Journal of the Nigerian Association of Mathematical Physics
Volume 57(**June – July** *2020 Issue*), **pp135 – 142**

AN ANALYSIS OF CRYPTOGRAPHY WITH EMPHASIS ON MODERN CRYPTOGRAPHY

S.S. Daodu[1] and E. Akinola[2]

[1]Department of Computer Science, University of Benin, Edo State, Nigeria
[2]Department of Computer Science, The Federal University of Technology Akure, Ondo State

Abstract

Cryptography is the science and study of secret writing. In section 1.0 the background of study is presented. In section 2.0, the literature review is presented. In section 3.0 we presented the areas of applications of modern cryptography and stated its principal objectives which are secrecy and authenticity. In section 4.0, we presented a specific application of modern cryptography. Section 5.0 is the conclusion.

Keywords: Cryptography, Cryptanalysis, Cryptology, Computational Hardness

1.0 Background of Study

According to [19], cryptography is cryptotogy (from Ancient Greek: KPWTLOG, Romanized: kryptos "hidden secret" and $\gamma\rho\alpha\varphi\varepsilon lv$ graphein, "to write" or -$\gamma oyla$ −logia study respectively).

In [24] cryptography is stated as the practice and study of techniques for secure communication in the presence of third parties called adversaries. In [2], it is noted that more generally, cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message share the decoding technique only with intended recipients to prechide access to from adversaries. Restoring the plaintext from the ciphertext is deciphering or decryption. The many schemes used for enciphering constitute the area of study known as a cryptographic system or a cipher. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code". The area of cryptography and cryptanalysis are called cryptology. Encryption has many benefits, but can also be used to conceal criminal activity.

Various aspect in information securing, such as data confidentiality, data integrity, authentication and non-repudiation are central to modern cryptography [20]. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics.

Modern cryptography protects data transmitted over high speed electronic lines or stored in computer systems. Modern cryptography is heavily based on mathematical theory and computer science practice, cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. According to [11], it is noted that two forms of modern cryptography exist: symmetric and asymmetric cryptography.

2.0 Literature Review

In [13] a research tittled "A Hyper Modern Cryptography Algorithm to Improved Data Security: HMCA" was presented. The objective of this research was to improve on block cipher symmetric encryption algorithm that has the same structure of encryption and decryption. The motivation behind this research was to propose their own algorithm to obtain randomization number and encryption number from the initial text key. The methodology used in this research was that an algorithm was devised by inserting a symmetric layer using random number, encryption number and XOR operations in which the whole proposed algorithm uses encryption procedure. The main feature of the encryption/decryption program implementation was the generation of the encryption key. A newly developed technique was discussed in this research named "A new Symmetric Key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm [10] where a substitution method was used by taking 4 characters from any input file and then searching for the corresponding characters in the random key matrix file after getting the encrypted key which is stored in another file. This method can be used for encrypting digital signature watermark before embedding it in some cover file to make the entire system fully secured. The authors also made a comparison of the proposed technique with another newly developed technique named, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology". The proposed cryptography algorithm designed in this research makes use of a random number for generating the initial key. The proposed algorithm uses a 512 bit key size to encrypt a text message and one has to apply a 2^{256} trial run which is intractable. In this technique, there is a common key between the sender and the receiver known as the secret key. This key represents a shared secret between two or more parties that can be used to maintain private information. The block cipher symmetric key was also used in this research because it has a high level of security and efficiency. According to the authors, the technique employed in this research is simple, robust, time efficient, flexible and easy to apply. The limitation of this technique is that it is only applicable to the block cipher method.

Corresponding Author**:** Daodu S.S., Email: segedaodu@gmail.com, Tel: +2348130762937

In [6] a research titled "A Study on Modern Cryptography and their Security Issues" was carried out. The objective of this research was to review a few common encryption Algorithms, their Security levels along with the possible attack that these algorithms might face. A number of factors greatly determine the security of any crypto system and some of which are: the type of algorithm used, number of keys in the algorithm, number of rounds etc. The motivation of this research was based on the fact that due to the exciting developments in the field of cryptography, there has been an urgent need to ascertain the level of security of various cryptographic algorithms which will ensure proper security in transmission of data over wireless network. The most obvious application of any encryption scheme is confidentiality which is a message that a sender encrypts can only be decrypted by the recipient. Cryptanalysts tend to break the methods used in building the system which in turn contributes to the next level of security. According to [6] Modern Cryptography can be classified into Symmetric and Asymmetric key Cryptography. Symmetric Key Cryptography algorithm uses a single key for both encryption and decryption process. The sender uses the key and a certain encryption algorithm to encrypt the data while the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. Symmetric key ciphers are divided generally into two types which are Stream Ciphers and Block Ciphers.

Asymmetric or Public Key Cryptography Algorithm uses two separate keys, one to encrypt plain text and one to decrypt the cipher text. One of the keys is public while the other is private. It is a method of assuring the confidentiality, authenticity and non-repudiability of electronic communications and data storage

The various Data encryption techniques reviewed by [6] are as follows:

a. Data Encryption Standard (DES). This is a symmetric key algorithm for the encryption of electronic data. DES is a block cipher that enciphers 64-bit blocks of data with a 56-bit block of data. The remaining eight bits are used for checking parity. Decryption uses the same structure as encryption but with the keys used in reverse order. DES can be relatively easy to break with an exhaustive key search attack and thus plain DES is not suitable for most applications. However variants of DES in particular 3DES and AES are still secured.
b. In [7] the Diffie-Hellman Key Exchange (DHKE) was developed. This is a specific method of exchanging cryptographic keys. This method allows two parties that have no prior knowledge of each other to jointly establish a shared secret over an insecure communication channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. This method by itself does not provide authentication of the communicating parties and is thus vulnerable to a man in the middle attack. Variants of this method such as STS protocols may be used instead to avoid these types of attack.
c. In [25] a method for obtaining digital signatures was developed. This is a public key Cryptosystem that is used for securing data transmission. In RSA the encryption key is public and it differs from the decryption key which is secret. The public key consists of modulus n and the public exponent e. The modulus n is the product of two large prime numbers p and q. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. The security of this algorithm depends on the difficulty of factoring n into p and q, it also depends on using carefully the selected primes p and q. The enciphering and deciphering functions are mutually inverses, the RSA scheme can be used for secrecy and authenticity.
d. ElGamal Encryption: In [12] this method which is an asymmetric key encryption algorithm for public key cryptography was developed. This is based on the Diffie-Hellman key exchange. Its security is based on the intractability of the discrete logarithm based on the Diffie-Hellman problem. This method is unconditionally malleable and therefore is not secured under chosen ciphertext attack. To ensure adequate security in this encryption algorithm, different random integers should be used to encrypt two messages.
e. Advanced Encryption Standard: This is a symmetric key block cipher which is fast in both software and hardware. This algorithm has a fixed block size of 128bits and a key size of 128,192 and 256bits which is basically a substitution permutation network. There are four stages in every round of AES, they can be implemented on various platforms and they work better in smaller devices. The security margin of this algorithm is large especially if one uses a 192 bit or 256 bit keys.
f. Elliptic Curves Cryptography(ECC). This is also an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields. It has a low key size for the user and a hard exponential time challenge for an intruder to break into the system. In ECC, a 160-bit key provides the same security as compared to the traditional crypto system RSA with a 1024 bit key. The RSA scheme with a 1024 bit key, thus lowers the computing power because of the large size of the key. Therefore ECC offers considerably greater security for a given key size. Security level of 80 bit provides medium term security so, in practice, an elliptic curve bit lengths up to 256 bit are commonly used and they provide security levels of up to 128 bit and this security level is only achieved if cryptographically strong elliptic curves are used.

In [6] only the common cryptography algorithms and their security levels were considered.

According to [18] a research titled "Overview of Modern Cryptography" was presented. The objective of this research was to analyze modern cryptography algorithms based on the number of keys that are used for the encryption and decryption process. The motivation of this research was to define the areas of applications and usefulness of modern cryptography. The various types of cryptographic algorithms considered by the authors are:

a. Secret key Cryptography (SKC). This algorithm uses a single key for encryption and decryption. The key must be known to the sender and the receiver. The biggest difficulty with this approach is the distribution of the key. Secret Key Cryptography is also known as symmetric encryption because a single key is used for both functions. Some secret key algorithms analyzed in this research are:
   i. Data Encryption Standard (DES): This is a block cipher employing a 56-bit key that operates on 64-bit blocks.
   ii. Advanced Encryption Standard (AES): This algorithm uses an SKC scheme called Rijndael, a block cipher designed by Belgian Cryptographers Joan Daemen and Vincent Rijmen. This algorithm can use a variable block length and key length.

iii. CAST-128/256: This is a DES-like substitution-permutation crypto algorithm that employs a 128-bit key operating on a 64-bit block. CAST is named after its developers, Carlisle Adam and Stafford Tavares
iv. INTERNATIONAL DATA ENCRYPTION ALGORITHM(IDEA): This is a 64-bit SKC block cipher that uses a 128-bit key. This secret key cryptosystem was written by [22]
v. Rivest Ciphers: This is a SKC algorithm that is named after Ron Rivest and they are in series: RC1,RC2,RC3,RC4 and RC5
vi. Blowfish: This is a symmetric 64-bit block cipher algorithm invented by Bruce Schneider. They are mostly used for processors with large cache and its key length varies from 32 to 448 bits in length.
vii. TwoFish: This algorithm is a 128-bit block cipher that uses 128-192 or 256-bit keys. They are highly secured, very flexible and very suitable for large microprocessors.

b. Public Key Cryptography(PKC): This cryptographic algorithm makes use of two different keys, one for encryption while the other is used for decryption. This algorithm describes a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key. Public key Cryptography Algorithms that are discussed in this research are:

i. RSA(Rivest, Shamir and Adleman 1978): This algorithm uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number n that is the product of two prime numbers chosen according to special rules. One security feature of RSA is that users can easily stay ahead of the computer processing curve.
ii. Diffie-Hellman (1977): This is algorithm is suitable for secret key exchange only, it is not suitable for authentication or for digital signatures.
iii. DIGITAL SIGNATURE ALGORITHM(DSA): This algorithm provides digital signature capability for the authentication of messages
iv. ElGamal (1985): This PKC algorithm was designed by TaherElgamal and it is used for key exchange.
v. Elliptic Curve Cryptography (ECC). This is a PKC algorithm that is based on elliptic curves. ECC can offer levels of security with small keys compared to RSA. This algorithm was designed for devices with limited compute power such as PDAs, smartcards etc.
vi. Public Key Cryptography Standards (PKCS): They are a set of interoperable standards and guidelines for public key cryptography designed by RSA Data Security inc.
vii. Key Exchange Algorithm (KEA): This is a variation of Diffie-Hellman and it is the proposed key exchange method for capstone.

(c) Hash Functions: Also called message digests and one-way encryption makes use of no key instead uses affixed length has value which is computed based on the plaintext. Hash functions are basically used by operating systems to encrypt passwords as they provide a measure of integrity for a file. Hash algorithms commonly used in recent times are:

i. Message Digest (MD) Algorithms: They are a series of byte-oriented algorithms that produces a 128-bit hash value from an arbitrary-length message. The series are MD2(RFC 1319), MD4(RFC 1320), MD5(RFC 1321).
ii. Secure Hash Algorithm (SHA): This algorithm is basically used for NIST's Secure Has Standard (SHS). The series of this algorithm are SHA-1, SHA-2 and SHA-3
iii. RIPEMD: A series of messages gotten from the RACE Integrity Primitives Evaluation Project. Other variants are RIPEMD-256, RIPEMD-320, RIPEMD-128
iv. HAVAL (Hash of Variable Length): A hash algorithm with many levels of security. They can create hash values that are 128, 160,192, 224 or 256 bits in length.
v. Whirlpool: This is a new hash function designed by V. Rijmen and P.S.L.M Barreto. This algorithm operates on messages less than 2^{256} in length and produces a message digest of 512 bits.

3.0 Areas of Applications

Modern cryptography protects data transmitted over high speed electronic lines stored in computer systems. There are two principal objectives: secrecy (or privacy), to prevent the authorized disclosure of data, and authenticity or (integrity), to prevent the unauthorized modification of data. The authors further stated that information transmitted over electronic live is vulnerable to passive wiretapping, which threatens secrecy and to active wiretapping which threatens authenticity. This is shown in figure 1.

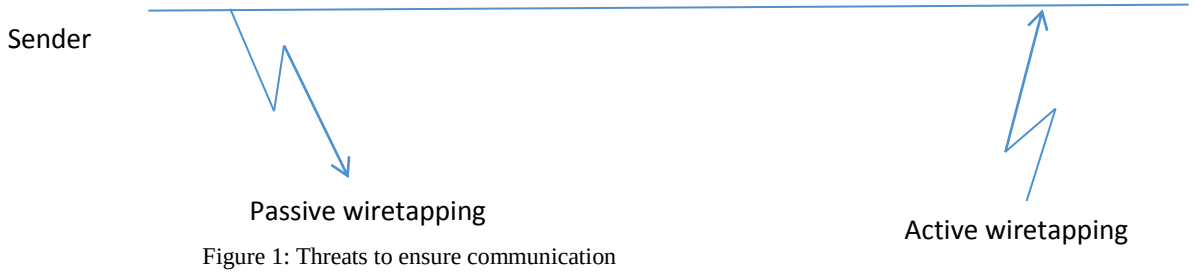

Figure 1: Threats to ensure communication
Source: [8]

In [15], it is stated that modern cryptography intersects the disciplines of mathematics, computer science and electrical engineering. The authors also noted that applications of cryptography include ATM cards, authentication, electronic commerce, cable television networks, and so on.

4.0 Specific Application

Various cryptographic algorithms are been designed by various people in order to achieve some goals such as confidentiality, Data Integrity, Authentication etc. Although public key cryptography is more secured than secret key cryptography, it is difficult to ascertain which one is better as it all depends on the purpose and area of application.

In [26], a research titled "Integrating Classical Encryption with Modern Technique" was presented. The objective of this research is to develop a hybrid encryption technique that is a blend of both Classical encryption as well as modern technique. The motivation of this research was to infuse the strength of the classical encryption with the strength of modern encryption in order to get a higher level of security. In this work, the methodology used was a blend of vigenere cipher with the structural aspects of DES and SDES. According to [26] Some Classical cryptography algorithm isclassified into Caesar Cipher, Vigenere Cipher and Playfair Cipher. In Caesar Cipher, classical substitution is done and it is easily to attack through brute force attack as only 26 possible options of key is available. Vigenere Cipher gives a higher level of security when compared to Caesar Cipher because there is an introduction of a keyword. This keyword is repeated to cover the length of the plain text to be encryptedwhile Playfair Cipher has a square matrix of 5x5 alphabetic letters arranged in an appropriate manner. A key is selected and placed in the matrix; the remaining letters of English alphabets are then placed one by one in the matrix of playfair cipher. The modern techniques discussed in this work by [26] is a hybrid of S-DES and DES Algorithm.

This method deals with the drawbacks of classical techniques that included usage of key as it is without inducing any confusion in the primary key, it was done by generating two sub-keys from the primary key. Similarly the key size of the proposed concept varies from 4 character or 32 bits onwards, it can be 64bits, 128bits. There are also examples of SDES and DES that have fixed key structure. In this hybrid technique, a black box was introduced in which the 64-bit plaintext is divided intotwo halves, left half has 2 bits whereas right half has 6-bits. These 6-bits are fed into a special function block where they are further divided into two halves first two bits represent the row while the last four bits represent column from where the corresponding values are selected. The avalanche effect which is the phenomenon that describes the effect in the output cipher if a single or few bits are changed in the plain text was also considered in this research. Comparison was done between Playfair, Vigenere, S-DES, DES and the hybrid technique. Same key and Plaintext was used for the testing. The example below was used:

S-DES

As S-DES takes 8bit data and 10bit key, they divided the text into two bits, F's 8 bit and 2bits of A to constitute the key in DISASTER and DISCTER. The difference is in the letter A and C, the calculations of these two letters will be the same

0100011001 key F and 2bits of A

A 01000001 of "DISASTER"

Result

01110011

Now change in plaintext from DISASTER to DISCSTER

C=01000011

Result

11001110

Avalanche effect

01000001

11001110

5 bit difference was noted when one character was changed from "A" to "C"

DES

Key:FAUZANCE

0100011001000001010101010110100100000101010011

10010000110100010

Plaintext: DISASTER

0100010001001001010100110100000101010011010101

000100010101010010

Cipher: DISASTER

0101011110100101000001001101101110110001010111

01001110000101011

Cipher: DISCSTER

1111101101010100010010010010111111101110100001

1010011101011101 11

Avalanche effect

When we encrypted our message using DES and changed the same character "A" to "C" the change or avalanche effect gotten was spread over 35bits which is quite significant when compared with S-DES

Playfair
The same key and plaintext was placed in the playfair algorithm and the avalanche effect was calculated as follows
KEY: FAUZANCE
PLAINTEXT:DISASTER
CIPHER: ELPNOYDP

CHANGE PLAINTEXT: DISCSTER
CIPHER: ELOGOYDP

When the two bits are compared, the bits are calculated, the difference was a change in 7-bits.
Viginere

Same data set of key and plaintext were used for vigenere and results were taken

KEY: FAUZANCE
PLAINTEXT: DISASTER
CIPHER: HMBSGGV

When compared the two cipher texts in bits and found the difference to be 2bits
The Hybrid Technique
This technique is a hybrid of both classical and modern techniques were put through the same test

KEY: **FAUZANCE**
010001100100000101010101010110100100000101001110010
000110100010

PLAINTEXT: **DISASTER**
010001000100100101010011010000010101001101010100010
0010101010010

CIPHER
000100001000001010101110101110100011
111100111001110001101111010 10

KEY: **FAUZANCE**

PLAINTEXT: **DISCSTER**
CIPHER
11000111 1111 01100 11011100 1111 1100
00101101 0000 1101 00001011 01011111

Based on the avalanche effect higher in the proposed hybrid technique when compared with the other algorithms, the proposed hybrid technique is reported a more superior method. The limitation of this research is that its computational time is more [26].
In [14] a research titled "Multiphase Encryption": A new concept in Modern Cryptography was presented. The objective of this research was to develop a new encryption technique named Multiphase Encryption. It is an encryption technique that allows data to be encrypted as many times using different strong encryption algorithms at each phase in order to enhance the security of such data. The motivation of this research was to tackle the security challenges that are common in data communications in recent times and also to prevent unauthorized users from using such data for malicious purposes. The methodology used in this research was the use of the multiphase data encryption. Multiphase data encryption describes the enhanced complexity of data encryption due to multiple operations of single phase encryption techniques in cryptography. This methodology encrypts a message twice with some block cipher either with the same key or by using two different keys which would make the resultant encryption stronger with only a few exceptional circumstances. Also using three encryption algorithms produces a greater level of security. An example is shown below:
Original Data/Plain Text – GURUKULA
Algorithm – C=$((P+3)+3)+3 \ldots +3)(N\ Times)$
Cipher Text –
JKOCPUJW(After First Cycle)
MNRFSXMZ(After Second Cycle)
PQUIVAPC (After Third Cycle)
……..
……..
Encrypted $N\ Times$

Multiple encryptions will be repeated a number of times for each phase until it achieves the desired level of security.
Multiphase Data Encryption also described the enhanced complexity of data encryption due to performing the same operation multiple times in an existing way which is the single phase encryption technique. When Multiphase Data Encryption was used, it reduces the problem of key management in the existing technology of Personal Identity Verification (PIV) due to the use of different encryption algorithms with fixed size keys instead of using large number of variable length keys. The limitations encountered in this research were

that (i) the process of the multiphase encryption is complex at the initial phase and (ii) the method also consumes more time when compared to other encryption techniques.

In [1] a research titled "An Overview of Modern Cryptography" was presented The objective of this research was primarily to discuss modern approaches used in cryptography. The motivation of this research was to analyze the types, features, importance and give a brief history of Modern Cryptography in recent times. Modern Cryptography as defined in this research states that it is the process of converting ordinary information (called plaintext) into unintelligible gibberish (called ciphertext) while Decryption is defined as a pair of algorithms that create the encryption and the reversing decryption which is a secret parameter only known to the communicants for a specific message exchange context. In this research, Modern Cryptography was classified into:

a) Symmetric Key Cryptography: This refers to encryption methods in which the sender and receiver share the same key (or which are slightly different and which are easily computable). The modern study of Symmetric Key Ciphers relates mainly to the study of block ciphers, stream ciphers and their applications. This remained the only cryptographic algorithm till June 1976. Cryptographic algorithms considered in this research are Advanced Encryption Standard (AES) and Data Encryption Standard (DES). These algorithms are block cipher designs. DES and its variant are quite popular and they are used across a wide range of applications like in ATM encryption, e-mail privacy and secure remote access. Stream Cipher is another type of Symmetric Cryptographic algorithm. In this algorithm, the output stream is created based on a hidden internal state which changes as the cipher operates. Cryptographic Hash Functions are a third type of Cryptographic algorithm. They take a message of any length as input and output a short fixed length hash function which can be used in a digital signature. A hash function is described as good when an attacker cannot find two messages that produce the same hash. Examples of hash functions are MD4 and MD5.
Message Authentication Codes(MAC) is similar to hash functions but that a secret key can be used to authenticate the hash value upon receipt.

b) In Public Key Cryptography, two different but mathematically related keys are used for encryption and decryption: a secret key and a public key. This Public Key Cryptography is also known as Asymmetric Key Cryptography and it was developed by Whitfied Diffie and Martin Hellman in 1976. A public key is constructed such that the calculation of one key (private key) is computationally infeasible from the other (public key). Even though these keys are necessarily related, both keys are generated secretly as an inter related pair. The public key is used for encryption while the private key is used for decryption.
RSA(Ronald Rivest,Adi Shamir, Len Adleman): This is another public key algorithm which is widely used and it was invented in 1978by Ronald Rivest,Adi Shamir, Len Adleman. Cramer-Shoup cryptosystem, Elgamal Encryption and various Elliptic Curve techniques are other types of cryptographic algorithms. The disadvantage of public key algorithms is that they are slow and they do not allow online encryption.
The limitation of this research is that only a few cryptographic algorithms were discussed in details.

According to the authors [32] Modern Cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman when they presented an article titled "New Directions in Cryptography". The article introduced the revolutionary concept of public key cryptography in order to meet new threats arising from the development of information networks and the massive digitization of documents. Examples of these capabilities are guaranteeing the authenticity of messages (their provenance and contents) and certifying a person's identity which is realized by digital signature algorithms and the latter by identification techniques. Cryptographic Algorithms were classified in this research into Symmetric and Asymmetric Cryptography.

In Symmetric Cryptography, the sender and the receiver share the same secret key both for encryption and decryption. An essential parameter for the security of a secret key system is the size of the keyspace. A secret key encryption offers good security if there is no attack of complexity less than an exhaustive search. In this work, block cipher techniques were also considered. A cipher system is referred to as block if it divides the clear text into fixed blocks and enciphers one block at a time of which the block size is generally 64 or 128bits. Some block cipher techniques discussed here are:

i. DES(Data Encryption Standard): DES operates in 64bits blocks and uses a 56-bit secret key which makes it vulnerable to future exhaustive attacks. Because of this limitation a variant of it known as 3-DES was invented. 3-DES consists of 3successive DES encryption with two secret keys. This technique permits doubling of the secret key size to 112 bits because the use of three different secret keys does not increase the security of the algorithm.

ii. AES (Advanced Encryption Standard):It is an algorithm with 128 bit message blocks which is available in 3 different sizes, 128,192 and 256 bits. AES consists of an iterating permutation which is parametized by a secret subkey which changes at each first iteration. The first iteration is preceded by a bit wise exclusive-or of the cleartext and subkey 0

Public Key Algorithm: This algorithm is also known as Asymmetric Key Cryptography. RSA is the most often used public key system which consists of a secret key and a public key. Decrypting RSA consists of finding the secret key d from the public values (e, n) which can only be secured by factorizing the integer n and currently there are no fast factorizing algorithms for this. Also to be protected from factorizing algorithms, it is necessary that integers p and q with a product of at least 768 bits be used and prime numbers with a 1024-bit product be used.

Digital Signatures consists of appending a small number of bits to the cleartext and this bits depend simultaneously on the message and its author. Signature Scheme is composed of signature and verification functions because it is essential for a signature to be verified but it should not be easy to be forged. Only the owner of the secret key should be able to sign his name and it must be impossible to reuse a signature. There are also principle signature scheme in cryptography, one of which is RSA Signature. In the RSA Signature, certain reversible public key cipher systems are used to construct signature schemes. The signature function corresponds to the decryption function parameterized by the user's secret key and the verification function is derived from the encryption function. In this RSA

Signature, a user signs a message m by applying the RSA decryption function to his secret key$d$. To verify the signature, it suffices to apply the RSA encryption function and also to verify that the result of this calculation corresponds to the cleartext sent.
DSA Scheme is also part of the signature algorithms based on the discrete logarithm of the problem. In 1994, it became the American digital standard for the protection of non-classified information. Its performance scheme is comparable to that of the RSA as a signature scheme. It produces short signatures (as compared to RSA Signatures which are typically 1024 bits) namely 320 bits and offers analogous security and this level of security makes it difficult to forge the signature. In this research, ensuring that cryptography is practically viewed, Hybrid Ciphers, Signatures and Hash Functions are used. Hybrid ciphers are used when a sender wants to ensure the confidentiality of exchanged messages, one does not in general have access to a single type of cipher system. Using a public key algorithm allows a secure exchange of information without preliminary of a shared secret and thekey will also serve to encrypt the exchange of information with the aid of a symmetric algorithm. Combination of the two techniques permits both the speed of secret key encryption and the resolution of the problem of exchanging secret keys between the two interlocutors. They are used practically to encrypt short messages while the hash functions are used in the public key system is relatively short and cannot be used to sign long messages. Most hash functions are improvements of the Message Digest 4 and they have the advantage of compressing messages. Certification of public keys is also a necessity in public key algorithm and this introduces a third party called a witness who validates the link between users and their public keys. A public key certificate consists of clear text and a signature while the clear text consists of a public key and a character string identifying the key owner. The signature corresponds to the digital signature through the witnessing of the preceding text. If this signature is confirmed authentic, it validates the link between the user's identity and his public key.

5.0 Conclusion

In this work we defined Cryptography as the science and study of secret writing. In section 1.0 the background of study is presented, while is section 2.0 the literature review of cryptography with emphasis on modern cryptography was done. In section 3.0, the areas of applications of modern cryptography was presented. We also noted that despite the fact that encryption has many benefits, it can also be used to conceal criminal activity.

References

[1] Al-Vahed, A., &Sahhavi, H. (2011). An overview of modern cryptography. *World Applied Programming*, *1*(1), 55-61.

[2] Bellare M and Rogaway, P (2005), "Introduction to Modern Cryptography"

[3] Chatterjee, D., Nath, J., Dasgupta, S., &Nath, A. (2011, June). A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm. In *2011 International Conference on Communication Systems and Network Technologies* (pp. 89-94). IEEE

[4] C.E Shannon: *Communication theory of secrecy systems*, Bell System Technical Journal, 28 (1949), pp. 656-715.

[5] Daemen, J., &Rijmen, V. (1999). AES proposal: Rijndael.

[6] Das, J. (2014). A study on modern cryptography and their security issues. *International Journal of Emerging Technology and Advanced Engineering*, *4*(10), 320-324.

[7] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, *22*(6), 644-654.

[8] Diffie, W., & Hellman, M. E. (1977). Special feature exhaustive cryptanalysis of the NBS data encryption standard. *Computer*, *10*(6), 74-84.

[9] Dorothy Elizabeth, Robing Denning, "Cryptography and Data Security, Addison- Wesley Publishing Company; 1st edition (June 1982)

[10] Dripto Chatterjee, JoyshreeNath, SuvadeepDasgupta, AsokeNath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.

[11] Edgar, T. W., &Manz, D. O. (2017). *Research methods for cyber security*. Syngress.

[12] ElGamal, T. A. (1985). CRYPTOGRAPHY AND LOGARITHMS OVER FINITE FIELDS.

[13] Gupta, V., Singh, G., & Gupta, R. (2011). A Hyper Modern Cryptography Algorithm to Improved Data Security: HMCA. *International Journal of Computer Science & Communication Networks*, *1*(3), 258-263.

[14] Gupta, H., & Sharma, V. K. (2013). Multiphase encryption: A new concept in modern cryptography. *International Journal of Computer Theory and Engineering*, *5*(4), 638.

[15] Hassan, N. A., & Hijazi, R. (2017). *Data Hiding Techniques in Windows OS*. Syngress..

[16] Islam, M. N., Mia, M. M. H., Chowdhury, M. F., &Matin, M. A. (2008, August). Effect of security increment to symmetric data encryption through AES methodology. In *2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing* (pp. 291-294). IEEE.

[17] Katz, J., Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

[18] Kundalakesi, M. Overview of Modern Cryptography. Stallings

[19] Lidell, H.G, Scott, R, Jones, H.S and Mckenzie, R.(1984), A Greek – English Lexicon, Oxford Press.

[20] Menezes, A. J., Katz, J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

[21] Massey, J. L., & Lai, X. (1992). Device for converting a digital block and the use thereof. *European Patent*, *482*, 29.

[22] Polk, W. T., Dodson, D. F., Burr, W. E., Ferraiolo, H., & Cooper, D. (2006). *Cryptographic algorithms and key sizes for Personal Identity Verification*. US Department of Commerce, National Institute of Standards and Technology.

[23] Robling Denning, Dorothy. Elizabeth. (1982). *Cryptography and data security*. Addison-Wesley Longman Publishing Co., Inc..
[24] Rivest, R.L. (1990), Cryptography, J.VanLecuwen (ed). Handbook of Theoretical Computer Computer Science 1. Elsevier
[25] Rivest, R. L., Shamir, A., &Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.
[26] Saeed, F., & Rashid, M. (2010). Integrating Classical Encryption with Modern Technique. *IJCSNS International Journal of Computer*, *280*, 280-285.
[27] Sastry, V. U., Shankar, N. R., &Bhavani, S. D. (2009). A modified playfair cipher involving interweaving and iteration. *International journal of Computer theory and Engineering*, *1*(5), 597.
[28] Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell system technical journal*, *28*(4), 656-715.
[29] Stallings, W. (2005). Data and computer communications. *Prentice Hall*.
[30] Tanembaum A.S (2009) Basics of cryptography by a.stanebum 2009, Modern Operating Systems, PHI Learning, Private Limited, New Delhi
[31] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol.IT-22, Nov 1976, pp 644-654.(pdf)
[32] Whitfield Diffie and Martin Hellman, "Multi-User Cryptographic Techniques" [Diffie and Hellman, AFIPS Proceedings 45, pp109-112, June 8, 1976]
[33] Available online at: http://www.cs.trincoll.edu/crypto/historical/caesar.html
[34] W. Diffie and M. Hellman, Exhaustive Cryptanalysis of the NBS Data Encryption Standard, June 1977, pp. 74-84
[35] NIST Special Publication 800-78-2, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, February 2010.