www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 5 Issue 8 August 2016 Page No. 17787-17793

Taxonomy of Cryptography Techniques for Network Security

Kanika Sharma[1], Dr. Nischay Bahl[2]

[1]Assistant Professor, P.G Department of Computer Science
D.A.V College, Jalandhar, India
[2]Associate Professor and Head, P.G Department of Computer Science
D.A.V College, Jalandhar, India

Abstract-
Cryptography is the art of secret writing. Data encryption means that only a person having the secret code or key can read scrambled information. The important role of cryptography is to provide the security to the wireless networks. Over the years, many encryption techniques have been provided and used. The conventional methods of encryption can only preserve the data. Developing the new concept in cryptography is a demand of the current time, because the modern cryptography is very much needed to boost the data security. Therefore, it is necessary to relate efficient encryption technique to boost data security. This paper discusses different historical cryptography techniques, modern encryption algorithms (symmetric and asymmetric), and newer areas that are being explored in cryptography. This paper also explores its applications in network security.
Keywords-Data security, Encryption, Decryption, multiple encryptions.

1. Introduction

The word cryptography is taken from the Greek word “Kryptos”. Kryptos is used to hidden, secret or mysterious anything from the outer world. Cryptography, defined as "the science and study of secret writing”, so that only authorized people can see the real message. In cryptography, messages and data can be encrypted to prevent there interception, using codes, ciphers, and other methods [1]. Network security is highly based on cryptography. Security often requires that data be preserved safe from unauthorized access. [2]. Basic methods used in Cryptography are:

Plain Text: Plain text is the original message and put as an input at the time of encryption process. For example: if the sender sends message “cryptography” to the receiver then it is considered as a plain text.

Cipher Text*:* Ciphertext is not understandable by anyone. It is an output of the encryption process. For example: “fubswrjudskb” is a ciphertext produced for plain text “cryptography”.

Encryption: By using the encryption key a plain text converts into cipher text and an algorithm identified at that time is known as “encryption algorithm”.

Decryption: Converting a cipher text into a plain text by using decryption key is known as decryption. An algorithm identified at that time is known as “decryption algorithm”.

Keys: A Key is a numeric, alpha-numeric text or may be a special symbol. At the time of encryption the key is used on the Plain Text and at the time of decryption the key is used on theCipherText

2. Historical Cryptography

Cryptography and encryption have been used for secure communication for thousands of years. Some of the historical encryption techniques are discussed in Table 1.

DOI: 10.18535/ijecs/v5i8.60

Table 1: Historical cryptography method

S. No	Name	Year	Developer	Description
1	Ancient Egypt	1900 B.C.	Khnumhotep's	This method of encryption is an example of a substitution cipher, which is any cipher system which substitutes one symbol or character for another. Those who could read and write were easily breaking this method of encryption [3].
2	Greece	500 B.C.	Spartans	This technique used a device. The device was a cylinder message that was then written lengthwise on the parchment. Once it was unwound the message on the strip of parchment became unreadable [4].
3	Rome	2,000 years ago	Julius Caesar	Caesar developed a substitution cipher method in which different letters were used for substitute letters. Only those who knew the substitution used this technique for sending the secret messages and by that, these messages were not exposed [5].
4	Alberti-Vigenere Cipher	Mid 1400's	Leon Battista Alberti	They use Cipher disk, a mechanical device with sliding disks for encryption. It was permitted for many different methods of substitution. This is an encryption method based on the concept of a polyalphabetic cipher [6].
5	Jefferson Wheel Cipher	Late 1700's	Thomas Jefferson	This technology was used 26 wheels with the alphabet randomly scattered on each wheel, and these were numbered with a specified order. Only a person having wheels in the proper order can decrypt the ciphertext [7].

3. Modern Encryption

Modern encryption can be separated into two parts based on the use of keys, Secrete Key, and Public key.

3.1 Symmetric Encryption

At both encryption and decryption level same encryption key is used. Symmetric Encryption involves the use of a single key. A message called plaintext and secret key, encryption generates unreadable data called "ciphertext", which is about the same length as the plaintext was. Decryption is the overturn of encryption and uses the same key as encryption. The key plays an extremely important role in this type of encryption. Conventional cryptography or symmetric cryptography is also known as Secret key cryptography. Example: DES, 3DES, BLOWFISH, AES etc. discussed in Table 2.

Table 2: Example of Symmetric Encryption

S.No	Name	Year	Developer	Description
1	DataEncryption Standard (DES)	1975	IBM	DES is used in many commercial and financial applications. It has proved resistant to all forms of cryptanalysis.[8]
2	3DES	1978	IBM	It uses 64-bit block size with 192 bits of key size. In 3DES the encryption level and the average safe time increased by 3 times. 3DES is easy to implement in both hardware and software.
3	Advanced Encryption Standard (AES)	1998	Joan Daemen and Vincent Rijmen	The AES has also been used to secure information in smart cards and online transactions. The design and strength of the AES algorithm (i.e., 128, 192 and 256) are adequate to protect confidential information up to the SECRET level. CONFIDENTIAL information will require the use of either the 192 or 256 key lengths.[9]

3.2 Asymmetric Encryption

Public key cryptography is sometimes also referred to as asymmetric cryptography. In this type of encryption dissimilar keys is being used for encryption and decryption process. Unlike secret key cryptography, keys are not shared. Each individual has two keys: a private key that need not be revealed to anyone, and a public key that is possibly known to the entire world. Two different key is generated at once and one key is distributed to another side before the transmission starts.
Example Diffie-Hellman, RSA, and Merkle-Hellman discussed in Table 3.

Table 3: Example of Asymmetric Encryption

S.No	Name	Year	Developer	Description
1	Diffie-Hellman key Exchange	1976	Whitfield Diffie and Martin Hellman	The Diffie-Hellman Key Exchange allows two parties with no prior knowledge of each other to establish a public secret key, which typically cipher. The Diffie-Hellman Key Exchange protocol gives two parties the same key without essentially transmitting it.[10]
2	RSA Encryption	During 1990	Rivest, Shamir and Adleman	RSA works with two dissimilar keys: A "public" key, and a "private" key. Both keys work complementary to each other, a message encrypted with one of the key can only be decrypted by its matching part.[11]

4. Current Expansion in Data Encryption

Early Encryption keys were exclusively concerned with converting messages into unreadable facts to defend the message from unauthorized access during its transmission. Today encryption techniques have expanded its area and are
widely used to protect data by encryption in a cost effectual manner. The earliest forms of cryptography were easy to decode and were vulnerable to various attack. In the modern age, cryptography has grown from basic message confidentiality to include some phases of message integrity checking, sender/receiver identity authentication, and digital signatures, among other things. In Table 4, the current expansions are discussed

Table 4: Current Expansion in Data Encryption

S.No	Name	Year	Developer	Description
1	Policy based cryptography	1984, 2000 and 2001	Adi Shamir, devised by Sakai and Boneh and Franklin	Policy based cryptography uses a policy to encrypt data in such a way that only the policyholders are able to decipher the data. The encryption of such may contain AND'ing or OR'ing of conditions [12].
2	Elliptical Curve Cryptography	1985, widely in use 2004-05	Neal Koblitz and Victor S. Miller	It's become popular due to its improved security and a smaller key. This encryption technique utilizes the complex nature of elliptic curves over finite fields. Diffie-Hellman Key Exchange and RSA Encryption algorithms are used in ECC. But the numbers used in ECC are chosen from a finite field defined within an elliptic curve expression [13].
3	Genetic Algorithm	Mid 1980s,	John Holland	Genetic Algorithm (GA) which is typically used to obtain results for optimization and search problems. They model genetic processes usually of inheritance and DNA pattern and make use of the transformation, population size, selection and individual fitness theories [14].
4	Biometric cryptosystems	1984	Adi Shamir first proposed	It also widely in use today. They don't have the need to memorize passwords or swap keys and still provide accurate identification and privacy but require the existence of the user at all times [15].
5	Quantum key cryptography and id Quantique company	1991 and in 2004, 2007, 2010, 2014	Artur Ekert and (Swiss company based in Geneva, Switzerland)	This area focuses mainly on the quantum key exchange and the uses an invisible photon. These use photons to generate a common bit string between two parties. The security of QKE rests on the law that no information about the quantum state can be acquired without introducing disturbance [16]. The first commercial quantum cryptography system turns out to be available from id Quantique. Several world premieres in quantum

				technology has realized by company in 2004,2007,2010,2014 [17] [18].
6	Visual cryptography	1994	Moni Naor and Adi Shamir	In this two transparent images are used. One contains random pixels and the other image contains the message. It is impossible to retrieve the message from only one of the images. Both the images in the correct order are required to disclose the information. It does not require complex mathematical calculations for decryption. The two images are usually printed on a transparent sheet. [19] [20].
7	Neural cryptography	1995	By an IT Master Thesis	It is another emerging field which deals with the application of Neural Network algorithms for use in encryption. It is based on the detail that neural networks can synchronize by mutual learning [21].
8	Identity-based cryptography	In 1984, devised in 2000 and in 2001	Shamir, devised by Sakai, and Boneh and Franklin	It is based on public key cryptography. Users' identifier information such as email or IP addresses instead of digital records can be used as the public key for encryption or signature confirmation. As an effect, identity-based cryptography widely reduces the system complications and the cost of establishing and managing the public key authentication framework known as Public Key Infrastructure (PKI) [22].
9	Steganography And Network steganography	Firstly used in 1499, in 2003	By Johannes Trithemius, by Krzysztof Szczypiorski	Steganography includes the suppression of information within computer files. Media files are perfect for steganographic communication because of their huge size, e.g. a sender might start with an bland image file and exchange the color of every 50^{th} pixel to a lower letter or a upper letter in the alphabet, a change in the image was so slight that someone does not look for it [23]. After that, the network steganography technique may be used to exchange steganogram in telecommunication networks for hiding all information.
10	Lightweight cryptography	2007	Orange Labs, Ruhr University Bochum and the Technical University of Denmark	Lightweight cryptography is modified for such confined devices, with the goal of balancing the tradeoffs between performance, low resource requirements, and cryptographic strength [24]. Block ciphers, hash functions, and public key cryptography for lightweight cryptography.
11	Bitcon Cryptocurrency	In 2008-2009	Satoshi Nakamoto	Bitcoin is a form of money that is used to control cryptography creation and management. It is known as cryptocurrency, a payment system. It is a direct system, without an intermediary. There is a public distributed ledger, called the block chain used for recording the verified transactions. These transactions are verified by network nodes [29].
12	Position-based quantum cryptography	In 2010	Buhrman et al.	The target of position-based quantum cryptography is to relate the geographical location of a user as its (only) credential. For example, a sender sends a message at a specific position with the undertaking that a receiver with a specific position can only be received the message [25].
13	Threshold Cryptosystem	In October 2012	RSA Security	The participating parties send and receive messages using RSA security technology. This technology built for many public encryption schemes. These encryption schemes are to be as secure as the original scheme [30].
14	Quantum Teleportation	Sept. 2014	University of Geneva, with the collaboration of Nasa's JPL, Nist, Chimie ParisTech and the University of Paderborn.	In quantum physics, it is possible for two particles that were to be "knotted" as, if they were a whole, even though separated by large distances. In the macroscopic world, shifting of a quantum state of a photon over long distances makes the quantum teleportation so interesting, which is potentially very useful. In the research of quantum computation and quantum networks, the grouping of quantum teleportation with quantum memories opens new possibilities [26].
15	Quantum Non-Locality	October 2015	Kavli Institute of Nanoscience	Quantum non-locality fact is supported at the 96% confidence level based on a "loophole-free Bell test" study [27].
16	Double Ratchet Algorithm	March 2016	Trevor Perrin and Moxie Marlinspike	It uses the signal protocol and end-to-end encryption method which is used to secure all communications to other Signal users. Send and receive encrypted instant messages, group messages, attachments and media

	and Signal protocol			messages can be used Signal [31].

5. Encryption in Network Security

Network security is an ever increasing area. As the complexity of the network rises the need for security also rises. Computer users need to hide details from the unauthorized users. Encryption is one of the techniques that provide the system to meet the said terms. Apart from security cryptography also provides-

- Certificates- It is an electronic document that identifies an individual, organization or a server.
- Proxy signature mechanism-this allows a proxy signer to sign on behalf of an individual.
- Key distribution-Security in most networks is ensured by applying cryptographic methods in various protocols. Diffie-Hellman and Quantum Key Exchange were designed specifically for this purpose. Some of the protocols which use encryption in some form are:
- SSL: It provides all the basic security services except for access control.
- SSH: It provides access control and a channel for secure exchange of data.
- KERBEROS: It uses an only symmetric key for encryption.
- SET: It provides security in credit card transactions.
- PGP: It is used to encrypt the data of an email with the use of asymmetric key encryption [28].

While data encryption can ensure security against some types of attacks there are other factors which can degrade the quality of the network to a great extent.

6. Conclusion

The field of cryptography includes algorithms and methods for the encryption of a message and its safe traversal over a network. Network Security is one of the import aspects of data communication. Cryptography is used to achieve the security objectives like confidentiality, integrity, authentication, non-repudiation. The selection of one of the best algorithm is also very important. With the help of these algorithms and techniques, one can generate his own ciphers by making minor alterations to the existing cipher algorithms. Also, the performance evaluation of various techniques can be done and be improved upon in the future.

References

[1] International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 A Survey on Various Most Common Encryption Techniques by E.Thambiraja, G. Ramesh and Dr. R. Umarani.

[2] IJARCET International Journal of Advanced Research in Computer Engineering & Technology, Vol. 2, Issue 12, Dec 2013" Cryptography The art of hiding Information" by Manoj Kumar Pandey1, Mrs. Deepty Dubey2.

[3] The Art of Cryptology: From Ancient Number System to Strange Number System http://www.ijaiem.org/Volume2Issue4/IJAIEM-2013-04-29-100.pdf

[4] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub, Mohammad Odeh, "Survey Paper: Cryptography Is the Science of Information Security", International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3): 2011.

[5] Richard A. Mollin, codes: the guide to secrecy from ancient to modern times https://www.semperfidelis.ro/request.php?59

[6]Chris Christensen : Cryptography of the VigenèreCipher,http://www.nku.edu/~christensen/section%2011%20vigenere%20cryptography.pdf

[7]David G. Luenberger: ciphers, http://press.princeton.edu/chapters/s11_8214.pdf

[8] E. Biham and A. Shamir. Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, New-York, 1993.

[9] Advanced Encryption Standard (AES) . FIPS. November 23, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (accessed March, 15, 2010).

[10] Whitfield Diffie and Martin Hellman New Directions in Cryptography. IEEE Communications Magazine. 1978.
[11] RSA Algorithm: http://www.di-mgt.com.au/rsa_alg.html
[12] Giovanni Di Crescenzo and Marc ,"Policy-Based Cryptography:Theory and Applications" December 2006http://www.eurecom.fr/en/publication/2122/download/cebaggwa-061208.pdf.
[13] Avi Kak , Elliptic Curve Cryptography and Digital Rights Management,https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture
[14] Swati Mishra,and Siddharth Bali, "Public Key
Cryptography Using Genetic Algorithm" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, May 2013.
[15] IEEE, Biometric Cryptosystems: Issues and Challenges http://www.cse.msu.edu/~jain/BiometricCryptosystemsIssuesAndChallenges.pdf
[16]Hoi- kwong Lo and Yi Zhao,"quantum cryptography"April2008http://arxiv.org/pdf/0803.2507.pdf.
[17] Although the commercial availability was announced earlier, the first orders were shipped to customers around 2004.
[18] http://arxiv.org/abs/1407.742714.pdf
[19]Matthias Baumgart " Visual Cryptography" January2003http://wwwmayr.informatik.tumuenchen.de/personen/baumgart/download/public/vc.pdf.
[20]http://users.telenet.be/d.rijmenants/en/visualcrypto.htm
[21]Andreas Ruttor, Neural Synchronization and Cryptography, http://arxiv.org/pdf/0711.2411.pdf
[22] F. Hess, Efficient Identity Based Signature Schemes Based on Pairings , Selected Areas in Cryptography { Proceedings of SAC 2002, LNCS 2595, pages 310{324, Springer-Verlag, 2002.
[23] R. J. Anderson and A. P. Petitcolas, "On the limits of steganography" IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 474--481, May 1998.
[24]http://cybersecurity.mit.edu/2013/09/lightweight-cryptography/.
[25] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum cryptography protocols against entanglement attacks. ArXiv/quant-ph: 1009.2256, Sep 2010.
[26] Takeda et al., "Deterministic quantum teleportation of photonic bits by a hybrid technique", Nature, August 2013.
[27] A. Broadbent. Delegating private quantum computations. Canadian Journal of Physics , 93(9): 941{946, 2015. DOI: 10.1139/cjp-2015-0030.
[28]http://www.dis.uniroma1.it/~alberto/didattica/cnsslides/IPSEC&SSL.pdf.
[29] Joshua Kopstein (12 December 2013). "The Mission to Decentralize the Internet". The New Yorker. Retrieved 30 December 2014. The network's "nodes"—users running the bitcoin software on their computers—collectively check the integrity of other nodes to ensure that no one spends the same coins twice. All transactions are published on a shared public ledger, called the "block chain"
[30]http://kindle.worldlibrary.net/articles/Threshold_cryptosystem
[31] "Advanced cryptographic ratcheting" Moxie Marlinspike, 26 November 2013.

Author Profile

Kanika Sharma received her M.C.A degree from P.T.U in 2008. Since 2009- present, she is working as Assistant Professor in Post Graduate department of computer science, D.A.V College, Jalandhar (Punjab). Her research interest includes Wireless Networks, Cryptography and Information security, Computer

Networks. She has published 7 research papers in various reputed international, national journals and conferences.

Dr. Nischay Bahl is working as Associate Professor and Head in Post Graduate department of computer science, D.A.V College, Jalandhar (Punjab) since 1999 – Present. He received his B.Tech degree from Kerala University and M.S degree from Birla Institute of Technology (BITS) Pilani. He did his PhD from Dr. B.R Ambedkar National Institute of Technology, Jalandhar. His areas of interest are Wireless Sensor Networks, Wireless Communication, Numerical Computing, Network Design and Optimization etc. He is a reviewer for numerous national and international journals and has a number of international and national publications to his credit.