ISSN No. 0976-5697

Volume 4, No. 3, March 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Comparative study of Cryptography Algorithms

Manisha Vishwakarma
4th year B.Tech.-ECE
School of Electronics Engineering
VIT University, Vellore-632014

***Abstract*:** The need for improved techniques ensuring secure transmission and storage of information has been ever increasing. This has led to keen interest in the field of cryptography across the globe.The focus of research and development in cryptography has been directed towards meeting security requirements. The essence of this field is the optimal realization of encryption algorithms in software or hardware or a combination of both. Encryption algorithms transform messages by addingsome cryptographic protection, such as confidentiality, authenticity or integrity to them. These algorithms employ one or more keys that are cryptographic variables used to control the algorithm and provide security against attackers. This paper deals with a comparative study of encryption algorithms along with their applications in real world scenario.

Keywords: Cryptography, Encryption, Key, Decryption

I. INTRODUCTION

In traditional telecommunication systems, securing the channel meant securing the messages. With the advent of internet and advancement in packet switching techniques, securing the channel is neither possible nor effective. This increases the importance ofcryptography. Webster defines cryptography as "the enciphering and deciphering of messages in secret code or cipher; also: the computerized encoding and decoding of information" [12]. Cryptography aims at hiding information and making it secure. Whereas, there is another field of study which is concerned with the techniques of defeating such attempts called cryptanalysis.Cryptology is a broad domain which includes both cryptography and cryptanalysis.

Encryption is defined as the process of converting original information which is referred as "plaintext"in cryptographic terms to hidden information called as "ciphertext". This ciphertext is in unreadable form. Decryption is the reverse process

of encryption, which convertsciphertextinto plaintext and makes it readable. As defined in RFC 2828 [18], cryptosystem is "a set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context." Plaintext is converted into ciphertext by means of an encryption engine whose operation is fixed and determinate. Encryption engine function depends on a piece of information (the encryption key) which has a major effect on the output of the encryption process. A cryptosystem is uniquely designed such that decryption can be accomplished only under certain specified conditions, which generally means only by persons in possession of both a decryption engine and a particular piece of information, called the decryption key. These days, generally a computer program comprises the decryption engine.

The encryption key and decryption key may or may not be the same. When these keys are same, the cryptosystem is called a "symmetric key" system; when they are not it is called an "asymmetric key" system. The most familiarexample of a symmetric cryptosystem is the DES (Data Encryption Standard) algorithm whereas the PGP (Pretty Good Privacy) is that of an asymmetric key cryptosystem.

II. GOALS OF CRYPTOGRAPHY

NIST Computer Security Handbook [10] defines computer security as "the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)". Accountability and authenticity are included to give a complete picture. All security systems share a common vision of achieving these five main goals of computer security.

- Confidentiality: It deals with two major aspects namely data confidentiality and privacy. RFC 2828 [18] defines data as "information in a specific physical representation, usually a sequence of symbols that have meaning; especially a representation of information that can be processedorproduced by a computer."
- Integrity: It deals with both data integrity and system integrity. Integrity assures that information has not been altered in any unauthorized manner and that the system has been free from any kind of illicit manipulation.
- Authentication: It directly relates to genuineness.

It ensures validity of information transmission i.e. each message which is sent and received is from a valid source.

CONFERENCE PAPER II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,

Accountability: It is a very crucial security goal to be achieved. It deals with non-repudiation, fault isolation, deterrence and legal action.

Availability: It aims at ensuring information access to authorized users and counters ill effects of Denial-of-Service attacks.

III. CLASSIFICATION OF ENCRYPTION ALGORITHMS

Encryption algorithms can be distinctly classified into different classes on the basis of the transformation employed in these and the keys used.Each class of encryption addresses a different security problem. Based on the secret key used cryptographers broadly classify encryption algorithms as symmetric-encryption algorithms and asymmetric-encryption algorithms.

Symmetric Encryptionuses a single key, therefore, it is also known as single key cryptography or as conventional encryption.

In this class of encryption, the receiver and the sender have to agree upon a single secret (shared) key.Symmetric encryption process produces unintelligible data (called ciphertext) for a given a message (called plaintext) and the key. The ciphertext is about the same length as the plaintext.

In contrast to symmetric encryption, asymmetric Encryptionuses two keys, viz., public key and private key. As the name speaks, public key is known to the public, which is used for encryption. The private key is known only to the intended and is used for decryption.Asymmetric encryption is also called as public key cryptography. The public and the private keys are related to each other by any mathematical means. Thus, data encrypted by one public key can be encrypted only by its corresponding private key.A classic example of asymmetric encryption is the Rivest-Shamir-Adleman (RSA) algorithm. This algorithm is block cipher which previously used a key of length of 512 bits. But, it was claimed to be cracked a decade ago. Now, it employs a key of length 1024 bits.

Another set of protocols which include key-agreement protocols, identification protocols, commitment schemes and zero-knowledge proofs are only briefly mentioned here and not discussed in detailbeing beyond the scope of this study. The key-agreement or key-exchange algorithms are used to manage keys through an exchange of messages resulting from private values that are not shared. The Diffie-Hellman algorithm is the earliest and the most simplest key-agreement algorithm. It also belongs to the class asymmetric encryption algorithms.

Table I: Encryption algorithm classes and their properties

Class	Privacy/ Confidentiality	Integrity	Authentication and Non-repudiation	Key Management	Prior key Agreement
Secret-key or Symmetric-encryption	Yes	No	No	Yes	Yes
Public-key or symmetric-encryption	Yes	No	No	Yes	No
Digital Signature Scheme	No	Yes	Yes	No	No
Key-exchange or management	Yes	No	Optional	Yes	No
Cryptographic hash functions	No	Yes	No	No	No
Authentication codes	No	Yes	Yes	No	Yes

The wide spread use of electronic documents for commercial and private purpose necessitated the need of equivalent of signatures used in paper documents. This led to the development of digital signatures. These meet a somewhat broader requirement that of authentication. These schemes “sign” messages and “verify” the resulting signature with twodifferent keys in such a way that it is difficult to sign without the signing key, thus satisfying need of all parties. They mimic public-key cryptosystems, whereparties need not first agree upon the secret key.

Table-I illustrates different classifications ofencryption algorithms and their properties judging them on various characteristics. The symmetric-encryption algorithms include: AES (Advanced Encryption Standard), 3DES (triple Data Encryption Standard) and DES. Table-II shows comparison of symmetric algorithms basedon 6 major aspects which include the average time characterizing them on the basis of key length and the average time required for exhaustive key search.

Table II: Comparison of Symmetric Encryption Algorithms

Factors	DES	3DES	AES
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Key length (Bits)	56	112, 168	128, 192, 256
Block Size (Bits)	64	64	128, 192, 256
Possible Keys	2^{56}	2^{112}, 2^{168}	2^{128} , 2^{192} , 2^{256}
Time required to check all possible keys at 50 billion keys per second	For a 56-bit key: 400 days	For a 112-bit key: 800 Days	For a 128-bit key: $5x10^{21}$ years
Security	Proven inadequate	the one with 112-bit key is weak	Considered secure

IV. CRYPTOGRAPHY APPLICATIONS

Cryptography has found its application in more than what one can imagine. Major sectors which use cryptographic techniques include defence, government and law enforcement agencies, banking, insurance, business and industry. It has even found its way into sectors like healthcare, education, tourism and social welfare.Cryptography could be applied to text, image, audio and video based scenarios including both real time and non-real time systems.

During the last years, the use of embedded cryptographic processors has spread from low-cost crypto-processors, such as smart cards used for holding decryption keys, to more modern applications, such as user authentication, identity management, e-mail, mobile communication, electronic payment schemes, digital right management and trusted computing Initiative (TCI).

In a special mention here, hash functions are used to create one-way password filespredominantly stored by an operating system.

An operating system could store a hash of password instead of the actual password, thus safeguarding password from a hacker. These can also be used for virus and intrusion detection. A cryptographic hash function can be employed to build a pseudorandom function (PRF) or a pseudorandom number generator (PRNG). A hash-based PRF or PRNG can be potentially be used to generate symmetric keys as well.

Table III summarizes someof the cryptographic classes along with their applications.

Table III: Summary of Cryptographic Applications

Class of Cryptography	Brief Description	Application Area	Example Scenario
Public key Cryptography	Two pairs of keys used: encryption and decryption key	Secure Message Transmission on using Proxy-Signcryption	Low power computers
Public key Cryptography (SSL)	Uses two keys: Public and private key	Certificates and authentication	Password Authentication
Public key Cryptography	Two pairs of keys used: Public and private key	Digital signature and Authentication	Electronic mail
Symmetric key Cryptography	Single key used at both ends	Transferring files	Document files, Message authentication code

ISSN No. 0976-5697

Volume 4, No. 3, March 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

V. CONCLUSION

Security plays a very important role in preserving the integrity of data. And the ever persisting desire to develop a secure system has brought cryptography in the lime light. In this paper a survey on security challenges and cryptographic encryption schemes has been done from different perspectives. The applicability of cryptography in data security has been studied and summarized.

VI. AKNOWLEDGEMENT

I would like to thank my university and my project guide Prof. M. Shanmugasundaram for providing necessary facilities and able guidance in carrying out this work.

VII. REFERENCES

[1] S. Hirani, "Energy Consumption of Encryption schemes in wireless device Thesis", university of Pittsburgh, Apr. 9, 2003,Retrieved Oct.1, 2008.

[2] A. Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.

[3] Ravi, S., Raghunathan, A., Kocher, P., Hattangady, S.: "Security in embedded systems: Design challenges". ACM Transactions on Embedded Computing Systems (TECS) 3 (2004) 461-491

[4] Kocher, P., Lee, R., McGraw, G., Raghunathan, A.: Security as a new dimension in embedded system design. In: Proceedings of the 41st annual Design Automation Conference. DAC '04 (2004) 753{760 Moderator-Ravi, Srivaths.

[5] Kang, K.D., Son, S.H.: Towards security and qos optimization in real-time embedded systems. In: SIGBED Rev. Volume 3., New York, NY, USA, ACM (2006) 29-34

[6] S. Kim, Ingrid Verbauwhede, "AES implementation on 8-bit microcontroller," Department of Electrical Engineering, University of California, Los Angeles, USA, September, 2002.

[7] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES implementation on a grain of sand," IEE Proc. Inf. Security, vol. 152, IEE, pp. 13-20, Oct. 2005.

[8] National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook.* Special publication 800-12. October 1995.

[9] FIP 197: Announcing the Advanced Encryption Standard, Nov. 26,. 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[10] http://www.merriam-webster.com/dictionary/cryptography

[11] G. Bertoni, L. Breveglieri, P. Fragneto, M. Macchetti and S. Marchesin, "Efficient Software Implementation of AES on 32-bit Platforms," *CHES 2002, LNCS 2523*, pp. 159–171, 2003.

[12] X. Zhang and K. K. Parhi: "High-Speed VLSI Architectures forthe AES Algorithm", *IEEE Transactions on VLSI Systems*, vol.12, Issue 9, pp. 957-967, Sept.2004

[13] S. Tillich, J. Großsch¨adl and A. Szekely, "An Instruction Set Extension for Fast and Memory-Efficient AES Implementation," *J.Dittmann, CMS 2005, LNCS 3677*, pp. 11–21, 2005.

[14] K. Nadehara, M. Ikekawa and I. Kuroda, "Extended Instructions for the AES cryptography and their Efficient Implementation," *Signal Processing Systems*

[15] G. Bertoni, L. Breveglieri, P. Fragneto, M. Macchetti, and S. Marchesin. "Efficient Software Implementation of AES on 32-Bit Platforms". In B. S. K. Jr., C¸ etin Kaya Ko¸c, and C. Paar, editors, Cryptographic Hardware and Embedded Systems - CHES 2002, volume 2523 of Lecture Notes in Computer Science, pages 159–171. Springer, Berlin, Aug. 2002.

[16] http://www.ietf.org/rfc/rfc2828.txt

[17] Hamdan.O.Alanazi, B.B.Zaidan, .A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani"New Comparative Study Between DES, 3DES and AESwithin Nine Factors", Journal Of Computing, Volume 2, Issue 3, march 2010, ISSN 2151-9617

[18] Burt Kaliski, "A Survey of Encryption Standards", IEEE Micro, 13 (6) 1993, 74-81.