the pairs of hash values by making fraudulent values to the original hash value so after large number of trials there will be some value which will match the original hash value
Dictionary Attack	Intruder will try for different possibilities of input to hash value by choosing or randomly selecting words from dictionary
Passive Attacks	Here one can make use of information but without affecting the resources of the system. Two kinds of passive attacks are message content and another traffic analysis.
Active Attacks	This involves change of data entities. it is divided in following types :- • Masquerade • Modification of messages • denial of service • Replay

VII. Benefits of Cryptography

Yes it is essential to have cryptography as it provides enormous range of services such as data security, data integrity, data privacy and authentication. Cryptography has many advantages because of them it is widely used to secure data getting exchanged between different parties over a risky wireless medium. In today's era of ubiquitous computing where internet is the main root for providing door to door network for communication, security is of major concern. Different people can communicate from different regions across the world safely and exchange confidential information securely using security techniques which can be applied to the exchanging medium. From [25] we can see the following advantages of having cryptography for data security:

- Whenever a connection is there between our PC and internet to make use of e-mail or any social network site or we browse something a secure connection is made by TLS commonly known as transport layer security.
- When we do shopping via e-commerce the entire entered customer data is verified and scanned thus fully protected through cryptography.
- When there is communication between two people on phone the digitized voice of communicating users is encrypted so that it can be prevented from eavesdropping.
- All online transactions say withdrawing money from ATM is secured by cryptography.
- For the central lock car system a remote key is associated with them which produce keys which are unique by communicating with the car hence protected by cryptography..
- Cryptography also ensures authentication where user can verify one's identity and different statements using a public cryptography.
- Public cryptography provides one way communication as only a specific receiver can decode the message.

VIII. Conclusion

Today ubiquitous computing is adopted world-wide for providing services through internet. Internet helps in transmission of information between different groups of people from different regions through wireless or wired media. For communicating through wireless channels security is necessary as risk of information stealing is there. This paper presents the basic preface of cryptography and discussed various cryptography algorithms which are used extensively such as symmetric, asymmetric and hashing for securing information. It also covers major attacks to the data sent over an insecure channel. User before transmitting data must be aware of these attacks as they can steal confidential information and an external party or third person can modify the data so cryptography is necessary to ensure the security of the data. Asymmetric encryption is better in terms of key distribution than symmetric but slow in computation hence is suitable for client and server systems whereas hashing ensures the privacy of original data as it supports irreversibility. So at the end paper concludes that cryptography ensures security, integrity, confidentiality and non-repudiation of data.

References

[1] Denning, Dorothy E.,"Cryptography and Data Security". Addison-Wesley Publishing Company, America, 1982.

[2] Devi, T.R.,"Importance of Cryptography in Network Security". Communication Systems and Network Technologies (CSNT), International Conference on IEEE, 6-8 Apr, pp. 462-467, 2013.

[3] Kessler, G., (1998),"An Overview of Cryptography". [Online] Available: http://www.garykessler.net/library/crypto.html#purpose.

[4] IBM,"Data Security and Protection". [Online] Available: http://www-03.ibm.com/software/products/en/category/data-security.

[5] Jain, A., "Cryptography". [Online] Available:http://www.ankitjain.info/articles/Cryptography_ankit.html.

[6] Abdulrahman, H., Poh, N., Burnett, J.,"Privacy Preservation, Sharing and Collection of Patients Records using Cross-

Clinical Secondary Analytics". Computational Intelligence in Healthcare and e-health (CICARE), 2014 IEEE Symposium, 9-12 Dec, pp. 148-153, 2014.

[7] Stallings, W.,"Cryptography and Network Security". Pearson Education, 2006.

[8] Kahate, A.,"Cryptography and Network Security". Tata Mac-Graw Hill Education, 2013.

[9] Chandra, S., Paira, S., Alam, S.S.,"A Comparative Survey of Symmetric and Asymmetric Key Cryptography", Electronics, Communication and Computational Engineering (ICECCE), International Conference on. IEEE, 17-18 Nov, pp. 83-93, 2014.

[10] Forouzan, B., Mukopadhyay, D., "Cryptography and Network Security (SIE)". Mac-Graw Hill Education, 2011.

[11] Jie, L., Yuxiang, Lv., Huafang, S.,"A power analysis resistant DES cryptographic algorithm and its hardware design". Digital Manufacturing and Automation (ICDMA), 2012 Third International Conference on IEEE, 31 jul-2 Aug, pp. 121-124, 2012.

[12] Guo, G., Qian, Q., Zhang, R. (2015), "Different implementations of AES cryptographic algorithm". High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conference on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on IEEE, 24-26 Aug, pp: 1848-1853.

[13] Minni, R., Sultania, K., Mishra, S.,"An algorithm to ,enhance security in RSA". Computing, Communications and Networking Technologies (ICCCNT), Fourth International Conference on IEEE, 4-6 Jul, pp. 1-4, 2013.

[14] Alabaichi, A., Ahmad, F., Mahmod, R.,"Security analysis of blowfish algorithm". Informatics and Applications (ICIA), Second International Conference on. IEEE, 23-25 Sep, pp. 12-18, 2013.

[15] Vigila, S. Maria C., Muneeswaram, K.,"Implementation of text based cryptosystem using elliptic curve cryptography". Advanced Computing, 2009. ICAC 2009 First International Conference on IEEE, 13-15 Dec, pp 82-85, 2009.

[16] Zhu, Z., Zhai, K., Wang, B.,"Research on Chaos-based Message Digest Method for Medical Images". Image and Signal Processing, 2009. CISP'09. 2nd International Congress on. IEEE, 17-19 Oct, pp. 1-5, 2009.

[17] Zinov, K.,"Take control of your Files". [Online] Available: www.fastsum.com.

[18] Goodin, D., "SHA1 algorithm securing e-commerce and software could break by year's end". [Online] Available: http://arstechnica.com/security/2015/10/sha1-crypto-algorithm-securinginternet-could- break-by-years-end/.

[19] Lin, C.H., Yeh, Y.S., Chien,"Generalized secure hash algorithm: SHA-X". International Conference on Computer as a Tool (EUROCON), IEEE, 27-29 Apr, pp. 1-4, 2011.

[20] McGregor, P.K.,"Animal Communication Network". Cambridge University Press, 2005.

[21] Syverson, P.,"A taxonomy of replay attacks [cryptographic protocols]". Computer Security Foundations Workshop VII, 1994 CSFW 7 Proceedings IEEE, 14-16 Jun, pp. 187-191, 1994.

[22] Biham, A.,"Types of cryptanalytic attacks using related keys". Journal of cryptology, Vol. 7, No. 4, pp. 229-246, 1992.

[23] Ruppert, B., "Protecting Against Insider Attacks". SANS Institute InfoSec Reading Room, 2009.

[24] Orbitco (2015), "Network Threats to Physical Infrastructure". [Online] Available: http://www.orbit-computer- solutions.com/network-attacks-threats-to-physical-and-network-infracstructure/.

[25] Rijmenants, D. (2004), "What is Cryptography". [Online] Available: http://users.telenet.be/d.rijmenants/en/cryptography.htm.

Samiksha Sharma received her B. Tech degree from Beant College of Engineering and Technology, Gurdaspur, Punjab, India and currently pursuing Master's from DAV Institute of Engineering and Technology, Jalandhar, Punjab, India. Her research areas include Cryptography and Network Security.