iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5445

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

Comprehensive Analysis of different Cryptographic Algorithms

Angad Singh Ojha
Department of Applied Science, MITS Gwalior

Abstract: Digital technologies is the demand of our society. To maintain digital property cryptography becomes more popular to protect data when it is being processed, transferred and stored. Cryptography algorithms provide security when we encrypt the messages or information in any system. This paper contains analysis of various cryptographic algorithm used in different emerging fields, also it emphasis the application fields, pitfalls and benefits .This survey classify the cryptographic algorithms based on their properties and behaviour also include the performance comparison in between various cryptographic algorithm used in the real world.

Keywords: Cryptography, Modular Arithmetic, Encryption, Symmetric, Asymmetric, RSA, ECC, DES, AES, IDEA

I. INTRODUCTION

Cryptography contain two words "crypt" means hidden and “graph" means writing. This Algorithm gives the way of protecting the information and communications with the help of some code. Information can read and process it only those for whom is intended. Algorithms are made in such way that is inflexible to interpret. These algorithms are used for cryptographic key generation and verification and digital signing to secure data confidentiality, network browsing and secret connections such as credit card, email and transactions. Anyone cannot understand the information for which it was unintended. An important role has been played in curbing down most information threats like the person within the middle and eavesdropping attacks which is focus on data and knowledge because it moves over the Internet system. Various areas are benefitted the service of this algorithm. Like signature verification is also emerging techniques based upon this algorithm. These functions are generally encrypts exclusively a hash of the message. Another type of cryptography is also very commonly used i.e. Public- key cryptography [1]. It might be a very significant, and wide used technology. Fig1. Show the basic block diagram of cryptography.

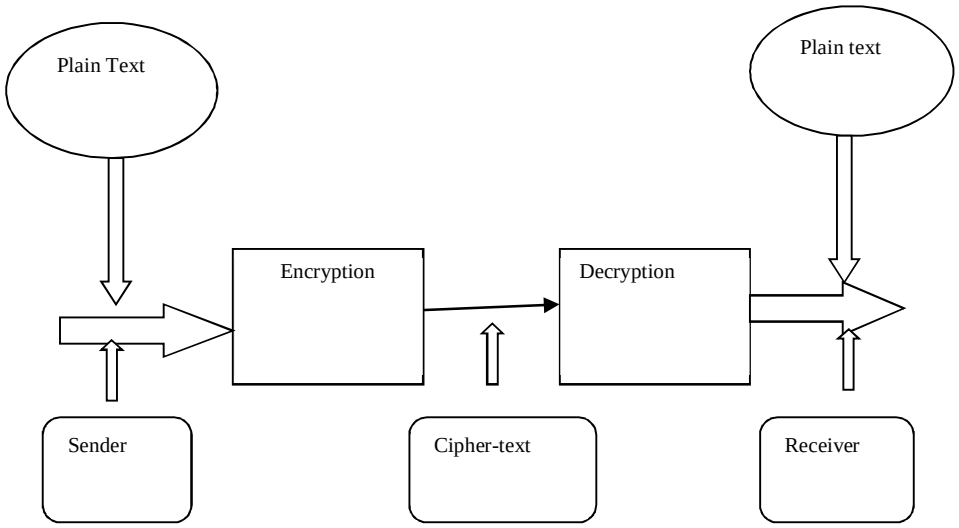


Fig.1 Basic Block Diagram of Cryptography System

Modular arithmetic theory is only for integers. This algorithm understands with the numbers and the basic Operations like multiplication, division, addition and subtraction. Modular arithmetic considers the reminder, which is often tied to a prime numbers. A value x mod y is the equivalent of asking for the reminder of x which is divided by y. Modular operations are used in many applications on large integers such as coding, cryptography and computer algebra. Consider the example1 for modular arithmetic to understand the complete process, that how it works [1] .

Example1: 145 mod 13 = 2

145mod 13 = 2	158 mod 13 = 2
146 mod 13 = 3	159 mod 13 = 3
147 mod 13 = 4	160 mod 13 = 4
148 mod 13 = 5	161 mod 13 = 5
149 mod 13 = 6	162 mod 13 = 6
150 mod 13 = 7	163 mod 13 = 7
151 mod 13 = 8	164 mod 13 = 8
152 mod 13 = 9	165 mod 13 = 9
153 mod 13 = 10	166 mod 13 = 10
154 mod 13 = 11	167 mod 13 = 11
155 mod 13 = 12	168 mod 13 = 12
156 mod 13 = 0	169 mod 13 = 0
157 mod 13 = 1	170 mod 13 = 1

This Cycle Repeat from 0 to 12 with Mode Operation of 13

Fig 2. Example of Modular arithmetic

II. DIFFERENT ENCRYPTION ALGORITHMS USED IN SECURITY PURPOSE

Encryption algorithms are comes under the categories of two types. Symmetric algorithms and Asymmetric algorithms. These algorithms are also contain various types. Some of them are defined below:

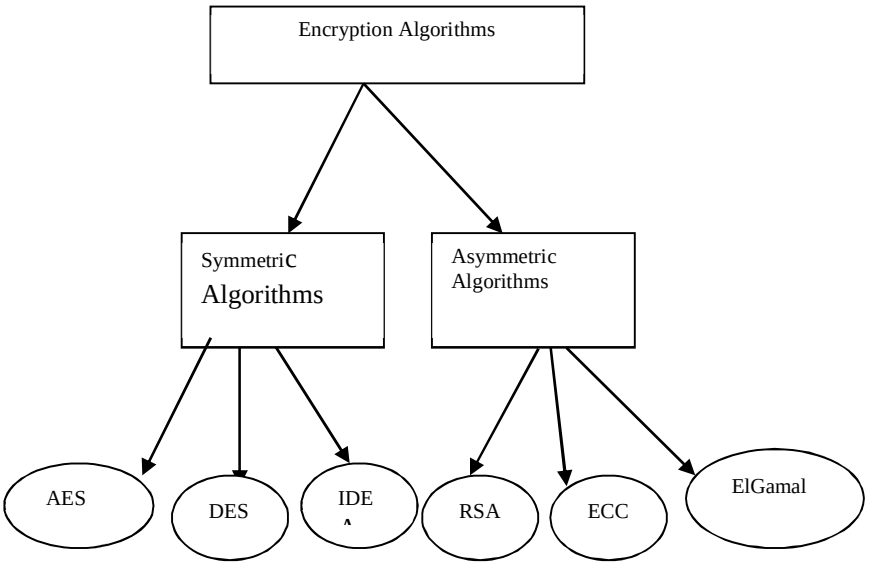


Fig3. Hierarchical structure of Encryption algorithm

A. Symmetric Algorithms

1) *DES:* DES stands for Data Encryption Standard. This algorithm is a symmetric key. Its short key length is 56-bits and block size is 64-bits. It is less secure as compare to other symmetric algorithms. Now a days this algorithm is no longer suggested for data encryption. This algorithm is very hard to understand because it is highly significant for the advanced modern cryptography system[1]. DES supports five different modes. First is ECB (Electronic Code Book) it is simplest mode to encrypt the block using secret key, it is least secure mode. Second mode is CBC (Cipher Block Chaining Mode). Before its encryption, CBC describes the mode in which each block of plaintext is XOR with previous cipher text block. . Third is CFB (Cipher Feedback Mode). It is little bit similar with version of CBC. Its decryption process is near-about same to CBC encryption mode. Fourth mode is OFC (Output Feedback Mode). It works same as CFB. There is no chaining function. It permits various error correcting codes for their function normally. This is the biggest advantage of this mode. Fifth and last mode of this algorithm is CTR (Counter Mode). It is similar to OFC mode. It allows breaking the operation in multiple steps. It gives the environment like multi-processing type[5].

2) *AES*: AES stands for Advanced Encryption Standard. The previous Standard DES was no longer enough for security purpose. AES is a symmetric encryption algorithm proposed to replace DES. AES does not use a Feistel structure. It is used 128, 192 and 256-bits key size and 128- bits block size. It is much strong and fast than triple DES standard. AES processes its operation on bits structure only[1][2].
3) *IDEA:* IDEA stands for International Data Encryption Algorithm. It is a replacement of the DEA standard. IDEA is also a symmetric based encryption algorithm. This algorithm contain key size is 128- bits and block size or plain text is 64- bits. The International data encryption algorithm is very easy to combine any encryption methods. It can be used to secure storage and data transmission. IDEA is also used five mode same as a DES algorithm[2].

B. Asymmetric Algorithms

1) *RSA*: RSA stands for Rivest, Shamir, Adleman.. It is Asymmetric Cryptography algorithm. Asymmetric key means it works on two dissimilar keys like Public key and Private Key. Public key used by each person and Private key used only authorized person. The Public key consists of two digits; one digit is multiply by two large prime facts. Private Key also used two prime facts [2]. In RSA Encryption, if we encrypted the message with a code it is called public key which can be protect or secure our data with key. No one can access its easily. RSA algorithm is based on the following facts. Given two large prime numbers a and b are selected randomly and a positive number n relatively calculating by a and b. According to Euler's theorem :

$$n = a * b$$
$$\emptyset = (a-1) * (b-1)$$

Exponent e is selected based on n and private exponent d from e, a and b. Here, (n, e) is treated as the public key and (n, d) as the private key. The RSA encryption shown in equation (1) , for some cipher text block C and plain text block M. The decryption shown in equation (2).

$$C = M^e (mod\ n) \longrightarrow (1)$$

$$M = C^d (mod\ n) \rightarrow (2)$$

Sequential steps of RSA algorithm

a) Generate a two large prime numbers a and b.
b) Compute the module n as $n = a * b$
c) Select an public key e , 1 and $n-1$ that is relatively prime to $a-1$ and $b-1$
d) Compute the private key d from e, a and b
e) Outcomes (n, e) as the public key and (n, d) as the private key

2) *ECC:* Elliptic curve cryptography is like Public-key cryptography. Public-key algorithms generate a technique for sharing keys and large numbers of participant in a very advanced data system. ECC maybe better for most purposes, but not for everything. In ECC, we can use small size of keys for the same level of security. Especially at high level of security. It is more complex to implement in comparison to RSA. [3]. This algorithm emphasis a lot of attention and achieved enormous recognition due to the similar level of security they offer with much lesser key sizes than conventional public-key crypto-systems have. It contains all relative asymmetric cryptographic primitives like agreement protocols, key exchange and Digital signature [11].
3) *El Gamal:* It is Asymmetric key encryption algorithm, which is proposed for Public key cryptography. It is based upon on discrete logarithm. It is very well connected to the DH(Diffie-Hellman) techniques. In ElGamal encryption algorithm speed is very fast for large amount of data storage or messages also. But it has a very complicated calculation to solve discrete logarithm.[3][4]

III. COMPARISON BETWEEN DIFFERENT TYPES OF CRYPTOGRAPHIC TECHNIQUES

In Section III Comprises Table 1. which has been given the different properties or features of the algorithm. This tabular structure gives the comparative analysis regarding in between algorithms. Features conatin the type, Key size, Block size and the truthiness of the security. Table 2 also contain the work done in the existing algorithm .This structure give a better outcome performance of the presented algorithms.

Table 1 Features of various Cryptographic Algorithms

Parameters	Abbreviation	Developed by and year	Type	Key size	Block size	Security
DES	Data encryption standard	IBM(1972)	Symmetric	56 bits	64 bits	Proven secure
AES	Advanced encryption standard	Joan Daemen, Vineent Rrijmen (1997)	Symmetric	128,192,224, 256 bits	128, 192, 224, 256- bit	secure
RSA	Rivest, Shamir, Adleman	R. Rivest, A. Shamir, L.Adleman(1977)	Asymmetric	Variable	variable	Secure
IDEA	International data encryption algorithm	James L. Massey Xuejia Lai (1990)	Symmetric	128 bits	64- bits	High
ECC	Elliptic curve cryptography	Neal Koblitz Victor miller	Asymmetric	Order of base point of elliptic curve bit length of n	variable	Low in comparison to RSA
ElGamal	El-Gamal	Taher El-gamal (1985)	Asymmetric	Variable	variable	Low in comparison to RSA

Table 2. Comparison in between the techniques used in cryptography system

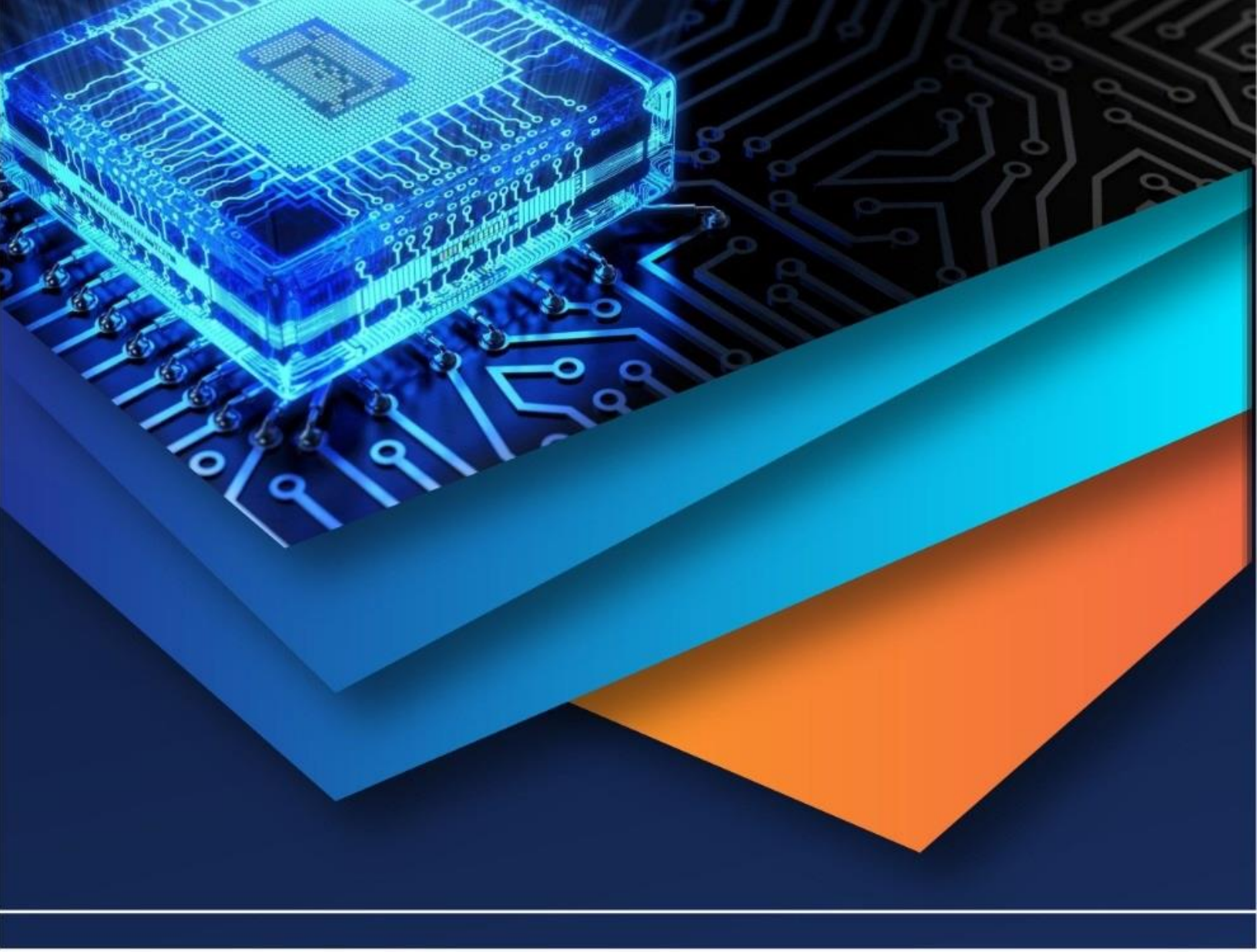
Year & References	Author	Used techniques and work done	Advantage	Disadvantage	Result
2016,[5]	Ayman E. Mohammed and Faisal M. Abdalla	DES, Proposed method for creating DES sub-key for simplifies the creation and expansion process of the encryption key.	This is very suitable for software and hardware.	Key size of this algorithms is the biggest disadvantage of DES	The proposed method is able to give different 16 sub-key
2017,[7]	Pooja Bhadauriya, Foram Suthar	AES, DES, IDEA, Proposed a new key algorithm of 128-bits which increase the security level.	Extremely secure, relatively fast	Sharing the key, more damage if compromised.	Result shows the proposed algorithms to enhance the security but it is also enhance the complexity of an algorithm.
2017,[7]	Venkata Mounika Namburi, TN Shankar	IDEA, Finding the major attacks in MANET	Better performance in terms of speed in comparison to asymmetric algorithm.	Less secure in comparison to asymmetric algorithm.	The result are reproduce and execute in NS2 simulator.
2017,[8]	Saheed Yakub Kayode, Gbolagode Kazeem Alagbe	RSA, Proposed an efficient approach to improve RSA algorithm using parallel technique.	It is safe or secure for its users because it is hard to crack.	RSA algorithm can be very slow in cases of large amount of data needs to encrypted by the same computer.	Result shows the improvement of speed of the RSA using CRT.
2018,[9]	Prasenjit Das and Chandan Giri	ECC, Proposed two algorithms DYNCBASE and DIGTBASE for mapping message for security.	It is light weight, efficient and more secure as compare to any other public key cryptography.	ECC algorithm is more complicated and more difficult to execute as compare to RSA.	The algorithm provides the same security level as compare to other ECC based encryption.
2019,[10]	Edwin R. Arboleda	E1-Gamal, Proposed an enhancement by combining two extant encryption schemes. It is combination of secure and fast chaos cryptography.	Encryption is very fast for lengthy messages and same block size gives a different key size each time.	El-Gamal has very complex calculations to solve discrete logarithm.	Proposed method provided for the El-Gamal cryptosystem to influence the number of key.

IV. CONCLUSIONS

Security of the network is a significant element in the exchange of knowledge. One such technique is cryptography that enables secure transmission of data despite destroying confidentiality and integrity. This paper emphasis on various existing algorithms and also give brief comparison between recent algorithms according to the new trends. This study highlighted merits and demerits of several explicit algorithms in the field of cryptography system.

REFERENCES

[1] W. Stallings, Cryptography and Network Security, 4th Edition, pp. 58-309, Prentice Hall, 2015.
[2] K. Sujatha, P V Nageswara Rao, A Arjun Rao, L V Rajesh, "Renowned Information Security Algorithms: A Comparative Study", International Journal of Engineering Research & Technology (IJERT) Vol. 5 Issue 02, February-2016.
[3] Amara M, Siad A., "Elliptic Curve Cryptography and its applications", 7th International Workshop on Systems Signal Processing and their Applications (WOSSPA),May 2011, pp 247 –250, IEEE.
[4] Fu Minfeng,Chen Wei, "Elliptic curve cryptosystem El-Gamal encryption and transmission scheme", Computer Application and System Modeling (ICCASM), 2010 International Conference on Computer Application and System modeling (Volume:6), Oct. 2010, pp : V6-51 - V6-53, IEEE.
[5] Ayman E. Mohammed , Faisal M. Abdalla "DES Security Enhancement using Genetic Algorithm", SUST Journal of Engineering and Computer Science (JECS), Vol. 17, No. 1, 2016.
[6] Pooja Bhadauriya, Foram Suthar, Sumit Chaudhary " A Novel Technique for Secure Communication in Cryptography", International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 6, Issue 3, March 2017.
[7] VenkataMounika Namburi1,Sisir Bolisetty, Saketh Krishna Velugoti,T N Shanka "Detecting Greyhole & Blackhole Attack Using Idea Cryptography in MANET", International Journal of Pure and Applied Mathematics Volume 116 No. 5 2017, 151-156 ISSN: 1311-8080 (printed version); ISSN: 1314-3395.
[8] Saheed Yakub; ALAGBE, Gbolagade Kazeem. "An Improved RSA Cryptosystem Based On Thread And Crt**",.** E-Academia Journal, [S.l.], v. 6, n. 2, jan. 2017. ISSN 2289-6589.
[9] Prasenjit Das, Chandan Giri, "An Efficient Method for text Encryption using Elliptic Curve Cryptography", 8th International Advance Computing Conference (IACC). 978-1-5386-6678-4/18/$31.00_c 2018 IEEE.
[10] Edwin R. Arboleda **"**Secure and Fast Chaotic El Gamal Cryptosystem", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June 2019.
[11] Amara M, Siad A., "Elliptic Curve Cryptography and its applications", Systems, Signal Processing and their Applications (WOSSPA), 2011 7th International Workshop, May 2011, pp 247 – 250, IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY