A Review on Classical and Modern Encryption Techniques

Ali Mir Arif Mir Asif[1], Shaikh Abdul Hannan[2]
[1]Assistant Professor, I.M.S.I.T., Aurangabad, India.
[2]Assistant Professor, Department of CS & IT, Albaha University, Albaha, Saudi Arabia.

Abstract- **Over the centuries, an elaborate set of protocols and mechanisms has been created to deal with information security issues when the information is conveyed by physical documents. Often the objectives of information security cannot solely be achieved through mathematical algorithms and protocols alone, but require procedural techniques and abidance of laws to achieve the desired result. For example, privacy of letters is provided by sealed envelopes delivered by an accepted mail service. The physical security of the envelope is, for practical necessity, limited and so laws are enacted which make it a criminal offense to open mail for which one is not authorized. It is sometimes the case that security is achieved not through the information itself but through the physical document recording it. For example, paper currency requires special inks and material to prevent counterfeiting. Achieving information security in an electronic society requires a vast array of technical and legal skills. There is, however, no guarantee that all of the information security objectives deemed necessary can be adequately met. The technical means is provided through cryptography [1]. In this paper study of various classical and modern encryption techniques has carried out. Also a review of research and development of encryption techniques has done. Finally we compared the results and concluded that which technique is superior.**

Keywords- **Cipher, Encryption, Plain Text, Avalanche Effects Decryption, Cipher Text.**

I. INTRODUCTION

Conceptually, the way information is recorded has not changed dramatically over time. Whereas information was typically stored and transmitted on paper, much of it now resides on magnetic media and is transmitted via telecommunications systems, some wireless. What has changed dramatically is the ability to copy and alter information. One can make thousands of identical copies of a piece of information stored electronically and each is indistinguishable from the original. With information on paper, this is much more difficult. What is needed then for a society where information is mostly stored and transmitted in electronic form is a means to ensure information security which is independent of the physical medium recording or conveying it and such that the objectives of information security rely solely on digital information itself [1]?

One of the fundamental tools used in information security is the signature. It is a building block for many other services such as non-repudiation, data origin authentication, identification, and witnessing, to mention a few. Having learned the basics in writing, an individual is taught how to produce a handwritten signature for the purpose of identification. At contract age the signature evolves to take on a very integral part of the person's identity. This signature is intended to be unique to the individual and serve as a means to identify, authorize, and validate. With electronic information the concept of a signature needs to be redressed; it cannot simply be something unique to the signer and independent of the information signed. Electronic replication of it is so simple that appending a signature to a document not signed by the originator of the signature is almost a triviality.

Analogues of the "paper protocols" currently in use are required. Hopefully these new electronic based protocols are at least as good as those they replace. There is a unique opportunity for society to introduce new and more efficient ways of ensuring information security. Much can be learned from the evolution of the paper based system, mimicking those aspects which have served us well and removing the inefficiencies.

Achieving information security in an electronic society requires a vast array of technical and legal skills. There is, however, no guarantee that all of the information security objectives deemed necessary can be adequately met. The technical means is provided through cryptography.

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is not the only means of providing information security, but rather one set of techniques. Of all the information security objectives listed in Table 1, the following four form a framework upon which the others will be derived: (A) privacy or confidentiality; (B) data integrity; (C) authentication ; and (D) non-repudiation.

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

A. *Confidentiality*

Confidentiality is a service used to keep the content of information from all but those authorized to have it. *Secrecy* is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.

B. *Data Integrity*

Data integrity is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

C. *Authentication*

Authentication is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be

authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).

D. Non-repudiation

Non-repudiation is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute [1].

A fundamental goal of cryptography is to adequately address these four areas in both theory and practice. Cryptography is about the prevention and detection of cheating and other malicious activities.

TABLE I
SOME INFORMATION SECURITY OBJECTIVES

Privacy or confidentiality	keeping information secret from all but those who are autho-rized to see it.
data integrity	ensuring information has not been altered by unauthorized or unknown means.
entity authentication or identification	corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.).
Message authentication	corroborating the source of information; also known as data origin authentication.
Signature	a means to bind information to an entity.
authorization	conveyance, to another entity, of official sanction to do or be something.
Validation	a means to provide timeliness of authorization to use or ma-nipulate information or resources.
access control	restricting access to resources to privileged entities.
Certification	endorsement of information by a trusted entity.
timestamping	recording the time of creation or existence of information.
Witnessing	verifying the creation or existence of information by an entity other than the creator.
Receipt	acknowledgement that information has been received.
Confirmation	acknowledgement that services have been provided.
Ownership	a means to provide an entity with the legal right to use or transfer a resource to others.
Anonymity	concealing the identity of an entity involved in some process.
non-repudiation	preventing the denial of previous commitments or actions.
Revocation	retraction of certification or authorization.

It describes a number of basic *cryptographic tools* (*primitives*) used to provide information security. Examples of primitives include encryption schemes, hash functions and digital signature schemes. It provides a schematic listing of the primitives considered and how they relate. These primitives should be evaluated with respect to various criteria such as:

A. Level of Security

This is usually difficult to quantify. Often it is given in terms of the number of operations required (using the best methods currently known) to defeat the intended objective. Typically the level of security is defined by an upper bound on the amount of work necessary to defeat the objective. This is sometimes called the work factor.

B. Functionality

Primitives will need to be combined to meet various information security objectives. Which primitives are most effective for a given objective will be determined by the basic properties of the primitives.

C. Methods of Operation

Primitives, when applied in various ways and with various inputs, will typically exhibit different characteristics; thus, one primitive could provide very different functionality depending on its mode of operation or usage.

D. Performance

This refers to the efficiency of a primitive in a particular mode of operation. (For example, an encryption algorithm may be rated by the number of bits per second which it can encrypt).

E. Ease of Implementation

This refers to the difficulty of realizing the primitive in a practical instantiation. This might include the complexity of implementing the primitive in either a software or hardware environment.

The relative importance of various criteria is very much dependent on the application and resources available. For example, in an environment where computing power is limited one may have to trade off a very high level of security for better performance of the system as a whole.

Cryptography, over the ages, has been an art practiced by many who have devised ad hoc techniques to meet some of the information security requirements. The last twenty years have been a period of transition as the discipline moved from an art to a science. There are now several international scientific conferences devoted exclusively to cryptography and also an international scientific organization, the International Association for Cryptologic Research (IACR), aimed at fostering research in the area.

Cipher plays a significant role in camouflaging the true nature of data; this is achieved by inducing the factor of confusion through a series of shift and other mathematical functions. In the field of cryptography there exist several techniques for encryption/decryption these techniques can be generally classified in to two major groups Conventional and Public key Cryptography, Conventional encryption is marked by its usage of single key for both the process of encryption and decryption whereas in public key cryptography separate keys are used. Further on conventional techniques are further broken in to Classical and Modern techniques [2].

Public key cryptography is also an option when it comes to encryption but it requires excessive communication and processing resources [9].

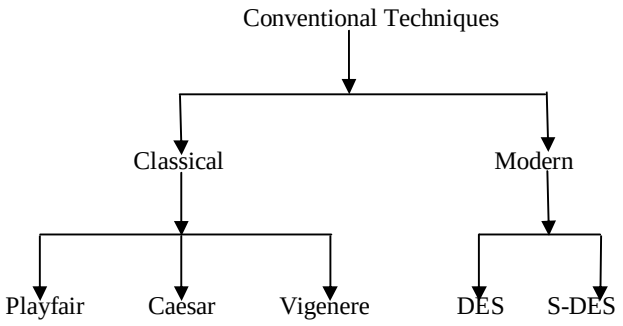

Fig. 1 Depicting some of the techniques of Classical and Modern Encryption

Several encryption algorithms are available and used in information security [3]-[5]. There are several algorithms that can be categorized as classical but out of many [2] will be shedding some light on 3 such techniques:

A. Caesar Cipher

Caesar Cipher is a classical substitution cipher, and one of the simplest example of substitution cipher [7], which replaces the letter of alphabet with a letter that is 3 paces ahead of it [6], for example "ZULU" will be converted in to "CXOX" as one can see that such a cipher may be difficult to break if you are trying to solve it on paper and have no clue of the key, but it has no standing these days in the age of computers and technology and through brute force attack it can be easily broken because in the end there are only 25 possible options of key available.

B. Vigenere Cipher

Vigenere cipher when compared with Caesar gives some level of security with the introduction of a keyword; this key word is repeated to cover the length of the plain text that is to be encrypted example is shown below:

KEY: f a u z a n f a u z a n
P.T: c r y p t o g r a p h y
Cipher: H R S O T B L R U O H L

As we can see from above example that "fauzan" is the keyword and plain text is "cryptography" which was encrypted in to "HRSOTBLRUOHL" this was done using Vigenere table which contains alphabets in form of rows and columns left most column indicates keywords and top most row indicates plaintext and at the junction of two alphabetic letters resides our replacement and after individually transforming every letter we get an encrypted message [2].

C. Playfair Cipher

Another example of classical cipher is Playfair cipher that has a square of matrix of 5X5 alphabetic letters arranged in an appropriate manner [8]. We can select a key and place it in the matrix the remaining letters of English alphabet are then one by one placed in the matrix of Playfair cipher, the plain text is broken in to pairs and if a pair has same alphabet then they are separated by introducing a filler letter like 'x', otherwise if the pair are different alphabetic letters and reside in the same row of matrix then each letter is replaced by the letter ahead of it. If the pair of letters are in same column of matrix then each letter is replaced by the letter below it, and when the pair of letters are neither in same column nor in same row then are they replaced by the letter in their row that resides at the intersection of paired letters.

II. Modern Techniques & Avalanche Effects

Several modern encryption techniques exist but here it will focus on two variants of Data Encryption Standard one is DES other is S-DES.

A. S-DES

Simplified-DES has a process of key generation instead of using key as it is for encryption and decryption the key generation process of S-DES generates 2 sub keys after processing the initial 10 bit input, it has 8 bit plaintext input the two sub keys are generated at both transmission and

receiving ends the two keys are applied to 2 complex functions respectively, with the inclusion of initial permutation, expansion permutations expansions and s-boxes the security is substantial when compared with the classical techniques, S-DES gave some structure and formation to encryption techniques with step to step procedures for both encryption and decryption.

B. DES

DES enhances the structure of S-DES by increasing the key size from 10-bits to 64-bits out of which its affective length is 56-bits [10]. 16 rounds are introduced with each round containing XOR, substitutions and permutations for 16 rounds 16 keys are generated each of 48-bits which strengthens the security of this algorithm further in terms of processing DES is 3 times faster than 3 DES [11]. DES takes plain text in 64-bits of block these 64-bits are divided into 32-bits each the right half of 32-bits goes through the expansion block which increases the bit count from 32 to 48-bits by reusing some bits after expansion block comes XOR operation with the sub-key which is also of 48-bits result of this operation is again of 48-bits these 48-bits now goes into 8 S-boxes the 48-bits are divided in to 8 parts of 6-bits each going in to S-box1 to S-box8 , the overall result of S-box substitution is reduced from 48 to 32-bits which is then XOR with the left half of the initial plain text block to give a 32-bit result which is placed on right and the initial right half of the block is placed at left to get the 64-bit output of 1st round similarly this output of 1st round becomes input of the 2nd round and same procedure is pursued till the 16th round , after 16th round there is a 32-bit swap and finally the bits are placed in inverse permutation table to get the encrypted message reverse method is applied to yield the result.

C. Avalanche Effects

Avalanche effect is the phenomenon that describes the effect in the output cipher text if a single or few bits are changed in the plain text. This change that occurs at the output should be sufficient if we want to create a secure algorithm. Avalanche effect of the proposed technique is given below [2].

KEY**: FAUZANCE**
0100011001000001010101010101101001000001010011100100011010010
PLAINTEXT: **DISASTER**
0100010001001001010100111010000010101001101010100100010101010010
CIPHER:
00010000 0100 000101010111 0100 0111
111100111011 001110001101 11101010

Now it will keep the key same and will introduce 1 character change in plaintext than that plaintext will become "DISCSTER".

KEY: **FAUZANCE**
PLAINTEXT: **DISCSTER**
CIPHER:
11000111 1111 0110 11011100 1111 1100
00101101 0000 1101 00001011 01011111
AVALANCHE EFFECT
Original plaintext's (DISASTER) cipher output
00010000 0100 000101010111 0100 0111
111100111011 001110001101 11101010
Change in one character
11000111 1111 0110 11011100 1111 1100
00101101 0000 1101 00001011 01011111

As it can be seen from the above results that there is 42-bits difference in the cipher of DISASTER and DISCSTER this means that 65.6% bits were changed when we changed a single character of our plain text.

The Avalanche Effect is calculated as [12]:

$$\text{Avalanche Effect} = \frac{\text{No. of bits flipped in the ciphered text}}{\text{No. of bits in the ciphered text}} \times 100\%$$

III. COMPARATIVE ANALYSIS

Encryption Algorithms are considered essential in any secure communication environment. Several encryption techniques are proposed in this regard, one of the recent techniques [2] talks about an algorithm that have surpassed DES, S-DES, Vigenere and Playfair algorithm in terms of Avalanche Effect, in [2] they compared their proposed idea with the above mentioned techniques and found that the proposed technique [2] have better results and Avalanche effect was in the region of 65% in contract to DES which has avalanche effect 54% but a drawback was observed in the proposed technique which was absence of key generation on which the focus in this paper [12] also discusses an algorithm that lacks proper key generation techniques. [12] and [13] has shown that average avalanche effect of blowfish algorithm is 28.71% approximately i.e. change of 19 bits which is much lower than the algorithm proposed by Fauzan and Mustafa [2].

In this technique [2], the amendments were being made in the classical encryption technique which were Playfair and Vigenere used in the algorithm being further enhanced by collaborating with modern encryption technique structure of DES and S-DES. The algorithm begins by producing two sub keys from Playfair and Vigenere to induce more disguise. The plaintext is taken in 64-bit block size which is fixed [2]. Black box is introduced in the algorithm [14] in which 64-bit block size is fed which is divided into 8 octets, these 8 octets takes 8 bits each and these 8 bits are further divided into two parts, R.H and L.H. R.H is of 2 bits and remaining 6 bits are of L.H which is passed through 'special function', these 6 bits are further divided into as first 2 bits represents rows in the 'special function' values box and remaining 4 bits represents column, the value is being selected with the special function selection method by rows and columns values. After the 'black box', the 64 bit block size comes to create more confusion when they are divided into 8 octets where the octets further subdivides into two halves of R.H and L.H dividing 4 bits each. This algorithm provides more efficiency of complexity when all the 4 bits of R.H are being combined together into forming a 32 bits block at R.H and 4 bits of all

L.H are being combined together into L.H forming 32 bits block, the L.H is XORED by R.H and completes the first cycle, this algorithm proposes N=3 cycles of repetitions. The avalanche effect of this proposed method [14] is much better than the classical encryption techniques and modern encryption techniques mentioned in [2]. The Avalanche Effect is 45 bits, 70.31% [14] as compared to DES (35 bits, 54.6%), S-DES (5 bits, 7.8%), Playfair (7 bits, 10.9%), Vigenere (2 bits, 3.1%) [2], Caesar (1 bit, 1.56%) [8], Blowfish (19 bits, 28.71%), Proposed (42 bits, 65.6%) [2].

The following Table -II given below shows the Avalanche effect of various encrypting algorithms.

TABLE II
DEPICTING ALGORITHMS AND THEIR RESPECTIVE AVALANCHE CHANGE IN PERCENTAGE

Encryption Technique	Avalanche Effect	%
DES	35	54.6
S-DES	5	7.8
Playfair	7	10.9
Vigenere	2	3.1
Caesar	1	1.56
Blowfish	19	28.71
Proposed [2]	42	65.6
Proposed [14]	45	70.31

From the above Table – II we come to know that the superiority of the proposed technique [14] when compared with DES, S-DES, Playfair, Vigenere, Caesar, Blowfish and proposed technique [2] in the terms of Avalanche effect.

FIGURE II
INDICATING EFFECT OF AVALANCHE IN VARIOUS ALGORITHMS

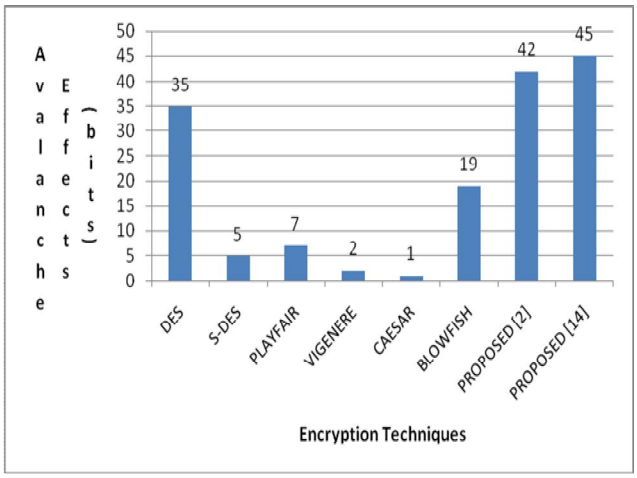

Fig. 2 Indicating effect of Avalanche in various algorithms

Several encryption algorithms are available and used in information security [3], [4], [5]. There are several algorithms that can be categorized as classical but out of many [2] will be shedding some light on 3 such techniques:

IV. CONCLUSIONS

The history tells us that algorithms for modern and classical techniques have been built by many researchers over a long period of time consisting implicitly of something like a worldwide human research network. Despite these intimidating statistics, research indicates that at least the outcome was in the favor of the proposed technique [14], this review showed that in terms of avalanche effect the worst technique is Caesar that gives a difference of 1 bit similarly it is seen that Vigenere giving better results than Caesar by giving a difference of 2 bits, it is also seen that Playfair giving better results than Vigenere by giving a difference of 7 bits DES that uses 16 rounds gave 35 bit difference and proposed [2] gave 42 bits difference when a single character was changed and for the same sample the proposed technique [14] gave an avalanche effect of 45 bits hence it concludes that this technique was superior to the ones mentioned and compared in this review paper. Such an invisible forum, people have made efforts, with “competition and cooperation”, to advance the research effort. In this sense, international conferences and workshops are being organized to stimulate the growth in the area.

REFERENCES

[1] Menezes AJ, Oorschot PCV, Vanstone SA, “Handbook of Applied Cryptography”, Boca Raton, Florida, USA:CRC Press, 1997.
[2] Fauzan Saeed and Mustafa Rashid, “Integrating Classical Encryption with Modern Technique”, IJCSNS, Vol. 10, no.5, May 2010.
[3] M. S. Hwang and C. Y. Liu, “Authenticated encryption schemes: current status and key issues", International Journal of Network Security, Vol. 1, no. 2, pp. 61-73, 2005.
[4] M. H. Ibrahim, “A method for obtaining deniable public key encryption", International Journal of Network Security, Vol. 8, no. 1, pp. 1-9, 2009.
[5] M. H. Ibrahim, “Receiver-deniable public-key encryption", International Journal of Network Security, Vol. 8, no. 2, pp. 159-165, 2009.
[6] William Stallings, “Cryptography and Network Security: Principles & Practices”, second edition, chapter 2 pg 29.
[7] http://www.cs.trincoll.edu/~crypto/historical/caesar.html
[8] V. Umakanta Sastry, N. Ravi Shanker and S. Durga Bhavani, “A Modified Playfair Cipher Involving Interweaving and Iteration”, International Journal of Computer Theory and Engineering”, Vol. 1, no. 5, December, 2009.
[9] Y. C. Hu, A. Perrig, and D. B. Johnson, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks”, Proceeding of IEEE Workshop on Mobile Computing Systems and Applications, 2003.
[10] V. Umakanta Sastry1, N. Ravi Shankar2, and S. Durga Bhavan, “A Modified Hill Cipher Involving Interweaving and Iteration”, International Journal of Network Security, Vol. 11, No. 1, PP. 11-16, July 2010.
[11] Results of Comparing Tens of Encryption Algorithms Using Di®erent Settings- Crypto++ Benchmark, Retrieved Oct. 1, 2008. (http://www.eskimo.com/wei-Dai/benchmarks.html).
[12] Sriram Ramanujam and Marimuthu Karuppiah, “Designing an algorithm with high Avalanche Effect”, IJCSNS, VOL. 11 No. 1, January 2011.
[13] Janan Ateya Mahdi, “Design and Implementation of Proposed B-R Encryption Algorithm”, IJCCCSE, Vol. 209, No. 1, 2009.
[14] Fauzan Saeed, Abdul Basit Abdul Qadir, Yar M. Mughal, Mustafa Rashid, “A Novel Key Generation for FMET”, International Journal of Computer Science and Network Security, Vol. 11, no. 6, pp. 197-202, 2011.