Proceedings of the SMART–2020, IEEE Conference ID: 50582
9th International Conference on System Modeling & Advancement in Research Trends, 4th–5th, December, 2020
Faculty of Engineering & Computing Sciences, Teerthanker Mahaveer University, Moradabad, India

Review and Analysis of Cryptography Techniques

Samya Al Busafi[1] and Basant Kumar[2]
[1]Deptt. of Comp SC, Modern College of Business & SC, Sultanate of Oman
[2]Deptt. of Comp SC, Modern college of Business & Science, Sultanate of Oman
E-mail: [1]20189264@mcbs.edu.om, [2]basant@mcbs.edu.om

2020 9th International Conference System Modeling and Advancement in Research Trends (SMART) | 978-1-7281-8908-6/20/$31.00 ©2020 IEEE | DOI: 10.1109/SMART50582.2020.9336792

***Abstract*—Recently, there has been a significant increase in the number of Internet users. Thus, digital data has occupied the highest rank in our time, because most companies and governments adopt the total dependence for the transmission of their data transactions with customers and banking transactions over the World Wide Web. Therefore, total reliance on digital data needs to secure this data and preserve it from theft and modification in order to reach the intended user intact without distortion, and this is done by securing this data using encryption with its various techniques. There are many technologies that encrypt the data sent to the receiving party called encryption techniques. This research will examine the analysis of different encryption techniques, for example, symmetric cryptography technique and asymmetric cryptography techniques, Rivest Shamir and Adleman, Diffie-Hellman, Digital Signature Algorithm, (ECC) Elliptic curve cryptography, and how can employ them and explore the best methods of cryptography techniques that give complete confidential and transmitted data.**

Keywords: Encryption, RSA, Diffie-Hellman, DES, ECC, AES, Blowfish

I. Introduction

There is a lot of information and data in our world that is transmitted through communication channels or e-mail, and in various forms. Examples of this data are pictures, videos, or personal data. Once the data is sent from a phone or laptop to the recipient on the website, this data may be stolen or changed by another party. And that, through the use of modern applications that are developing day by day, and therefore with the increase in the amount of data sent via e-mail or taken from the web, there is no guarantee that it is the correct data.

There is only one thing that helps the sender to ensure that the data sent is seen only by the intended recipient, using their encryption techniques that make the data saved from the tampering of others. Therefore, cryptography is a technique used to investigate data security. Therefore, encryption techniques are used to secure the appropriate transfer of data, and among them are the use of symmetric and asymmetric encryption techniques.

II. Cryptography Objectives

There are four objectives and goals of Cryptography use to achieve it such as [1][2]:

1. *Confidentiality:* protect user identity and privacy of data from being read by others [3].
2. *Integrity's:* that data protection from being changed by others [3].
3. *Authentication:* To ensure that the data comes from a specific party [3].
4. *Non-repudiation:* Preventing a specific party from denying sending a message [3].

III. Terms Of Encryption & Decryption Technique

There are some terms need to define it before doing Encryption & Decryption of Cryptography, such as [3]:

- Plaintext -> is the original text that which can be read and understood.
- Encryption -> is the method which use to hide the plain text to get an incomprehensible text.
- Ciphertext -> is encrypted plaintext encoded the original text.
- Decryption -> is the method which use to get the original plain text form from the Ciphertext [3].

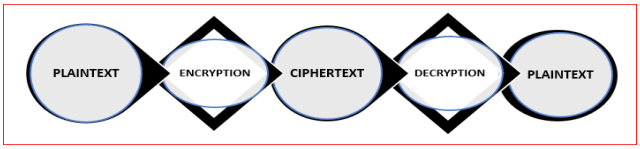

Fig. 1: Terms of Encryption & Decryption Technique

IV. Types of Cryptography

Cryptography splatted in to Two types as:

A. First Type: Symmetric Key Cryptography

It's one of the Cryptography techniques which use only single & the similar key that use to perform the encryption algorithm and decryption algorithm. Its known secret key encryption[4] [5].

B. Divided Into Two Types

The Block cipher: which deals with group of data, example of it are [6]:

- (DES) Data Encryption Standard [7].
- (3DES) or called as Triple Data Encryption Standard [7].
- (AES) Advanced Encryption Standard.
- Blowfish [7].

The Stream ciphers: which deals with data as single bite at a time, and example of it is RC4 [8].

C. How it's Work

It uses same Private key between sender and receiver, that key must be shared before the transmission occurs. It should follow specific roles to make secure transaction on encryption and decryption, as below roles:

- Should not use weak key that make easily data access by an unauthorized user.
- Should use strength key encryption that by choosing big size of the key that make it difficult to decrypt it [4].

1) Example

If the Original message need to send it to receiver is "HOW ARE YOU?"

Sender do encrypt the message => HOW ARE YOU? by using shared key which is shift value integer = 3, then get the decryption text => RYG KBO IYE?

Receiver once received the message do decryption to get the original message by using same shared key.

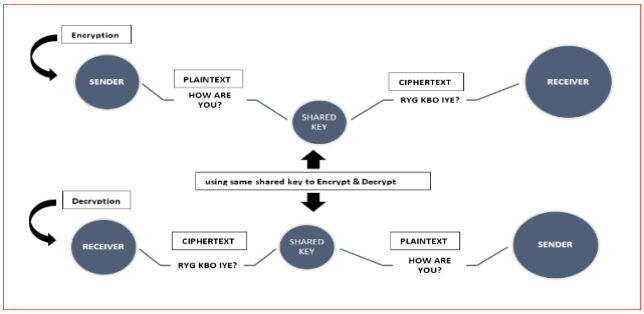

Fig. 2: How Symmetric Cryptography Work

D. Advantages & Disadvantages

Advantages of Symmetric Key Cryptography:

- Using one single & same key for encrypt and decrypt data.
- It easy and faster than A Symmetric Cryptography.
- It has Low cost.

Disadvantages of Symmetric Key Cryptography:

- Shared key must be stored in a secure location to be accessible for sender and receiver due to using same key, and that give chance to attacked.
- To transfer the Key should use a secure channel.
- regularly must change the keys.
- Easy dismantling
- It does not include blanks.
- Limited in the languages which covers.

E. Second Type: Asymmetric Key Cryptography

The second type of encryption technique uses two pair of keys, one use for encryption the plain text and the second for decrypt the cipher text. It is known as public key encryption [4].

F. Divided into Four Types

Thus, different Researchers divide asymmetric cryptography techniques in to commonly use types as [9] [3]:

- (RSA) Rivest Shamir and Adleman.
- Diffie Hellman.
- (ECC) Elliptic Curve Cryptography.
- (DSA) Digital Signature Algorithm.

G. How it's Work

It uses two pair keys one PUBLIC key[10] and the other one PRIVATE key for both the sender and receiver. During transaction use public key which known between sender and receiver. The private key must keep secret for each. Thus, sender send the message to receiver by using public key of the receiver once the message received by the intended receiver do the decryption by use of receiver private key and vice averse [11].

Should know at least one of the keys. impossible to decipher a message if not available any of the information.

H. Advantages & Disadvantages

Advantages of A Symmetric key cryptography technique:

By using pairs of the keys for encoding and decoding data that eliminate the key distribution problem.

- It uses standards for encryption.
- Increased security and make it stronger and less susceptible to penetration because there is no transfer of private keys to anyone.
- By using of the digital signatures give the verification that message which received it comes from specific sender.

Disadvantages of A Symmetric Key Cryptography [3]:

- It not suitable method to decode the bulk messages due to the slowness on processing compared to symmetric Cryptography.
- it Cannot decrypt the messages of an individual receives if loses private key.

1) Example

When Ahmed want to send message "HOW ARE YOU?" to Ibrahim he will use public key of Ibrahim to encrypt that message which received by Ibrahim as decrypted text => RYG KBO IYE?

Once Ibrahim received the message that which will decode the message by use of his Private key to get the original message text as => HOW ARE YOU?

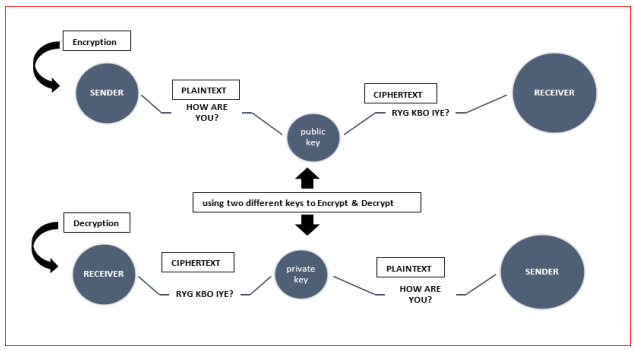

Fig. 3: How A Symmetric Cryptography Work

Table 1: Comparative between Symmetric Key Cryptography and a Symmetric Key Cryptography [4]

Comparative Points		Symmetric Key Cryptography
Features	No. of Key use	use only one single key
	Name of the key	secret key
	Criteria of the chosen key	Should not use weak key. The strength of the key by choosing a big size and increase the No. Of rounds.
	keys length	128-bit [6].
How its work	Step one	first need to be Shared the secret key among sender and receiver before the transmission occurs.
	Step two	sender encode the message by use of the Shared key to Incomprehensibly text then it is sent over a network to the intended receiver.
	Step three	once the encrypted message reach to the receiver use the same shard key that use to decode the message to understandable form and that be the plain message.
Types		DES 3DES AES Blowfish RC4
Advantages		Easy and faster It has Low cost.
Disadvantages		regularly must change the keys. Easy dismantling It does not include blanks.
Complexity		Easy and not complicated

Comparative Points		A Symmetric Key Cryptography
Features	No. of Key use	use two different keys
	Name of the key	public key. private key.
	Criteria of the chosen key	Should not use weak key. The strength of the key by choosing a big size and increase the No. Of rounds.
	keys length	2048-bit
How its work	Step one	At the beginning of the transaction, the sender and receiver should know the public key for everyone.
	Step two	Then once sender gets the Public key of the Receiver, use it to encode the plain text using the Public key of the receiver to get the encrypted text (ciphertext).
	Step three	Then sender sends the generated ciphertext to the receiver. Finally, receiver decode the ciphertext with its Private key and returns it to the original text.
Types		rivest shamir and adleman (RSA) Diffie-Hellman, Elliptic Curve Cryptography (ECC) digital signature algorithm. (DSA)
Advantages		Eliminate the key distribution problem. uses standards for encryption. Increased security and make it less susceptible to penetration use of digital signatures.
Disadvantages		Slower than Symmetric Cryptography. it Cannot decrypt the messages of an individual receives if loses private key.
Complexity		Rather complicated

V. Analyses of Different Cryptography Techniques

In the coming lines of this research paper, will go deeply on the Cryptography Techniques by analysing them according to what was included in the previous various research papers in the relevant journals.

A. Rivest Shamir and Adleman (RSA) [12][13]

The mostly frequent used of Asymmetric cryptography is RSA algorithm. Widely used in a communications security. That due to the security of RSA which derives in the complex difficulty calculation of integer factors that are the result of two large prime numbers [9][4].

To fined the product of Multiplying two large primes is very easy, but the difficulty is in determining what are the original factors that are security of public key encryption [14].

As Ravi K Sheth and Sarika P.Patel divided RSA algorithm on their paper in to three steps as [9]:

1. key generations 2. Encryption and 3. Decryption.

Basically, RSA Algorithm given as below points [15].

First: To get the value of public key K_p by below steps [1]:

a. Selected P and Q which are the two primes number.
b. Apply the primes P and Q on the following formula to get the value of x=(P-1)*(Q-1)
c. gives value of E which is the relative to Primes numbers to x that should satisfied the condition for K_s
d. fine the value of N=P*Q
e. As known K_p is N is the concatenated number with E.

Second: To get the value of private key:

a. give value for D by using following formula => D*E mod x=1
b. As known K_s is N is the concatenated number with E.

In case need to encrypt the plain text M by the following:

a. Suppose a value of M is number
b. To calculate the cyphertext by use of $C=M^E$ MOD N

In case need to decode the cyphertext C to get the original text M by using:

a. Do the calculate M= CD mod N.

Almost all previous researchers agreed that to calculate of the RSA need to follow specific points, according to them order as

1. the value of Ø (1) = 0
2. to get value of Phi and if the prime number is p, use the following formula => Ø (p) = p – 1
3. if the selective m and n as relative prime number, to get value of phi required to use the following equation as Ø (m*n)=Ø (m)* Ø (n)

4. if select p as prime number and have phi and e, suppose to use the following formula Ø (pe) =pe –pe-1
5. not necessary to know all the secret parameters p,q and Ø (n) by user.
6. M<N has the positive integer form of the plain text M.
7. As security case user can authenticate the communication by using his private key.
8. the facility of digital signature provided by RSA cryptosystem.
9. RSA cryptosystem uses public key technique for Encryption, Decryption that which followed by all of the hardware & software products [1].

B. Diffie-Hellman Algorithm

The concept of the Diffie-Hellman algorithm applies between two users that they use to exchange cryptographic keys, and not all of these users know the key that the other party used [3] [5].

There is a secret key shared between the two parties and is used via an insecure communication channel, and then used it for subsequent communications to be encrypted using a symmetric key encryption [9].

C. Elliptic Curve Cryptography (ECC)

ECC This technology works on encryption of the PUBLIC KEY and is based on the elliptic curve theory that works to create encryption keys that have advantages in terms of speed and accuracy, that can be fastest, smallest and most efficient. It is through the properties of the Elliptic Curve Equation that the ECC keys are generated.

One-way function used to reduce efficient cryptographic systems by use of function is called (ECDLP) stand of Elliptic Curve Discrete Logarithm Problem. it similar to the one-way function which based on DSA and Diffie-Hellman [16].

When calculating a separate logarithm of an elliptic curve that breaks the ECC, that due to causes ECC the sizes of the key to be much smaller than those which required RSA and in the future it provides equivalent and parallel security with less computing power and the use of battery resources that make it suitable for mobile applications From RSA.

D. Digital Signatures (DSA)[17]

Digital Signature is way that use to verify the user identity and the message which received by receiver not have been altered during transaction and it's that encrypted message which sender sent as well. Basically, It is an electronic digital signature proving to the recipient that the message is signed by the sender.

Erfaneh Noorouzil proposed Hash function as method of digital signature that sending low size and capacity of data. The hash function generates dynamics and makes the bits smaller because it depends on every byte of data.

Normally, hashing use bitwise or and multiply functions as main function. There are several applications generating digital signature by using hashing algorithms due to simplicity & quick responding [3][18].

As below the analysis of the asymmetric algorithm cryptography different types, in terms of (Features, Advantages, Complexity and Security Solutions) [5][9].

Table 2: Analysis of different Asymmetric Key Algorithms Techniques [4]

Method	Rivest-Shamir-Adleman (RSA)	Diffie-Hellman
Features	It consists of (d, e) the public key which know as e and the private key which represents as d, uses the same function in encryption and decryption.	Depends on the strength and on the hardness of the discrete logarithms, it uses shares the secret encryption key in the encryption and when decoding as well.
benefits and the Advantages	it Calculates the inverse of e and is very difficult for attackers. Hence, it is very safe.	Use the faster Algorithm Due to the symmetric key is of very short of the length of the key which is (256 bits),
Complexity	The process of key generation is very slow and complexity. there is no way or method been proven to be equivalent to the method of calculating factors.	The longer the symmetric key usage period, the more attacks it will face. It will be more vulnerable to humans in middle attacks.
Security & the best Solutions	The Key length is greater than1024 bits.	Periodically changing the size of the key is necessary. And Development of the protocol between stations defeats and eliminate the MAN IN THE MIDDLE ATTACKS. The best solution against attacks is the development of a digital signature.

Method	Elliptical Curve Cryptography (ECC)	Digital Signature Algorithm (DSA)
Features	By using of elliptic curve equations helps to computes the keys.	it is a pair of large numbers which calculated by using some of the algorithms for authentication of data.it generate signatures by using of private keys and use of public keys for verification.
benefits and the Advantages	It can provide security that by using 164 bits key and it gives advantageous once compare it with RSA and Diffie Hellman algorithms. It the best that because it consumes less of the power and provides better and efficient utilities to batteries	It has super-speed. Secures data and maintains its confidentiality against various of the attacks like the attacks of MAN-IN-THE-MIDDLE attacks. It is the best and useful than other asymmetric key algorithms. It provides nonrepudiation and the trust authenticity among data.

Complexity	compared with RSA, it has difficulty in implementation, it has complexity and possibility on increasing the size of encrypted message.	due to the short life span of Digital signatures not compatible with this algorithm that cause complication of sharing between each other.
Security & the best Solutions	As listed in the introduction to the ECDSA algorithm. And the ECMQV's major convention protocol protects against to the MAN-IN-THE-MIDDLE ATTACKS	it necessarily to care about software Verification and must be purchased the Digital certificates from trusted authorities.

As below the analysis of the symmetric algorithm cryptography different types, in terms of (Created done by, Structures of the Algorithm, Length of the Key, Sizing of the Block, Rounds No., Vulnerabilities, effectiveness).

Table 3: Analysis of Symmetric Algorithms Techniques [4][7].

Method	DES	3DES
Created by	It developed by IBM and US government in to 1974	Developed by IBM in to 1978
Structures of the Algorithm	It uses of Feistel network	It uses of Feistel Network
Length of the Key	56 bits	It uses 64-bit keys, with the key length of 192 bits
Sizing of the Block	64	64
Rounds No.	16	+48
Vulnerabilities	the type of vulnerability's is brute force and MAN IN THE MIDDLE ATTACK	Some theoretical attacks
effectiveness	quite Slow	It is somewhat slow in software

Method	AES	Blowfish
Created done by	National Institute of standards & Technology (NIST)	It developed by Bruce Schneier in 1993
Structures of the Algorithm	It uses of Substitution and Permutation Network	It uses Feistel Network
Length of the Key	128-bit, 192-bit, 256-bit	Variable key length with maximum key length of 448 bits
Sizing of the Block	128	64
Rounds No.	+9	+16
Vulnerabilities	Side channel Attack	Not vulnerable to Attack
effectiveness	Efficiency is distributed among both software and hardware	High software efficiency

VI. Conclusion

Our research has attempted to explore the best methods of cryptography techniques in view of the security for the data which are getting transmitted over the network and have turned out to be exceptionally vital. In short, symmetric Key encryption and asymmetric key encryption both of them are very effective to securing data and transmitting through any communication medium. Due to the use of only one key in the symmetric key encryption, for the purposes of encoding and decoding data turns into an apprehensive mechanism. Thus, Asymmetric key encryption uses two separate keys to prevent any unethical or unauthorized access to data. The secure trade of key amongst sender and receiver is an imperative errand.In brief, the benefit of using digital signatures provides high confidentiality and non-repudiation to safeguard our confidentiality, integrity and availability.

References

[1] K. Vanitha, K. Anitha, A. M. J. M. Rahaman, and M. M. Musthafa, "Analysis of Cryptographic Techniques in Network Security," J. Appl. Sci. Comput., vol. 5, no. 8, pp. 155–163, 2018.

[2] F. Ayoub and K. Singh, "Cryptographic techniques and network security," in IEE Proceedings F-Communications, Radar and Signal Processing, 1984, vol. 131, no. 7, pp. 684–694.

[3] R. K. Sheth, "Analysis of cryptography techniques," Int. J. Res. Adv. Eng., vol. 1, no. 2, pp. 1–6, 2015.

[4] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," 2014 Int. Conf. Electron. Commun. Comput. Eng. ICECCE 2014, pp. 83–93, 2014, doi: 10.1109/ICECCE.2014.7086640.

[5] A. Kahate, Cryptography and network security. Tata McGraw-Hill Education, 2013.

[6] J. J. Amador and R. W. Green, "Symmetric-key block cipher for image and text cryptography," Int. J. Imaging Syst. Technol., vol. 15, no. 3, pp. 178–188, 2005.

[7] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms," in 2005 international Conference on information and communication technologies, 2005, pp. 84–89.

[8] H. Feistel, W. A. Notz, and J. L. Smith, "Some cryptographic techniques for machine-to-machine data communications," Proc. IEEE, vol. 63, no. 11, pp. 1545–1554, 1975.

[9] N. Jirwan, A. Singh, and D. S. Vijay, "Review and analysis of cryptography techniques," Int. J. Sci. Eng. Res., vol. 4, no. 3, pp. 1–6, 2013, [Online]. Available: http://www.ijser.org.

[10] S. Goyal, "A Survey on the Applications of Cryptography," Int. J. Sci. Technol., vol. 1, no. 3, 2012.

[11] I. No, "Analysis of Cryptography and Comparison of its Various Techniques," vol. 8, no. 5, pp. 688–691, 2017.

[12] A. S. Alkalbani, T. Mantoro, and A. O. M. Tap, "Comparison between RSA hardware and software implementation for WSNs security schemes," in Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010, 2010, pp. E84–E89, doi: 10.1109/ICT4M.2010.5971920.

[13] K. Button, V. Saini, and R. Kaur, "A Review on Visual Cryptography Techniques.," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 4, p. 32114, 2017, doi: 10.1016/j.proeng.2012.06.377.

[14] V. Kumar, A. Sharma, V. K. Mitali, and A. Sharma, "A survey on various cryptography techniques," Int. J. Emerg. Trends Technol. Comput. Sci., vol. 3, no. 4, pp. 307–312, 2014.

[15] H. Anderson., Introduction to Computer Security, Prentice Hall. 2004.

[16] R. Zuccherato, "Elliptic curve cryptography support in entrust," Entrust ltd. Canada, Dated, 2000.

[17] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," Int. J. Inf. Secur., vol. 1, no. 1, pp. 36–63, 2001, doi: 10.1007/s102070100002.

[18] A. Baheti, L. Singh, A. U. Khan, and N. Technologies, "Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System, and Authentication Using Neural Network," in 2014 Fourth International Conference on Communication Systems and Network Technologies, 2014, pp. 664–668, doi: 10.1109/CSNT.2014.139.