ISSN No. 0976-5697

Volume 3, No. 7, Nov-Dec 2012

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Encryption Techniques as Security Tools: A Technical Review

Avanish Kumar Singh*
Department of Computer Science & Engineering
Nehru College of Engineering & Research Centre
Thrissur, Kerala, India
avnpt@rediffmail.com

Amit Kumar Pathak
Department of Computer Science & Engineering
Jahangirabad Institute of Technology,
Barabanki, Uttar Pradesh, India
myself_amit1@rediffmail.com

Ashutosh Kumar Rao
Department of Information Technology
Sunderdeep Engineering College,
Ghaziabad, Uttar Pradesh, India
ashutoshrao7@gmail.com

***Abstract**:* We all know that the security problems are occurring seriously on the internet and ratio of cyber threats are also increasing rapidly. So, protecting the confidential, sensitive and some private information from unauthorized disclosure have become need of every organization or any individual. In computerized information, it will be required the techniques for providing the security for information. Various methodologies and algorithms such as cryptographic techniques or security tools have been developed for security point of view and work for searching new techniques is continuing. In this paper, we have reviewed on those encryption techniques, which are used to protect the information during transferring from one place to another on shared network. Sometimes these encryption techniques can be helpful to encrypt the storage information for keeping it secure. Here, we have tried to cover all those encryption/decryption techniques, which provide reliable security for information.

Keywords: Cryptographic encryption, Symmetric key, Cipher text, Public key encryption, Wireless security, Digital signature

I. INTRODUCTION

Information security is term used to provide protection from unauthorized access, unauthorized uses, disclosures, intruders etc. The processes and activities for information security provide valuable input/output for organizing and managing IT systems and their development, enabling risk identification, planning and mitigation. In this business world, where the competition is neck to neck, there is confidential information of organizations, which is to be kept secret from any other person. Due to these prevailing scenarios, most of the classified information is kept on removable drives under lock and key, and the internal networks or defense intranets are never been connected to the internet.

Today's time, there is one of the big tasks to create and maintain secure information. Various companies or organization need to keep some important information such as private data or any confidential mater secure, which are not sharable with unauthorized or any other person. In term of computer system the information can be defined in form of files, which consists overall information created and saved by the companies or organizations. Protecting this type confidential information is business requirement for everyone. So the major problem of securing information data through information technology can be defined in many ways and there are also various approaches available, which ensure the security of information in their own way. This shows that how low our confidence on computer systems is. [1]

The fields of information security are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including: securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, etc.

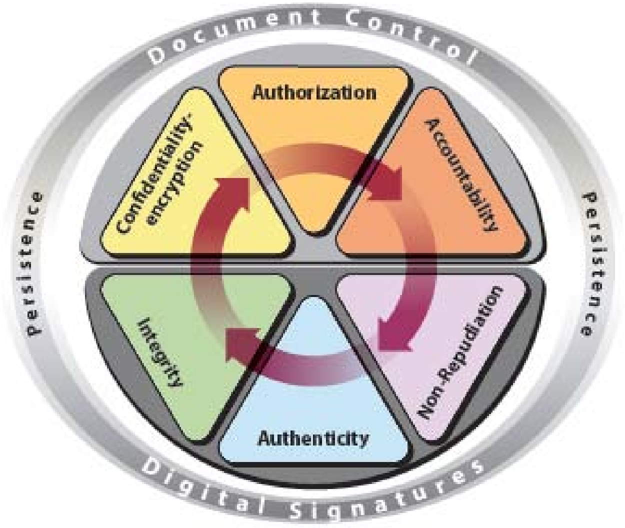

Figure 1: Six major key criteria for providing persistent information security

Information security has therefore assumed a greater importance in today's world. The primary aspects of information security are confidentiality, integrity and availability. These three major factors are important not only to business sector but also to the Government and critical infrastructure such as Power, Telecommunications, Transportation, Energy, Banking & Finance and Defense, etc. Information security has become essential part of the day-to-day functioning of these sectors. [2, 26] A significantly more effective solution for protecting an electronic document is to assign security parameters that are an integral part of the information itself. The following criteria define persistent Information security:

***a. Confidentiality*:** Who should have access to the information?

***b. Authorization*:** What permissions does the user have for working with the document?

***c. Accountability*:** What has the recipient done with the document?

***d. Integrity*:** How do you know if the document has been altered?

***e. Authenticity*:** How do you know where the document came from?

***f. Non-repudiation*:** Can the signatory deny signing the document?

The above all six factors [Shown in figure: 1] motivate for proving high security techniques for information and improvement in existing techniques. [1, 3]

II. HISTORY OF INFORMATION SECURITY

In the starting the information security was followed on basis of computer security. Cryptography security technique can be traced back to ancient times. Mostly ancient civilizations had developed some kind of cryptography. In India ancient people used allusive languages of ancient Egypt, who were using in inscriptions on sarcophaguses to increase the mystery of the place. To protect or providing security for the physical locations, hardware and software from unauthorized and outside threats had started during the second world war as the need of computer security, when the beginning of first mainframes had developed Since the early days of writing, heads of state and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of written correspondence and to have some means of detecting tampering. [4]

The beginning of information security was followed on the basis of history of computer security. To protect the physical location, hardware and software from outside threats had started during the Second World War as the need of computer security, when the first mainframe had developed to aid computations for code breaking, were put to use. Second World War brought about much advancement in information security and marked the beginning of the professional field of information security.

The researcher got attention for security methodology, when department of defense had focused on the security of system sharing within the group during spring and summer of 1967. During this period, the advance research project agency formed a task force for studying the security methodology of protecting all classified information system. The growth of security techniques have been explained in following. [5, 6, 7]

a. In 1968, Maurice Wikes had proposed the concept for information security by password in time sharing computer system.

b. During 1973, Shell, Downey and Popek analyzed about the additional security features in military system by their article “Preliminary Notes on the Design of Secure Military Computer Systems”.

c. Digital Encryption Standards (DES) had examined by Federal Information Processing Standards (FIPS) for the federal register in 1975.

d. During 1978, Bisbey and Hollingworth examined about the protection analysis project created by ARPA for better understanding the vulnerabilities of operating system security and described the possibility detection techniques in existing system software.

e. In 1979, Communication of association computing machinery (ACM) had published the research of Morris and Thompson about the history of a design for a Password security scheme on a remotely accessed time-sharing system. During this period, Dennis Ritchie has given the security concepts for secure user IDs and group IDs and problems inherent in the system, which was related to data-file contents in.

f. In 1984, Grampp and Morris had explained four important concepts for handling the computer security in their research for UNIX operating system security that was physical control of premises and computer facilities management commitment to security objectives, education of employees and administrative procedure aimed at increased security. Another research of Reeds and Weinberger regarding to file security in UNIX by crypto commands had also published in this year. According to them “No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the system administrator or other privileged users”.

g. During 1990s the computer network had started in use commonly. New concepts came in use such as rise to the Internet, the first manifestation of a global network of networks. So because of internet use security issue was challenging for researcher. The close of the twentieth century various security techniques and algorithms had published by different researchers, which have been discussed in next section.

III. RELATED CONCEPTS AND TECHNIQUES

During the end time of twentieth century and early years of the twentieth first century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through a network generically called the Internet or World Wide Web. The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit. The academic disciplines of computer security, information security and information assurance emerged along with numerous professional organizations - all sharing the common goals of ensuring the security and reliability of information systems. [4, 27] The large numbers of cryptographic techniques are used for information security from ancient time to modern time. The major techniques in computing have been described in these following subsections.

A. Cryptographic Encryption Techniques:

Cheap encryption, coupled with signal-hiding techniques (i.e., spread-spectrum and frequency-hopping) could seal the code-breaker's fate [8]. Cryptanalysis is the art and science of recovering the plaintext of an encrypted message without prior access to the key. The Department of Defense (DoD) defines cryptanalysis as "the steps and operations performed in converting encrypted messages into plaintext without initial knowledge of the key employed in the encryption [9]. In the digital age, the art of encryption is about devising ways to hide meaningful text behind walls of random numbers. The so-called "black art of code-breaking" is about finding patterns in that apparent randomness.

B. Symmetric Key Cryptographic Techniques:

Symmetric key (secret key) cryptography [10] is a classical form of cryptography in which the key required for encrypting is the same as the key required for decrypting. In Secret-key systems the key values held by two or more parties are the same, the sender and recipient. The three basic classes of cryptographic algorithms are; first one-key or secret key, also called symmetric key; second two key or public key also called asymmetric key. Both of these systems have their advantages and disadvantages. Secret-key cryptography is faster than public-key cryptography. The third basic category is no-key algorithms, the most common example being cryptographic hash functions, which are computationally irreversible algorithms that are widely used with digital signatures.

Symmetric methods are also known as single key ciphers. There is one key that is used to encrypt and decrypt the plaintext. The key needs to be passed on to the recipient. The legacy U.S. symmetric cryptography algorithm [the Data Encryption Standard (DES)] has been replaced by the Advanced Encryption Standard (AES) [11], an algorithm endorsed by NIST yet of foreign (Belgian) origin. Some United States Government (USG) systems have also replaced DES with classified algorithms.

C. Asymmetric Key Cryptographic Techniques:

Asymmetric key or public key cryptography [12] uses two related keys, which have the property that, given the public key, it is considered computationally infeasible to derive the private key. The key holder has two keys a private key (which only they know) and a public key (which is uploaded to a key server or given to people they want to correspond with). When a person wants to encrypt a message or file, they use the Public key of the recipient to encrypt it. This ensures that only the recipient (or anyone with the private key) can read the message or file. If the sender wants to guarantee that they were the sender, they will use their private key to sign the message (and the recipient will use their public key to verify that it was sent by them).

A public key system is so constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair [13]. In addition to encryption, public-key cryptography can be used to implement digital signature [14] schemes. In digital signature schemes, there are two algorithms: one for *signing*, in which a secret key is used to process the message (or a hash of the message, or both), and one for *verification*, in which the matching public key is used with the message to check the validity of the signature. RSA and DSA are two of the most popular digital signature schemes. Digital signatures are central to the operation of public key infrastructures and many network security schemes (e.g., SSL/TLS, many VPNs, etc.).

D. Embeddable Programmable Cryptographic Processor Techniques:

An embeddable programmable cryptographic processor is a remotely programmable processor chip that can be embedded in information system hardware to allow information (data) to be encrypted/decrypted wherever it is generated or transformed. In 1996, The National Institute for Standards and Technology (NIST) is responsible for the development of cryptographic standards and guidelines for the protection of the sensitive but unclassified information of U.S. federal government departments and agencies. [15] The NIST cryptographic standards and associated guidance is also widely used by defense industry and many other nongovernmental activities, businesses and the financial service industry. Many of the definitions and much of the crypto-logic information in this section is drawn from NIST publications. All of the information contained in this section is derived from public domain research; Internet searches; books, trade journals, technical literature, newspapers and magazines in the public domain and has been compiled for unclassified USG reference purposes.

In the digital age, the art of encryption is about devising ways to hide meaningful text behind walls of random numbers. The so-called "black art of code-breaking" is about finding patterns in that apparent randomness.

E. Wireless Security Techniques:

Secure wireless technology is the collective term for secure radio frequency communication systems. Wireless (RF) technologies use radio transmissions as the means for transmitting data. 'Wireless' in this item includes all: cordless telephones; cell phones; Wireless Wide Area Nets (WWAN); IEEE 802.11b Wireless Local Area Networks (WLAN) or "Wi-Fi" (for Wireless Fidelity) networks; radio, Cellular Digital Packet Data (CDPD); Global System for Mobile Communications, (GSM); and Mobitex. This technology data sheet is intended to cover commercial, modified commercial and wireless systems developed explicitly, or adapted, for military use incorporating low probability of detection (LPD) and resistance to jamming as well as localized jamming and denial service attack resistance required of strictly commercial systems [16].

The major competing wireless technologies for network computing are 802.11b, 802.11g, and Blue Tooth™. All three systems operate in the 2.4 GHz band [17]. These systems are intended for short-range computing and telecommunication applications among low powered devices up to 100 meters apart. The 100 meters is optimistic. The actual effective range is about ¼ of that in most indoor environments. The 802.11b is the most widely distributed and delivers 11 Mbps.

Bluetooth is a more complex standard, with some of the features specified in the Infrared Data Adapter (IrDA) standard [18] that allows unique identification of active devices in the immediate environment. That device identification capability is the basis of ad hoc networking, where each device manages its own information packet traffic. The ad hoc network is defined for a set of devices essentially by configuring them to ignore activity that originates from those not on a list.

F. Quantum key distribution Techniques:

Quantum key distribution (QKD) cryptography is a form of cryptography that exploits quantum theory, in particular the uncertainty principle—which states that it is impossible to measure all aspects of an object with absolute certainty [19]. Quantum key distribution cryptography has reached the point that it is no longer a scientific artifact and is beginning to cross over into the technology phase with companies in at least four countries producing commercial quantum key distribution cryptographic products that are, or soon will be, on the market.

Present quantum key distribution cryptography applications are intended as a communication-encryption technology, not a storage-encryption technology. Quantum cryptography offers some communication-encryption advantages for key management over conventional cryptosystems assuming the requirements for QKD can be met, and may also be the only way to secure communications against the hypothetical power of quantum computers [20, 21]. Quantum key distribution cryptography seeks to guarantee the secure exchange of a random series of bits, which can then be used as the basis for a one-time pad cipher [22].

With quantum methods, if the keys are used as one-time pads, complete security is assured as the collapse of quantum superposition generates truly random keys. This eliminates one of the major drawbacks of using one-time pads, which is the key distribution problem. In addition, the ability to detect the presence of an eavesdropper is an advantage over conventional methods [23, 24]. A group of scientists at Los Alamos National Laboratory in New Mexico has begun to experiment with quantum cryptography in air. Their ultimate aim is to create a quantum cryptographic system that can operate with satellites from ground station satellite command centers. If this can be achieved, it would enable absolutely secure global connectivity for the Command, Control Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4 ISR) systems [25].

IV. CONCLUSION

There are various concepts and encryption techniques have been explained here for the information security. In this technical review paper, we have described the most commonly used encryption techniques, discusses the protections provided by each type, and explains how these technologies are typically managed and tried to show that information security is one of the key hot topics which have an impact throughout an organization. One of the major concerns of any corporate irrespective of its size today is to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution.

The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review. This makes information security an indispensable part of all the business operations across different domains.

V. FUTURE SCOPE

We can define easily that the searching processes for information security have no end. It is outgoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. Today, Information Security professionals are widely sought after in Governments, military, financial institutions, educational institutions, hospitals, and private businesses. This is due to widespread use of Internet and heavy dependent on technology, and the Internet in particular. This leaves companies more exposed to information security threats than ever. In addition, there is increased regulatory focus on this area. To counter threats of increased hacking, many companies implement effective information security systems using methods such as security policies, security products, technologies and procedures. So it is very interesting and challenging work for researcher as well as corporate.

VI. ACKNOWLEDGMENT

First of all we are very grateful to our institutions and management for providing the environment for research work and encourage us for such initiatives.

We wish to express our deep sense of gratitude to Dr. K. Raghavan Nambiar, Prof. (Dr.) P. N Ramachandran, Dr. Zahir Hasan, Dr. Karthikeyan Chittayil, Dr. R. K. Sharma, Dr. R. Sreekumar, Dr. Ajit Singh and Dr. Sanjeev Kumar who gave us inspiration to take up the tasks.

We'd like to thank Prof. Akhilesh Mohan Srivastava and our colleagues for their invaluable suggestions and co-operation during our work.

I am particularly thankful to my all friends, especially Mr. Kranti Patel and Dr. Madhu Nadini Srivastava who have cultivated devotion and determination in me and also motivate and take care me at each step of my life.

In the end, we would like to thank to IJARCS reviewers committee who gave their valuable time for important corrections and helped us for giving final touch to this article.

VII. REFERENCES

[1] Dhiren R. Patel, “Information Security: Theory and Practice”, 2008, PHI, ISBN 978-81-203-3351-2.

[2] Kim Sehun, Moti Yung, and Hyung-Woo Lee, “Information Security Applications”, Springer Lecture Notes in Computer Science, 2007, Vol. 4867 ISBN 978-3-540-77535-5.

[3] Jason Andress, “The basic of Information Security: Understanding the Fundamental of InfoSec Theory and Practice”, Syngress Publications (Imprint of Elsevier), 2011.

[4] J. Pieprzyk, T. hardjono, and J. Seberry, “Fundamental of Computer Security”, Springer-Verlag Berlin Heidelberg New York, 2003.

[5] Bruce Schneier, “Beyond Fear”, Springer-Verlag, New York, 2006.

[6] Donn B. Parker, “Fighting Computer Crime”, Macmillan Library Reference, 1983.

[7] David Kahn, “Seizing the Enigma: The Race to Break the German U-Boats Codes”, 1939–1943 by 1991, Houghton Mifflin.

[8] Libicki, Martin C., “What is Information Warfare?, Center for Advanced Concepts and Technology Institute for National Strategic Studies”, National Defense University, August 1995, p. 32.

[9] The Joint Education and Doctrine Division, J-7, Joint Staff, “DOD Dictionary of Military and Associated Terms”, as amended through 15 November 2012, Joint Publication (JP) 1-02: Department of Defense, USA, Page available at http://www.dtic.mil/doctrine/dod_dictionary/index.html.

[10] Toshinobu Kaneko, “Report on Evaluation of Symmetric Key Cryptographic Techniques”, May 22, 2003, Chair, Symmetric-Key Cryptography Subcommittee (Science University of Tokyo).

[11] Federal Information Processing Standard (FIPS) PUB 197, “Advanced Encryption Standard (AES)”, 26 November 2001.

[12] J. Katz and Y. Lindell, “Introduction to Modern Cryptography”, CRC Press (2007), ISBN 1-58488-551-3.

[13] David Kahn, "Cryptology Goes Public", 58 Foreign Affairs 141, 151 (fall 1979), p. 153.

[14] R. Rivest, A. Shamir, L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, Vol. 21 (2), pp.120–126. 1978.

[15] Information Technology Management Reform Act of 1996 (ITMRA), “Responsibility for Acquisitions of Information Technology”, Federal Information Processing Standards Publications, 1996, (Public Law 104-106).

[16] V. A. Pentagon, “Information Security Technology”, Under Secretary of Defense, Acquisition, Technology and Logistics, April, 2009.

[17] Actual frequency/channel allocation varies by country. November, 2003. Page available at the following link: www.hp.com/rnd/pdfs/country_approvals_matrix520wl.pdf

[18] Charles D. Knutson and Jeffrey M. Brown, “IrDA Principles and Protocols: The IrDA Library”, Vol. 1”, MCL Press, 2004, ISBN 0-9753892-0-3.

[19] Singh, Simon, “The Code Book”, Doubleday, New York, 1999, p. 384.

[20] Black, Paul E., Kuhn, D. Richard and Williams, Carl J., “NIST”, Gaithersburg MD 20899, Quantum Computing and Communications, 2003, paragraph 5.3.

[21] Marvin Zelkowitx, ed., “Quantum Cryptography. In Advances in Computers”, Vol. 56, Academic Press, 2002, pp. 189–244.

[22] Singh, Simon, “The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography”, Doubleday, New York, 1999, p. 321.

[23] Black, Paul E., Kuhn, D. Richard and Williams, Carl J., “NIST”, Gaithersburg MD, 2009.

[24] S. IMRE, and Ferenc B., “Quantum Computing and Communications: An Engineering Approach”, Quantum Cryptography, A Wiley-Interscience Publication, April, 2003, paragraph 5.3.

[25] Singh, Simon, “The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography”, Doubleday, New York, 1999, p. 348

[26] William C. Barker, “Information Security”, NIST Special Publication 800-67, Version 1.1, 2008.

[27] Donald L. Evans, Phillip J. Bond, Arden, and L. Bement, “Security Requirement for Cryptographic Modules”, Federal Information, Processing Standards Publication 140-2, 2001.