International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

A Survey on Encryption Techniques

Mahendra Kumar Sahu[1], Mohd. Shajid Ansari[2]

[1]M-Tech Scholar Computer Science & Engineering, RSR RCET Bhilai (C.G.) India

[2]Asst. Professor, CSE Department, RSR RCET Bhilai (C.G.) India

Abstract: ***Cryptography play an important role in secure communication and it offer an admirable solution to compromise the necessary protection against the data intruders. As the use digital techniques for communicating, it becomes a key issue that how to keep the confidentiality, integrity and authenticity of data. There are various techniques, which discovered from time to time to encrypt the data to make it more secure.***

Keywords: Cryptography, cipher, encryption, decryption, symmetric key, asymmetric key.

1. Introduction

Now a days we send many secret information across the internet, like, account information, credit, debit card details. These information are essential to us, hence they need protection or security from being compromised. Here arises the need of some technique that protects our information. Cryptography is the study of techniques that are implemented to set up a secure communication in which no information is compromised [5]. In cryptographic terminology, the message called plaintext. Encoding the contents of the message in such a way that outsiders cannot uncover its contents called encryption [9].

There are two types of cryptography algorithms that are given below:
a) Symmetric key cryptography
b) Asymmetric key cryptography

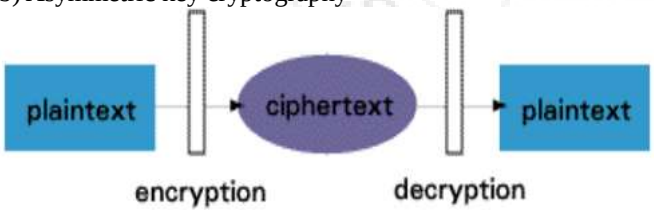

Figure 1: Cryptography process [3].

Basic terms used in cryptography:

a) **Plain Text:** A unique data that fed to the algorithm as input [5].
b) **Cipher Text**: The statement in which the actual data is concealed [5].
c) **Encryption:** Transforming original message into Cipher Text called Encryption. Cryptographers employ several encryption approaches to send secret messages through an insecure channel. The process of encryption requires two things - an encryption algorithm and a key [8].
d) **Decryption:** The reverse process of encryption called Decryption. It is the process of transforming Cipher Text into Plain Text. Decipherers employ the decryption algorithms at the receiver side to get the tangible message from non-readable message i.e. Cipher Text. The process of decryption needs two things - a Decryption algorithm and a key [8].
e) **Key:** A Key is a series of alphanumeric characters, which used to encrypt & decrypt the message. The Key used during encryption that works on the Plain Text and during decryption works on the Cipher Text. The selection of key in Cryptography is critical as the safety of encryption process depends directly on it [8].

2. Symmetric Key Cryptography

In symmetric key cryptographic algorithms single key used for both encryption and decryption process [10]. Symmetric encryption converts plaintext into cipher-text using a private key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext recovered from the cipher-text [3].

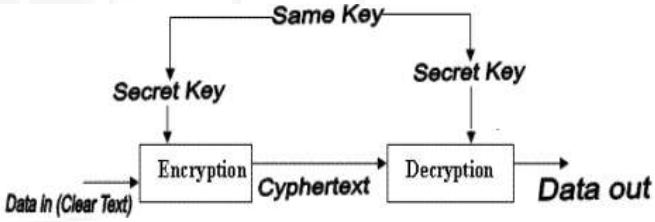

Figure 2: Symmetric key cryptography process [2].

There are different symmetric key algorithms, DES, 3DES, AES, RC4, BLOWFISH and TWOFISH.

a) Data Encryption Standard (DES)

DES uses same key for encryption and decryption of information hence both the sender and receiver knows and use same private key. To encrypt a plaintext DES group it into 64 bit blocks. By permutation and substitution, each block enciphered into a 64-bit cipher text by secret key. The process involves 16 rounds and can run in 4 different modes, encrypting blocks individually. Decryption is the inverse of encryption but reversing the order in which key applied. For any cipher, brute force attack is the basic one. It involves trying each key until finding the right answer. The size of the key defines the number of possible keys and the viability. DES uses a 64 bit key where 8 of those are parity checks and the rest would take 2^56 tries to find correct key [4].

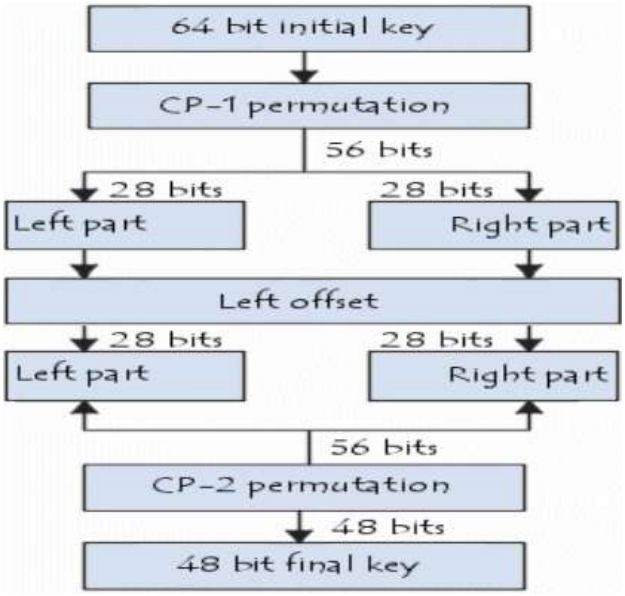

Figure 3: DES Process [4]

- The most efficient attack is still brute force. The 56-bit key size is the biggest defect [13].
- Hardware implementations of DES are very fast. DES was not design for software and hence runs relatively slowly [13].

b) Triple Digital Encryption Standard (3DES)

All Triple DES is DES algorithm used 3 times where key 1 used to encrypt a message which results in C1 cipher text, Key 2 used to decrypt C1 which results in C2 cipher text and Key 3 used to encrypt C2 resulting in C3 cipher text. Triple DES is not 3 times the strength of DES. Key 1 and Key 3, encryption done where Key 2, decryption done. Still uses DES block cipher with 56-bit keys but when using 3 keys yields key length of 168 bits. It used for higher-level security in the 1990s but dropped due to high overhead (slow) [1].

c) Advance Encryption Standard (AES)

AES is a symmetric key block cipher encryption algorithm designed by Vincent Rijmen and Joan Daemen in 1998. It support 128-bit block size and key length 128, 192 and 256 bits. AES performs 10, 12 or 14 round and the number of rounds depends on the key. It means for 128-bit key length AES performs 10 rounds, for 192-bit key it performs 12 rounds and for 256 bit key it performs 14 rounds [3].

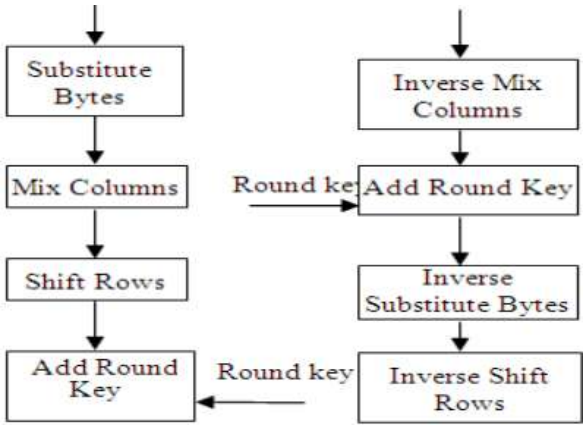

Figure 4: AES process [3]

- AES is highly efficient, secure and it is not complex.
- It needs more processing.
- It requires more rounds of communication as compared to DES [13].

d) Rivest Cipher 4 (RC4)

The RC4 algorithm generates pseudorandom stream of bits (key stream), and bitwise encryption / decryption has been performed. The generation key system involves two stages,

- Permutation of all 256 bytes.
- Two 8-bit index-pointers [3].

e) Blowfish

Blowfish is a symmetric key block cipher that uses a 64-bit block size and mutable key length. It takes a variable-length key from 32 bits to 448 bits. Blowfish has variants of 14 rounds or less. Blowfish is one of the fastest block ciphers, which have developed to date. Blowfish was created to allow anyone to use encryption free of patents and copyrights. Blowfish has remained in the public domain to this day. No attack known to be successful against it, though it suffers from weak keys problem [2].

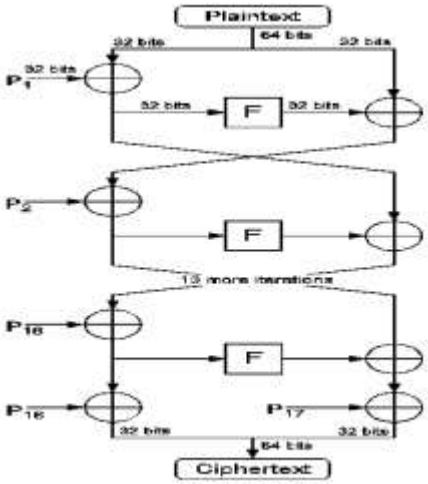

Figure 5: Blowfish [4].

f) Twofish

Twofish is the improved version of earlier block cipher Blowfish to meet the standards of AES for algorithm designing. It was one of the finalists of the AES, but not selected for standardization. The Twofish is an open to public sphere and not yet patented [11].

3. Asymmetric Key Cryptography

In asymmetric key cryptography, two different keys- public and private generated. These two keys are different but reliant on each other. In public-key cryptosystems, the public key may freely spread, while its paired private key must remain secret. In a public-key encryption system, the public key used for encryption; however, the private or secret key used for decryption [14].

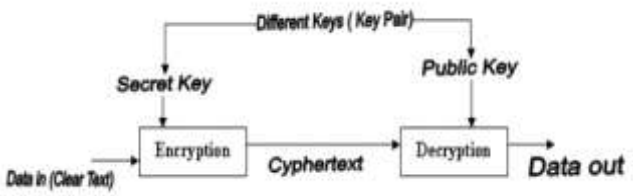

Figure 6: Asymmetric key cryptography process [2].

a) Rivest Shamir Adleman (RSA)

RSA is the most commonly used asymmetric algorithm. RSA can use for key interchange as well as digital signatures and the encryption of small blocks of data. Today, RSA mainly used to encrypt the session key used for secret key encryption or the message's hash value [6].

RSA mathematical rigidity comes from the ease in calculating large numbers and the difficulty in finding the prime factors of those large numbers. While employed with numbers using hundreds of figures, the math behind RSA is quite straightforward [6].

Key algorithm:

1) Choose two prime numbers, p and q. From p and q you can calculate the modulus, n = p*q.
2) Select a third number, e, which is relatively prime to the product (p-1)*(q-1). The number is the public exponent.
3) Calculate an integer d from the quotient
   (ed-1) / [(p-1)*(q-1)]
   The integer number d is the private exponent [6].

b) Elliptic Curve Cryptography

ECC based on distinct logarithms that are much more difficult to challenge at equivalent key lengths. The security of a public key system using elliptic curves based on difficulty of computing discrete algorithms in the group of points on an elliptic curve defined over a finite field. Elliptic curve equation over a finite field Fp is

$$y^2 = x^3 + ax + b \bmod p$$

Here, y, x, a and b are all within Fp, and p is a integers modulo p. a and b is the quantities which define what points will be on the curve. Curve coefficients have to fulfill one condition that is:

$$4a^3 + 27b^2 \neq 0$$

This condition guarantees that the curve will not contain any singularities [9].

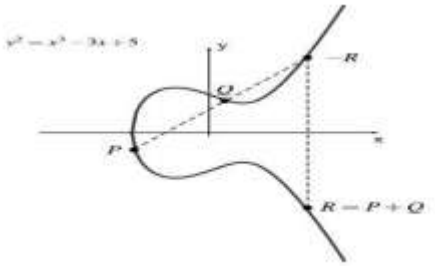

Figure 7: Elliptic curve cryptography [4].

c) Diffie-Hellman

The user does not have any information about the keys used by each other and they use a shared secret key over an insecure communication channel, then this key used to encrypt successive communications by a symmetric key cipher [12].

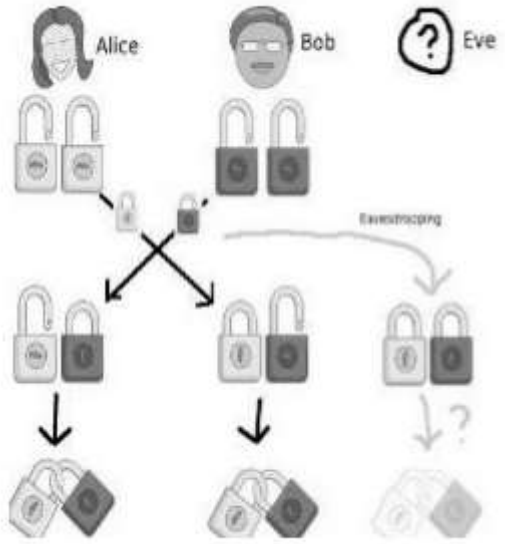

Figure 8: Diffie Hellman Key Exchange [4].

d) ElGamal Encryption Algorithm

ElGamal encryption system is an asymmetric key encryption algorithm for public key cryptography, which created on the Diffie-Hellman key exchange. It defined by Taher Elgamal in 1984. ElGamal is the prototype of Digital signature algorithm. ElGamal encryption comprises of three components: they are key generator, encryption algorithm, and the decryption algorithm [6].

4. Analytical Table

Table 1: Analytical table of cryptography techniques.

Algorithm	Created By	Year	Block Size	Key Length	Time Complexity	Analysis
DES	IBM	1975	64 bits	56 bits	High	The major issue in DES is key size i.e. 56 bits. It was implemented in Hardware not suitable for software [13].
3DES	IBM	1978	64 bits	192 bits	High	The security of 3DES is affected by the number of blocks processed with one key bundle [3].
AES	J. Daemen and V. Rijmen	1998	128, 192, 256 bits	128, 192, 256 bits	Low	Speed and code compactness on many platforms [13].
RC4	Ron Rivest	1994	2064 bits	40-2048 bits	Low	The major weakness of this technique is insufficient key

						scheduling [3].
Blowfish	Bruce Schneier	1993	64 bits	32 – 488 bits (128 by default)	High	Suitable for the application where the key remains constant for a long interval of time [2].
Tofish	Bruce Schneier	1998	128 bits	128, 192, 256 bits	High	Single key is sufficient in both software and hardware implementation for any length of bits up to 256 [3].
RSA	Rivest, Shamir, Adleman	1977	128 bits	1024 to 4096 bits	Low	Highly secure but slow in processing [6].
ECC	Victor Miller and Neil Koblitz	1985	128 bits	80,1024,160 bits	Low	Highly flexible, provide security with small key size [12].
Diffie-Hellman	Whitfield Diffie, Hellman	1976	512 bits	1024 to 4096 bits	High	It proposed authenticated key agreement and authenticated key agreement with confirmation in public key cryptography [12].
ElGamal	Taher Elgamal	1984	128 bits	1024 to 2048 bits	High	For same plain text it provides different cipher text, encrypted message is twice as long as original message [6].

5. Conclusion

Cryptography plays vital role in explosive development of digital data storage and communication. It is used to attain the mains of security areas like confidentiality, integrity, authentication, non-repudiation. In order to reach these goals, several cryptographic algorithms developed. In which some of the algorithms are successes and others unsuccessful due to lack of security. In this paper, we conclude that in private key encryption AES is better and in public key encryption ECC is better to provide security and to implement hardware as well as software.

References

[1] Shelveen Pandey, Mohammed Farik, Best Symmetric Key Encryption – A Review, international journal of scientific & technology research volume 6, issue 06, june 2017
[2] Sangeeta, Er. Arpneek Kaur, A Review on Symmetric Key Cryptography Algorithms, International Journal of Advanced Research in Computer Science , Volume 8, No. 4, May 2017.
[3] Sonia Rani, Harpreet Kaur, Technical Review on Symmetric and Asymmetric Cryptography Algorithms, International Journal of Advanced Research in Computer Science, Volume 8, No. 4, May 2017.
[4] V. Hemamalini, G. Zayaraz, V. Susmitha, M. Gayathri and M.Dhanam , A Survey on Elementary, Symmetric and Asymmetric Key Cryptographic Techniques, International Journal of Computing Academic Research (IJCAR) ISSN 2305-9184, Volume 5, Number 1 (February 2016).
[5] Md. Sarfara ziqbal, Shivendra Singh, arunima jaiswal, Symmetric Key Cryptography: technological developments in the Field, International Journal of Computer Applications (0975 – 8887), Volume 117 – No. 15, May 2015.
[6] Asithambi. N, A Study on Asymmetric Key Cryptography Algorithms, International Journal of Computer Science and Mobile Applications, Vol.3 Issue. 4, April- 2015, ISSN: 2321-8363
[7] Tannu Bala, Yogesh Kumar , Asymmetric Algorithms and Symmetric Algorithms: A Review , International Conference on Advancements in Engineering and Technology (ICAET 2015).
[8] Preeti Singh, Praveen Shende Symmetric Key Cryptography: Current Trends, International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 12, December 2014, ISSN 2320–088X
[9] Neha garg and partibha yadav, Comparison of asymmetric Algorithms in Cryptography, International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 4, April 2014,ISSN 2320–088X
[10] Saranyak, Mohanpriya R, Udhayan J, A Review on symmetric Key encryption techniques in Cryptography, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014, ISSN: 2278 – 7798
[11] Anjula Gupta, Navpreet Kaur Walia, Cryptography Algorithms: A Review, International Journal of Engineering Development and Research, 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939 IJEDR1402064.
[12] Nitin Jirwan, Ajay Singh, Dr. Sandip Vijay , Review and Analysis of Cryptography Techniques ,International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013 1 ISSN 2229-5518 IJSER.
[13] Divya sukhija , A Review Paper on AES and DES Cryptographic Algorithms, International Journal of Electronics and Computer Science Engineering, 2013, ISSN- 2277-1956 ISSN 2277-1956/V3 N4-354-359
[14] Pranab Garg, Jaswinder Singh Dilawari, A Review Paper on Cryptography and Significance of Key Length, International Journal of Computer Science and Communication Engineering IJCSCE Special issue on “Emerging Trends in Engineering” ICETIE 2012.