Cryptography and its Desirable Properties in terms of different algorithm

Mukta Sharma*
Dr. Jyoti Batra Arora**

Abstract

The proliferation of Internet has revolutionized the world. The world has become a smaller place to communicate. Especially in India, after demonetization Indian government is encouraging both customer and buyer to transact online (go cashless). Electronic payment is a new trend to transact online as any e-commerce environment needs a payment system. Payment system requires an intricate design which ensures payment security, transaction privacy, system integrity, customer's authentication, and purchaser's promise to pay and supplier promise to sell a high-quality product. There are several e-payments systems like paying via Plastic money (credit/debit/smart card), e-wallet, e-cash, UPI, Net banking, Aadhaar Card, etc. Electronic payment is made online without face to face interaction, which leads to electronic frauds. Therefore, the emphasis is given on security methods opted by banks especially on cryptography.

This paper begins with the primary security threats, followed by the prevention plan. It highlights the cryptography and discusses the desirable property to check the strength of encryption algorithm.

Keywords: Avalanche, Cryptography, Decryption, Encryption, Cipher Text, DES, Plain Text, Symmetric Cryptography

I. Introduction

With the technological advancement, everyone is using the Internet on their smart phones, laptops, desktops, iPads, etc. Users are transacting funds online. E-banking is growing phenomenally well. There are numerous advantages of using online banking from both customers and bankers' perspective such as cost-effective, paperless, immediate transfer of funds, geographical convenience, 24*7, etc. Several issues in internet banking are security, trust, authentication, Non-repudiation, privacy and availability. Since the inception of e-banking security is and always will remain a matter of great concern. After the development of e-banking, the bank needs to ensure payment security, transactions privacy, system integrity, customer authentication as it is a payment system online.

Every coin has two facets with the internet having numerous advantages it has significant security threats. Customers are reluctant to share their demography especially financial details online because of the security concerns. The need for the safety means to prevent unwanted access to confidential information. Cybercriminals steal sensitive data and misuse it for their benefits.

Mukta Sharma*
Research Scholar, TMU

Dr. Jyoti Batra Arora**
Assistant Professor, IITM

II. Security Threats

Electronic transactions have been facing various obstacles with context to security. Crimes like hacking, cracking, phishing; DOS, etc. are among few attacks or threats for the safety. Following attacks breach the security:

a) *Cracking / Hacking*- It defined as the unauthorized access to someone else information.

b) *Denial of Service attack*- DoS floods the computer with more requests than it can handle causing the web server to crash. Denying authorized users the service offered by the resource. Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. Controlling such attacks is tough. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the server's crash.

c) *E-mail spoofing*- A spoofed e-mail is one, which misrepresents its origin. It shows its origin to be different from which it originates.

d) *Phishing*- It is another criminally fraudulent process, in which a fake website resembling the original site is designed. Phishing is an attempt to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

e) *Salami Attack*- is an attack which is difficult to detect and trace, also known as penny shaving. The fraudulent practice of stealing money repeatedly in small quantities, usually by taking advantage of rounding to the nearest cent (or other monetary units) in financial transactions.

f) *Virus / Worm Attacks* – Malicious Programs are dangerous may it be Viruses, worms, logic bombs, trap doors, Trojan Horse, etc. As they are programs written to infect and harm the data by altering or deleting the information, or by making a backdoor entry for unauthorized person.

g) *Forgery*- Counterfeit currency notes, postage, and revenue stamps, mark sheets, etc. can be forged using sophisticated computers, printers, and scanners.

III. Security Measures

Security has become a necessity, and need to keep data safe, achieve it and many techniques are available. By using these techniques, one can ensure the confidentiality, authentication, privacy and integrity of their information. Information can be of any type; may it be in the form of text, image, audio or video. The need for security means to prevent unwanted access to confidential information, this can be attained by the following ways:-

a) *SSL*- Secure Socket Layer is a protocol developed by Netscape. It was designed so that sensitive data can be transmitted safely via the Internet. SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely. All browsers support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers.

b) *HTTPS*- Hyper Text Transfer Protocol combined with SSL to ensure security. S-HTTP is designed to transmit individual messages securely. SSL and S- HTTP, can be seen as complementary rather than competing technologies. Both protocols have been approved by the Internet Engineering Task Force (IETF) as a standard.

c) *Firewall*- Firewalls can be implemented in both hardware and software, or a combination of both to prevent unauthorized access. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages are entering or leaving the intranet pass through the firewall, which examines each message and blocks those messages that do not meet the specified security criteria.

d) *SET*- Secure Electronic Transaction is a standard developed jointly by Visa International, MasterCard, and other companies. The SET protocol uses digital certificates to protect credit card transactions that are conducted over the Internet. The SET standard is a significant step towards securing Internet transactions, paving the way for more merchants, financial institutions, and consumers to participate in electronic commerce.

e) *PGP*- Pretty Good Privacy provides confidentiality by encrypting messages to be transmitted or data files to be stored using an encryption algorithm. PGP uses the "public key" encryption approach - messages are encrypted using the publicly available key, but can only be deciphered by the intended recipient via the private key.

f) *Anti-Virus*- To secure PC, laptop, smartphone from any malicious attack the user must install a good anti- virus and always update the anti-virus software fortnightly for better security.

g) *Steganography*- It is the process of hiding a secret message with an ordinary message. The original

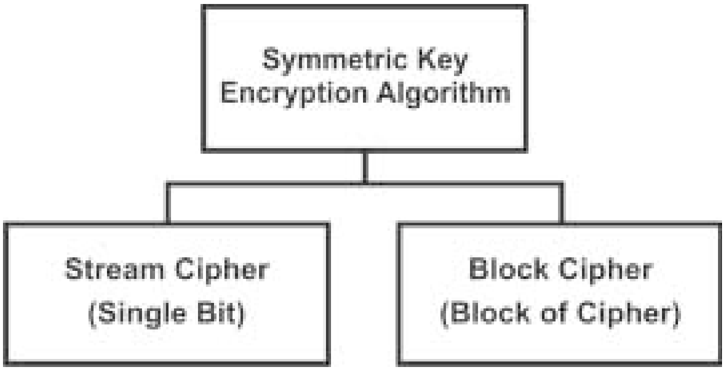

Symmetric Key Encryption Algorithm
Stream Cipher (Single Bit)
Block Cipher (Block of Cipher)

Figure 1: Symmetric Key Encryption Algorithm

user will view the standard message and will fail to identify that the message contains a hidden or encrypted message. The secret message can be extracted by only the authentic users who are aware of the hidden message beneath the ordinary file. Steganography is now gaining popularity among the masses because of ease of use and abundant tools available.

h) *Cryptography*- It is the "scrambling" of data done using some mathematical calculations and only authentic user with a key and algorithm can "unscramble" it. It allows secure transmission of private information over insecure channels.

IV. Cryptography

Cryptology is the study of reading, writing, and breaking of codes. It comprises of cryptography (secret writing) and cryptanalysis (breaking code). Cryptography is an art of mangling information into apparent incomprehensibility in a way permitting a secret method of unscrambling [11]. Human has a requirement to share private information with only intended recipients. Cryptography gives a solution to this need.

Cryptographic algorithms play a significant role in the field of network security. To perform cryptography, one requires the secure algorithm which helps the conversion efficiently, securely if carried out with a key. Encryption is the way to transform a message so that only the sender and recipient can read, see or understand it. The mechanism is based on the use of mathematical procedures to scramble data so that it is tough for anyone else to recover the original message.

There are two basic types of cryptosystems such as symmetric cryptosystems and asymmetric cryptosystems. Symmetric cryptography is a concept in which both sender and receiver shares the same key for encryption and decryption process. In contrast to symmetric cryptography, asymmetric cryptography uses a pair of keys for encryption and decryption transformations. The public key is used to encrypt data, and the private key is used to decrypt the message.

1) Symmetric Key Encryption Algorithms

Symmetric Key is also known as a private key or conventional key; shares the unique key for transmitting the data safely. The symmetric key was the only way of enciphering before the 1970s. Symmetric Key Encryption can be performed using Block Cipher or Stream Cipher.

Stream Cipher takes one bit or one byte as an input, process it and then convert it into 1bit or 1-byte cipher-text. Like RC4 is a stream cipher used in every mobile phone.

Block Cipher works with a single block or chunks of data or message instead of a single stream, character, or byte. Block ciphers mean that the encryption of any plaintext bit in a given block depends on every other plaintext bit in the same block. Like DES, 3DES have a block size of 64 bits (8bytes), and AES has a block size of 128 bits (16 bytes).

2) Need for Cryptography

It has given a platform which can ensure not only confidentiality but also integrity, availability, and non-repudiation of messages/ information. Symmetric Key encryption algorithm focuses on privacy & confidentiality of data.

3) Symmetric Key Block Cipher Algorithm

The paper focuses on Symmetric Key block ciphers. DES, 3DES, AES, IDEA, Blowfish are among most used and popular algorithms of Block ciphers.

a) *DES*- DES is based on Feistel network. It takes 64 bit Plain Text as an input and 64 bit Cipher Text comes as an output. Initially a 64 bit Key is sent which is later converted to 56 bits (by removing every 8th bit). Later using 16 iterations with permutation, expansion, substitution, transpositions and basic mathematical functions encryption is performed and decryption is the reverse process of encryption.

b) *3DES* – Triple DES is an enhancement of Data Encryption Standard. To make it more secure the algorithm execute three times with three different keys and 16*3=48 rounds; and a key length of 168 bits (56*3) [22]. The 3DES encryption algorithm works in a sequence Encrypt-Decrypt-Encrypt (EDE). The decryption process is just reverse of Encryption process (Decrypt- Encrypt-Decrypt). 3DES is more complicated and designed to protect data against different attacks. 3DES has the advantage of reliability and a longer key length that eliminates many attacks like brute force. 3DES higher security was approved by the U.S. Government. Triple DES has one big limitation; it is much slower than other block encryption methods.

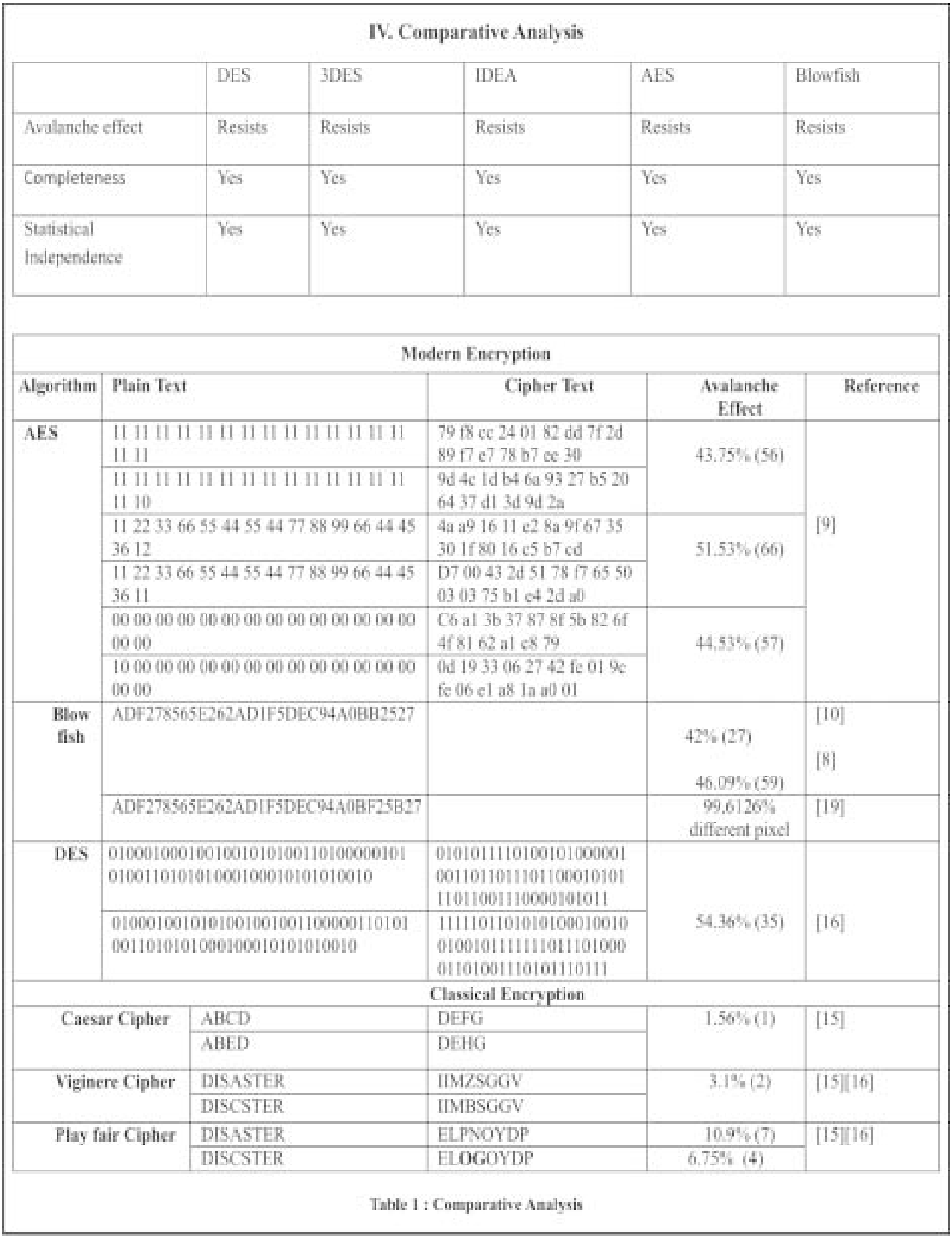
c) *IDEA*-International Data Encryption Algorithm is another symmetric key block cipher algorithm developed at ETH in Zurich, Switzerland. It is based on substitution-permutation structure. It is a block cipher that uses a 64 bit plain text, divided equally into 16 bits each (16*4=64); with 8 and s half rounds and a Key Length of 128-bits. For each round 6 sub keys are required 4 before the round and 2 within the round (8*6= 48 sub keys+ 4 sub keys are used after last or eighth round that makes total 52 sub- keys). IDEA does not use S-boxes. IDEA uses the same algorithm in a reverse order for decryption [2] [21].

d) *AES*- AES is also a symmetric key algorithm based on the substitution–permutation Network [4][7][23].

AES use a 128-bit block as plain text, which is organized as 4*4 bytes array also called as State and is processed in several rounds. It has variable Key length 128, 192 or 256-bit keys. Rounds are variable 10, 12, or 14 depends on the key length (Default # of Rounds = key length/32 + 6). For 128 bit key, number of rounds are 10; 192 bit key, 12 rounds and for 256 bit key, 14 rounds. It only contains a single S- box (which takes 8bits input, and give 8 bits output) which consecutively work 16 time. Originally the cipher text block was also variable, but later it was fixed to 128 bits.

The Encryption and decryption process consists of 4 different transformations applied consecutively over the data block bits, in a fixed number of iterations, called rounds. The decryption process is direct inverse of the encryption process. Hence the last round values of both the data and key are first round inputs for the decryption process and follows in decreasing order. AES is extremely fast and compact cipher. For implementers its symmetric and parallel structure provides great and an effective resistance against cryptanalytic attacks. The larger block size prevents birthday attacks and large key size prevents brute force attacks

e) BlowFish- It is a symmetric block cipher and works on of 64-bit block size. Key length is variable from 32 bits to 448 bits. It has16 rounds and is based on Feistel network. It has a simple structure and it's easy to implement. It encrypts data on 32 bit microprocessors at a rate of 18 clock cycles per byte so much faster than AES, DES, and IDEA. Since the key size is large it is complex to break the code in the blowfish algorithm. It is vulnerable to all the attacks except the weak key class attack. It is unpatented and royalty-free. It requires less than 5K of memory to run Blowfish [6] [18].



IV. Comparative Analysis

	DES	3DES	IDEA	AES	Blowfish
Avalanche effect	Resists	Resists	Resists	Resists	Resists
Completeness	Yes	Yes	Yes	Yes	Yes
Statistical Independence	Yes	Yes	Yes	Yes	Yes

Modern Encryption				
Algorithm	**Plain Text**	**Cipher Text**	**Avalanche Effect**	**Reference**
AES	11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11	79 f8 cc 24 01 82 dd 7f 2d 89 f7 c7 78 b7 cc 30	43.75% (56)	[9]
	11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 10	9d 4c 1d b4 6a 93 27 b5 20 64 37 d1 3d 9d 2a		
	11 22 33 66 55 44 55 44 77 88 99 66 44 45 36 12	4a a9 16 11 e2 8a 9f 67 35 30 1f 80 16 c5 b7 cd	51.53% (66)	
	11 22 33 66 55 44 55 44 77 88 99 66 44 45 36 11	D7 00 43 2d 51 78 f7 65 50 03 03 75 b1 e4 2d a0		
	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	C6 a1 3b 37 87 8f 5b 82 6f 4f 81 62 a1 c8 79	44.53% (57)	
	10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0d 19 33 06 27 42 fe 01 9e fe 06 e1 a8 1a a0 01		
Blow fish	ADF278565E262AD1F5DEC94A0BB2527		42% (27) 46.09% (59)	[10] [8]
	ADF278565E262AD1F5DEC94A0BF25B27		99.6126% different pixel	[19]
DES	0100010001001001010100110100000101 01001101010100010001010101010010	0101011110100101000001 0011011011101100010101 11011001110000101011	54.36% (35)	[16]
	0100010010101001001001100000110101 0011010101000100010101010010	1111101101010100010010 0100101111111011101000 01101001110101110111		
Classical Encryption				
Caesar Cipher	ABCD	DEFG	1.56% (1)	[15]
	ABED	DEHG		
Viginere Cipher	DISASTER	IIMZSGGV	3.1% (2)	[15][16]
	DISCSTER	IIMBSGGV		
Play fair Cipher	DISASTER	ELPNOYDP	10.9% (7)	[15][16]
	DISCSTER	ELOGOYDP	6.75% (4)	

Table 1 : Comparative Analysis

V. Algorithm Security

The two essential properties to check the complexity of any algorithm is time and space. According to Kerckhoff, the cryptanalyst knows the complete process of encryption and decryption except for the value of the secret key. It implies that the security of a secret-key cipher system rests entirely on the secret key [17]. Therefore, for better security in symmetric encryption one should keep the following criteria's in mind:

- Key should be exchanged very safely because if the key is known the entire algorithm is compromised.
- A secure encryption algorithm is robust & resilient against a potential breach using combinations of cipher texts & key [14] [20].

1) Desirable Properties of Block Cipher

The strength of a block cipher can be tested through these properties like Avalanche, Completeness and Statistical Independence.

- Avalanche Effect- It is an excellent property of cryptographic algorithm also stated as Butterfly effect. It means that by changing only one bit (small change) of the plain text or the key should produce a radical shift in the final output. If the final output is modified or flipped with 50% of bits, then it is said to be strict Avalanche effect. SAC is harder to perform an analysis on cipher text when trying to come up with an attack [5] [8] [17]. It's easy to impose conditions on Boolean functions so that they satisfy certain avalanche criteria, but constructing them is a harder task. Avalanche can be categorized as follows:

    - The strict avalanche criteria (SAC) guarantee that exactly half of the output bits change when one input bit changes [17].
    - The bit independence criterion (BIC) states that output bits j and k should change independently when any single input bit i is inverted, for all i, j and k[17].

    Avalanche Effect= Number of flipped bits in ciphered text/ Number of bits in ciphered text.

- Completeness -According to encryption, this is a necessary property. Completeness means that each bit of the cipher text/ output block needs to depend on each bit of the plaintext [15]. Change in one bit of the input (plaintext) will bring change in every bit of the output (Ciphertext). It has an average of 50% probability of changing.

    Let us imagine an eight-byte plain text, and there is a change in the last byte, it would only have affected the 8th byte of the Ciphertext. An attacker can very easily guess 256 different plaintext-Ciphertext pairs. Finding out 256 plaintext-Ciphertext pairs is not hard at all in the internet world, and standard protocols have standard headers and commands (e.g. "get," "put," "mail from:," etc.) which the attacker can safely guess.

    If the cipher has this property, the attacker need to collect 264 (~1020) plaintext-Ciphertext pairs to crack the cipher in this way.

- Statistical independence that input and output should appear to be statistically independent.

VI. Conclusion

Cryptography is a good way to protect data from getting breached. Symmetric cryptography ensures confidentiality of data. Asymmetric cryptography takes care of authenticity, integrity, non-repudiation of data. As can be seen in the above table of comparative analysis, where all the algorithms are built on these three desired properties. The percentages may vary but they all fulfil the basic criteria of an encryption algorithm. While building the understanding about the encryption algorithm and designing a new algorithm anybody can establish the significant role of thee building blocks.

These three important properties decide the strength and resistance of the algorithm.

References

1. Daemen, J., Govaerts, R. and Vandewalle, J. (1998). *Weak Keys for IDEA.* Springer-Verlag.
2. Engelfriet, A. (2012). *The DES encryption algorithm.* Available at www.iusmentis.com/technology/encryption/des.

3. Forouzan, B.A., &Mukhopadhyay, D. (2010). *Cryptography and Network Security*. Tata McGraw-Hill, New Delhi, India

4. Gatliff, B. (2003). *Encrypting data with the Blowfish algorithm.* Available at http://www.design-reuse.com/ articles/5922/ encrypting-data-with-the-blowfish-algorithm.

5. Kak, A. (2015). *Computer and Network Security- AES: The Advanced Encryption Standard.*Retrieved from https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf

6. Koukou, Y.M., Othman, S.H., Nkiama, M. M. S. H. (2016). *Comparative Study of AES, Blowfish, CAST-128 and DES Encryption Algorithm.* IOSR Journal of Engineering, 06(06), pp. 1-7.

7. Kumar, A., Tiwari, N. (2012).*Effective Implementation and Avalanche Effect of AES.* International Journal of Security, Privacy and Trust Management (IJSPTM).

8. Mahindrakar, M.S. (2014). *Evaluation of Blowfish Algorithm based on Avalanche Effect.* International Journal of Innovations in Engineering and Technology, 1(4), pp. 99-103.

9. Menezes, A., Van, P., Orschot, O. and Vanstone, S. (1996). *Handbook of Applied Cryptography*, CRC Press.

10. Mollin, R.A. (2006). *An Introduction to Cryptography.* Second Edition, CRC Press

11. National Bureau of Standards (1997). *Data Encryption Standard.* FIPS Publication 46.

12. Paar, C., Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners'.* Springer, XVIII, 372.

13. Ramanujam, S., &Karuppiah, M. (2011). *Designing an algorithm with high Avalanche Effect.* International Journal of Computer Science and Network Security. 11(1).

14. Saeed, F., & Rashid, M. (2010). *Integrating Classical Encryption with Modern Technique.* International Journal of Computer Science and Network Security, 10(5).

15. Schneier B. (1994). *Applied Cryptography.* John Wiley& Sons Publication, New York.

16. Schneier, B. (1994).*Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), Fast Software Encryption*, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, Available at http:// www.schneier.com/paper-blowfish-fse.html

17. Shailaja, S. & Krishnamurthy, G.N. (2014). *Comparison of Blowfish and Cast-128 Algorithms Using Encryption Quality, Key Sensitivity and Correlation Coefficient Analysis.* American Journal of Engineering Research, 7(3), pp. 161-166.

18. Stallings, W. (2011). *Cryptography and Network Security: Principles and Practice.* Pearson Education, Prentice Hall: USA

19. Thaduri, M., Yoo, S. and Gaede, R. (2004). *An Efficient Implementation of IDEA encryption algorithm using VHDL.* Elsevier

20. Tropical Software, Triple DES Encryption, Available at http://www.tropsoft.com/strongenc/des3.htm,

21. Wagner, R. N. *The Laws of Cryptography.* Retrieved From http://www.cs.utsa.edu/~wagner/laws/