This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference.

A Survey on Current Key Issues and Status in Cryptography

M. Guru Vimal Kumar
Department of EIE
Kongu Engineering College
Perundurai, Erode,
guruvimal22@gmail.com

U.S. Ragupathy
Department of EIE
Kongu Engineering College
Perundurai, Erode,
ragupathy.us@gmail.com

***Abstract*—Internet applications are increased and growing at very fast. Owing towards the technological development, secured way of data transmission over the internet is becoming a questioning task. Intruders hack the data and use it for their beneficial purpose. To avoid these undesirable acts, cryptography is used to ensure security of the covert and secure message. Although encrypted data is difficult to decipher, it is relatively easy to detect. Strong encryption algorithms and proper key management techniques for the systems will helps in achieving confidentiality, authentication and integrity of data. In this research work various encryption (symmetric and asymmetric) algorithms have been studied. Literature Survey has been carried out for cryptography by incorporating key papers related to data encryption based on performance metrics (Security and Time constraints). From this, the observation and future work has been identified.**

***Index Terms*— Cryptography, Symmetric Algorithm, Asymmetric Algorithm, Performance metrics**

I. Introduction

The volume of data is exploding and complexity of data is growing. Above 93% of all data is born digital. The amount of information added annually to the digital universe was about 988 EB (almost 1ZB). The digital universe will have 50 fold growths from beginning of 2010 to the end of 2020. The various information are collected from the sources like books, eBooks, images, journals, research publications, government documents, databases, etc. So, there is a need for securing these sources and applications. Data security is one of the essential components of an organization to keep the information safe from various organization competitors. It will help to ensure the privacy of user personal information from others who are accessing. Time and securely transmission of data is always an important aspect for all organizations. Security of the system is classified in two main types as shown in Fig.1 below.

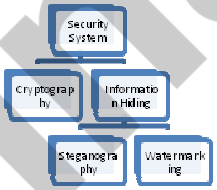

Fig.1. Security Sustem Types

Cryptography plays a major role in protecting the secret information in various applications. Information security is one of an important area of research under cryptography. The applications such as e-banking, ecommerce, medical databases, e-mail, and some more, all of them require the exchange of private confidential information. Military secret message is used to protect the National Security in military application. These are some of the applications involved. Cryptography and steganography are closely related concepts. Cryptography is secret writing and steganography is about hidden writing. Watermarking is other data hiding method similar to steganography.

A. Cryptography goals

Cryptography has some goals. These goals can be either achieve all at the same time in one application, or only one of them in one application. These goals are:

1. Authentication: To prove their own identities. Example: Login access.

2. Confidentiality: This ensures that nobody can understand the received message except the one who has the decipher key.

3. Data Integrity: The receiver receives message which has not been modified or altered from its original form.

4. Non-Repudiation: Prove that the sender sent this message, and the message was received by the specified person, so the recipient cannot claim that the message was not sent [20].

5. Access Control: Process of preventing an unauthorized use of resources. This goal controls who can have access to the resources, if one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

B. General Model and Fundamental Concepts

Cryptology: The field of both cryptography and cryptanalysis is called cryptology [20].

Cryptography: It is the transformation of readable and understandable data into another form which cannot be understood in order to secure data. A cryptography is a Greek word. "Kryptos" means hidden, and "graphikos" which means writing.

Crypto Analyst (Cryptanalyst): A person who is an expert in analyzing and breaking codes.

978-1-4673-9338-6/16/$31.00 ©2016 IEEE

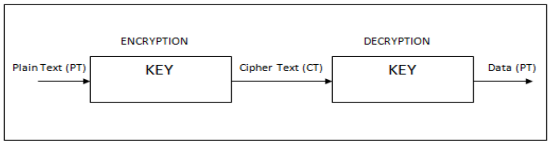

Fig.2. Model for Cryptography

Computer security: A set of tools are used to protect any data from intruders/hackers, theft, corruption, or natural disaster while allowing these data to be available to the users at the same time. One example of these tools is the Kaspersky antivirus program [20].

Network security: It refers to any activity designed with some goals like integrity, confidentiality and protecting the data during their transmission on a network.

Information security: It is about how to prevent attacks, and to detect attacks on information-based systems [20]. Fig.2 explains about the general model for cryptography.

Plaintext: Original text message which has to be encrypted.

Cipher text: Encrypted text message.

Key: It is a word or value that is used for encrypting the plain text or decrypts the cipher text [20].

Encryption: The method of converting the data into other coded form with the help of key

Decryption: A method of transforming the encrypted data to the original form with the help of key.

Section 2 discusses the literature survey. Section 3 introduces the cryptographic types. Section 4 discusses the observations. Section 5 & 6 will be future direction and conclusion

II. Literature Survey

This section discusses about the literature survey on some following papers in cryptography.

Martin E. Hellman [13] extended the shannon theory approach to cryptography. He discussed about Shannon's random cipher model was conservative than in such case when a randomly chosen cipher was considered, the security of model falls significantly. The limitation of this approach is that it is not directly applicable to designing practical cryptographic systems.

H. C. Williams [7] modified RSA public-key encryption algorithm. His opinion is, if the encrypting message procedure was broken into a certain operations than remainder used as modulus could be factored after few more operations. This technique was in similar appearance to RSA. The main limitation of this scheme was that very large prime numbers were used and generated mathematical errors were observed

Taher Elgamal [18] extended a signature scheme based on discrete logarithms and implemented public key cryptosystem achieved by Diffie-Hellman key distribution scheme. Computing discrete logarithms over finite fields faces the difficulty in security of both systems.

Adam J. Elbirt et al. [1] evaluated the AES block cipher algorithm using FPGA based kit and proposed reprogrammable devices (FPGAs). Hardware implementations of encryption algorithms are highly attractive options.

Haowen Chan et al. [6] worked on key pre-distribution scheme randomly used for WSN. a) There was a trade off for the unlikeliest of a large-scale network attack in order to significantly strengthen random key redistributions strength against smaller-scale attacks by q-composite keys scheme.

Chih-pin Su et al. [4] designed an AES processor which has high-throughput and low cost. They proposed effective implementation of hardware of the AES with key expansion capability.

Stefan Mangard et al. [17] proposed highly scalable and regular hardware architecture for AES which was suited for full-custom as well as for design flows of semicustom. This architecture was scalable in terms of throughput, used key sizes. Similarities of encryption and decryption were utilized for high level of performance by using only a relatively small area.

Hung-Yu Chien [8] presented time bound hierarchical key assignment scheme which is an efficient. New time-bound key assignment scheme is proposed by them for a tamper-resistant device. It improves significantly the computational performance and reduces the cost of implementation.

Ho Won Kim *et al.* [9] designed and implemented a asymmetric key crypto processor and its application to a Securing a System. For the execution of cryptography algorithms, a special-purpose microprocessor was optimized. This crypto processor could be used for various security applications such as storage devices, embedded systems, network routers, security gateways using IP Sec and SSL protocol, etc.

Hung-Min Sun *et al.* [10] proposed dual RSA algorithm and also analyzed the security of the algorithm. They presented new variants of RSA whose key generation algorithms output two distinct RSA key pairs having the same public and private exponent's two applications for Dual RSA were blind signatures and authentication. The security of Dual RSA was raised in comparison to RSA when there were values of e and d is small. The main disadvantage of using dual RSA was that the computational complexity of the generation of key algorithms is increased.

Jason H. Li *et al.* [11] worked on key management which is scalable and clustering scheme on communications in *Adhoc* for secure group and WSN. They describe scalable key management and clustering to achieve more secured system. The scalability problem was solved in communicating devices by partitioning into subgroups with a leader in each subgroup. This scheme was not suitable for large cluster size.

Elisa Bertino [5] worked on the approaches, concepts, and challenges on database security. Relevant summarizes the most well-known techniques and concepts underlying the notion of database security were also discussed which was focused on access control systems. The major limitation was that a new device needs to be issued,when an individual user wants to change the subscription.

Spyros T. Halkidis *et al.* [16] analyzed the architectural risk on security patterns for software systems. The step was to determine to what extent specific security patterns shield from known attacks. In this way detection can be done for security problems at an early stage that reduces the cost which compared during implementation on the introduction of security.

Aqeel Khalique *et al.* [2] worked on ECC Using Smart Cards for a password authenticated key agreement scheme. A public key technique has small key size and high security is best. It is also mainly for securing access of smart cards due to smart cards implementations.

Mao-Yin Wang *et al.* [14] configured for flexible security, a single and multi-core AES architectures. According to them the major building blocks for the architecture of AES were a number of AES processors. A block cipher schemes with a novel key expansion design approach by each AES processor is provided for the original AES algorithm.

Chong Hee Kim [3] developed differential fault analysis on AES key schedule and proposed advanced encryption standard for which the main target is known DFA. The major problem was that if the key is not scheduled properly, again for re computation then it cannot prevent DFA on the AES Key Schedule.

Tomasz Rams *et al.* [19] surveyed a key distribution by group scheme with the self-healing property. They analyzed, compared by looking at the selective key distribution algorithms for the most significant key distribution schemes. Limitation of the this techniques is to the broadcast message so as to allow user nodes to recover previous session keys which were lost due to communication errors due to adding some redundant information

A. Performance Metrics

Performance metrics and criteria for cryptographic research are security and time. The algorithms should perform the encryption and decryption of the input text/other multimedia file. For that some of the parameters and measures are to be considered. They are encryption computation time, decryption computation time, encryption, decryption security keys and block size.

First the performance is analyzed based on time and has some parameters. Such as,

- Data types
- Data size
- Data density
- Encryption Time
- Decryption Time

Data types: Data type represents the encoding of the files and has various data types files. Common examples are as follows:

- Text: ANSI, UNICODE-16, UNICODE- 32 bit little and UNICODE-Big Endian, UTF-8.
- Images: TIFF, JPEG, GIF, PNG, BMP.
- Audio: MP3, M4A, MP4, WAV, WMA, AIFF.
- Video: MOV, AVI, MP4, WMV, MPEG, GIF.
- Others: Medical Informatics Standard i.e. DICOM (Images/Binary + Text), HL7 etc.

Data Size: The space occupied by the file on a disk. The video and audio files will generally take more space on disk than textual files.

Data Density: The amount of different information present in the data. If the information is more, the dense will be the data and if the information is less, sparse is the data.

Encryption Time: Time taken to encrypt the data from plain text to cipher text. It is used to calculate Encryption Throughput.

Encryption Throughput (Kb/sec) = □ Input File Size/□ Encryption Execution Time

Decryption Time: Time taken to decrypt the data. It is used to calculate Decryption Throughput.

Decryption Throughput (Kb/sec) = □ Input File Size/□ Decryption Execution Time

Secondly, the security of various cryptographic algorithm are analysed based on some parameters. They are,

- Key size
- Cipher block modes

Key size: A size of the key which is measured in bits and will depend on algorithm. For example DES is having key sizes 56 bits.

Cipher Block Modes: In cryptography, block cipher mode for a block cipher algorithm indicates how cipher text blocks are encrypted from plaintext blocks and vice versa. Commonly used block cipher modes of operations are Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR).

B. Cryptographic Attacks

Basically there are two types of attack. One attack takes place on system and other attack takes place on data is shown in the Fig.3. Attacks classified into active and passive attacks which are of system attacks based on practical approaches.

System Attacks:

In general there is a flow of information from a source to a destination. The attacks will takes place on the flow of information are known as system attacks.

Interruption: An attack on availability of the resource. When the data flows through source to destination becomes unavailable.

Interception: An attack on the confidentiality of the system. In this attack an unauthorized party also has the access to a model. A person, program and a computer may be the unauthorized party [20].

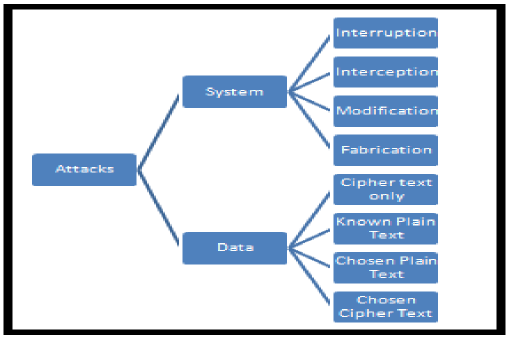

Fig.3-Attacks Types

Modification: An attack on integrity of the system. In this attack an unauthorized party not only has the access to an asset but has the power to modify it.

Fabrication: An attack on authenticity of the system.

Data Attacks:

Attempt made by crypto analysis is known as an attack. The level of information that decoder is able to extract from the cryptosystem and can be divided into five ways of decryption which are as follows:

Cipher text only attack: By knowing the cipher text for collected messages, which are encrypted by same encryption algorithm. Then job is to recover the key or the plain text. In other part on decryption, encrypted message will be decrypted based on same keys.

Known Plaintext attack: Cryptanalysts seek the possession of pairs of known plain text and cipher text. Then purpose is to hold the key used to encrypt the messages or an algorithm to decrypt messages

Chosen Plaintext Attack (CPA): Cryptanalyst not only keeps the cipher text, they also hold in some parts of the chosen plain text [20].

Chosen cipher text attack (CCA): In this crypto analyst hold the possession of chosen cipher text and plain text being decrypted from the private key.

Cipher Block Modes

An intruder will be able to get much information knowing a distribution of identical message parts, even if he would not be able to break the cipher and discover original messages. There are ways to blur and mix plaintext blocks (which are known) with cipher text blocks (which are created). They can prevent many identical output cipher text blocks. These methods are called the block cipher modes of operations.

III. Cryptographic Types

Cryptography is basically divided into two mechanisms.
a) Symmetric Cryptography, b) Asymmetric Cryptography.

A. Symmetric Encryption

A single key (same key) is used for encrypting and decrypting the message. There are some Symmetric algorithms, such as DES, 3DES, AES, RC2, RC6. Table-1 explains various symmetric algorithms.

a) Data Encryption Standard (DES)

IBM developed the DES but was later US Government adopted as a National Standard. It divides the original message into 64-bit blocks. Each block is then permutated to change the order of its bits. Two 28-bit halves is divided by 56-bit key.. Each half is than circular-shirted to the left, reconnected and enlarged to 48 bits. Then the half in right plaintext blocks is also expanded to 48-bits.

b) Triple Data Encryption Standard (3DES)

Triple DES goes through 3 iteration of DES effectively encrypting data with a 168-bit key which is very strong for securing the sensitive message [20]. The 56-bit DES key used for encrypting the data first, then another 56-bit DES key is for decrypting, and finally the original 56-bit DES key is used for encrypting again. 3 DES contains several levels of encryption and it can better protect against middle attacks.

c) Advanced Encryption Standard (AES)

AES algorithm uses 128 bits block size. Depending on size of the key, the standard name is modified to AES-128, AES-192 or AES- 256 correspondingly. A key length is dependent on number of AES parameters. For example, if the key size used is 192, the number of rounds is 12 whereas it is 14 for 256 bits respectively.

It is noted that, if there is a longer keys, it is difficult to crack, but it will take more time for computation.

B. ASymmetric Encryption

There are two keys are used for encryption and decryption of message. There are some asymmetric algorithms, such as Rivest Shamir Adleman (RSA), Diffie- Hellman, Digital Signature Algorithm (DSA).

The public cryptography is an encryption process and decryption process where two different keys are involved. There exist two keys, a) private key, and b) public key. Anyone may have access to the public key but the private key is kept secret. Few common types of asymmetric encryption are briefly explained below

Diffie - Hellman Algorithm

Diffie–Hellman Algorithm is one of the specific method of exchanging cryptographic keys proposed in 1976. It passes sender and receiver that have no prior idea of each other to jointly establish a shared secret key over an unsecured communications channel.

RSA

RSA algorithm was designed by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT. It has two keys (public and private). Both private and public keys will be used for encryption and decryption process. Sender will encrypts the data using receiver's public key and then receiver will decrypt the data using his own private key. It uses two prime numbers for generating private key and public key. The security of RSA depends on the product of these two numbers which is represented by n.

Digital Signature Algorithm (DSA)

It is a public key cryptographic algorithm designed for authenticating digital message. A data is signed by a secret key to produce a signature, and then this is verified against the message by a public key. Any party can verify the signatures but only one party with the secret key can sign the messages

IV. Observations

The following observations have been identified from the previous sections,

1) Short length single key is not capable to provide secured cryptographic model and long length key can be able to provide secured cryptographic model.

2) Asymmetric keys are used and preferred for high level security.

3) There should be a proper key arrangement in order to achieve secure cryptographic model.

TABLE I. SYMMETRIC ALGORITHM SPECIFICATIONS

Symmetric Algorithms	Rounds	Key Size	Block Modes
RC2	18	40 and 64-bit keys	ECB, CBC, CFB, OFB, CTR
RC4	256	1 to 256-bit keys	Stream Cipher
RC5	256	0 to 2040-bit keys	ECB, CBC, CFB, OFB, CTR
RC6	14	192, 256-bit keys	CBC, ECB, CFB, OFB, CTR
Blowfish	16	32 to 448-bit keys	ECB, CBC, CFB, OFB, CTR

V. FUTURE DIRECTION

Security of cipher algorithm varies according to the block cipher modes. Different block cipher modes are used for different applications. Security levels may differ according to type of application and can be classified as:

High: In some applications security matters the most than speed of encryption, like data related to National Security in Military communications (Defense Application) and health etc.

Medium: In some applications where speed of encryption and security both are important. For example, Social Networking application, chatting etc.

Low: In some applications speed of encryption more important than security, like securing data on personal systems or data transfer within an organization which will have no adverse effect on operation of organization if leaked.

Block Size- if the block size is larger, then greater will be security and there is a reduction in encryption/decryption speed.

Key Size- if the key size is larger, then greater will be security and there is a reduction in encryption/decryption speed.

Number of Rounds- Multiple rounds increases the complexity and security.

There is also another problem of data loss. To prevent this data loss during transmission and to promote faster transmission, many different compression algorithms are used to reduce the size of the data. Usually lossless compression algorithms are preferred for recovery of original and all data present without any loss before going for encryption.

Selection of best encryption algorithm in terms of performance such as security and time constraints should be developed in future.

The compression algorithm should be performed before encryption so the data will be in reduced form.

VI. CONCLUSION

In this survey paper, the discussions are made for some of the basic concepts in cryptography, performance metrics and some of the important parameters that are used in cryptography. From these earlier survey papers presented, there are some of the important points which contribute to cryptography system such as key selection for security and encryption, decryption process are relatively less investigated. Hence this survey paper is focused on such issues. Symmetric and Asymmetric types are discussed in brief. These are all some different approaches to secure the system to achieve high level of security. Some of the attacks are also been discussed. Thus by selecting a suitable encryption algorithm will result in secured information system that may defeat several attacks.

REFERENCES

[1] A. J. Elbirt, W. Yip, B. Chetwynd and C. Paar, "An FPGA Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists", *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 9, No. 4, pp. 545-557, 2001.

[2] A. Khalique, K. Singh and S. Sood, " A Password-Authenticated Key Agreement Scheme Based on ECC Using Smart Cards*", International Journal of Computer Applications*, Vol. 2, No.3, pp. 26-30, 2010.

[3] C. H. Kim, "Improved Differential Fault Analysis on AES Key Schedule", *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 1, pp. 41-50, 2012.

[4] C. P. Su, T. F. Lin, C. T. Huang and C. W. Wu, "A High-Throughput Low Cost AES Processor", *IEEE Communications Magazine*, Vol. 41, No. 12, pp. 86-91, 2003

[5] E. Bertino, N. Shang and S. S. Wagstaff, "An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting", *IEEE Transactions on Dependable and Secure Computing,* Vol. 5, No. 2, pp. 65-70, 2008.

[6] H. Chan, A. Perrig and D. Song, "Random Key Pre-distribution Schemes for Sensor Networks", *Proceedings of the IEEE Symposium on Security and Privacy- SP '03*, California, USA, 11-14 May, 2003, pp. 197-213

[7] H. C. Williams, "A Modification of the RSA Public-Key Encryption Procedure", *IEEE Transactions on Information Theory*, Vol. 26, No. 6, pp. 726-729, 1980

[8] H. Chien, "Efficient Time-Bound Hierarchical Key Assignment Scheme", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 16, No. 10, pp. 1301-1304, 2004.

[9] H. W. Kim and S. Lee, "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System", *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 1, pp. 214-224, 2004.

[10] H. M. Sun, M. E. Wu, W. C. Ting, and M. J. Hinek, "Dual RSA and Its Security Analysis", *IEEE Transactions on Information Theory*, Vol. 53, No. 8, pp. 2922- 2933, 2007.

[11] Jason H. Li, B. Bhattacharjee, M. Yu and Levy, "A Scalable Key Management and Clustering Scheme for Wireless Adhoc and Sensor Networks", *Journal of Future Generation Computer Systems*, *Elsevier Science Publishers*, Vol. 24, pp. 860-869, 2008.

[12] J. T. Park, J. W. Nah and W. H. Lee, "Dynamic Path Management with Resilience Constraints under Multiple Link Failures in MPLS/GMPLS Networks", *IEEE Transactions on Dependable and Secure Computing*, Vol. 5, No. 3, pp. 143-154, 2008.

[13] M. E. Hellman, "An Extension of the Shannon Theory Approach to Cryptography", *IEEE Transactions on Information Theory*, Vol. 23, No. 3, pp. 289-294, 1977.

[14] M. Y. Wang, C. P. Su, C. L. Horng, C.W. Wu and C. T. Huang, "Single and Multicore Configurable AES Architectures for Flexible Security", *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 18, No. 4, pp. 541-552, 2010.

[15] R. L. Rivest, A. Shamir and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, *Communications of the ACM Magazine*, Vol. 21, No. 2, pp. 120-126, 1978.

[16] S. T. Halkidis, Nikolaos Tsantalis and Alexander Chatzigeorgiou, “Architectural Risk Anaylisis of Software Systems Based on Security Patterns”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 5, No. 3, pp. 129-142, 2008.

[17] S. Mangard, M. Aigner and S. Dominikus, “A Highly Regular and Scalable AES Hardware Architecture”, *IEEE Transactions on Computers*, Vol. 52, No. 4, pp. 483- 491, 2003.

[18] T. Elgamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, *IEEE Transactions on Information Theory*, Vol. 31, No. 4, pp. 469-472, 1985.

[19] T. Rams and P. Pacyna, “A Survey of Group Key Distribution Schemes With Self- Healing Property”, *IEEE Communications Surveys and Tutorials*, Vol. 15, No. 2, pp. 820-842, 2013.

[20] W.Stallings, “*Cryptography and Network Security*”, 2nd Edition, Prentice Hall, 1999.