International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 05, May 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

CRYPTOGRAPHY (ZOVMQLDOXMEV) -THE ART OF WRITING OR SOLVING CODES

Thota Sunil Raj [1], Dr. S. Krishna Veni [2], Mr. N.V. Siva Krishna [3]

[1,2,3] *Department of Electronics and communication engineering (ECE)*
Gayatri Vidya Parishad College for Degree & PG Courses
School of Engineering, Visakhapatnam (India)

ABSTRACT

The use of technology is instructed but the creation of technology is the sophisticated part of it. Cryptography plays a vital role in Internet security. It is interlinked with the modern organizations to understand the usage of cryptography and its wide range of applications.A phenomenal mixture of existing technologies makes a trendsetter in the evolving fields like quantum computing and it's applications in various fields (quantum cryptography), cloud computing, IOT. For every invention or discovery there will be a massive exploration of knowledge flowing with many ideas in mind and delivering a huge beneficial output to the economy, society. Is random number technique helps for generating the key? What sort of encryption approach and decryption approach takes place? What is the length of the key for ciphers? What is Quantum key distribution (QKD)? Which type of block symmetry is used? ...all these are answered with a brief explanation of our idea in section 5. The main motto is to provide an emphasis on cryptography and an overview of its real-world applications.

Keywords–cryptography, internet security, real-world applications, sophisticated, technology

I. INTRODUCTION

Cryptography is the art of hiding information from spies by means of a secret that isonly known between the communicating ones. A cryptographic technique used in early days is 'Caesar Cipher' [2]. This method uses more or less random substitution table, to hide character frequencies, making it impossible for attackers to rely on counting the number of occurrences of a character. In the digital era, with the usage of modern digital computers, information security made several major steps. Now a day's algorithms are based on mathematical principles and can be used to encrypt any input data. Cryptanalysis [3] made some major ways and algorithms that were previously thought to be unbreakable are now considered some what easy to break.The most important invention in modern cryptography is asymmetric cryptography.

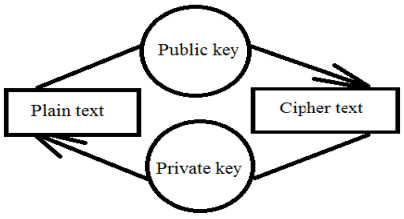

Fig.1.1

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Asymmetric cryptography allows sharing information publicly (a public key) that can be used to encrypt data that can then only be decrypted by someone owning the corresponding secret key (the private key). Modern cryptographic algorithms depend on random data generation, it is therefore very important to use a good random number generator. Most random number generators used on computers today are what so called 'pseudo random number [4]. Cryptographic algorithms always use keys to encrypt or decrypt a required cipher to see the data. The size of these keys is usually expressed in bits (e.g. 128 bits or 1024 bits). It can be very hard to compare the cryptographic strength of different cryptographic algorithms.To overcome this problem, the concept of 'bits of key strength' is often used. This number expresses the number of different keys that would have to be tried to break an algorithm by brute force. Actually, for every extra bit of key strength, the effort required to break an algorithm by brute force doubles. It may decrease overtime if successful attacks are discovered. This has happened for most commonly used algorithm.

II. TYPES OF QUANTUM CRYPTOGRAPHY

In recent years the development of quantum cryptography has become more influencive on many applications. Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best known example of quantum cryptography is quantum key distribution which offers an information-theoretically secure solution to the key exchange problem. It is a recent technique that can be used to ensure the confidentiality of information transmitted between two parties, by using the contrary to intuition behavior of elementary particles such as photons. Quantum key distribution (QKD) [8] uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random secret key known onlyto them, which can then be used to encrypt and decrypt messages. Information regarding photons can't be duplicated. Photons will get tampered if they are measured. The entangled state is pure and how the encryption key is depended on the number of photons reaching to the receiver is to be identified & analyzed.

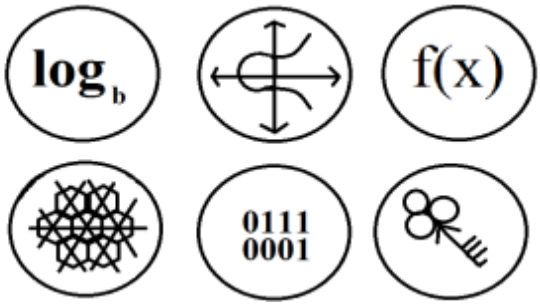

Fig 2.1

2.1 RSA encryption

A message is encrypted using the calculated receiver's public key, which the receiver then decrypts with a private key. The difficulty of computing the private key from the public keys connected to the hardness of prime factorization.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

2.2 Diffie-Hellman key exchange

A shared secret key over an insecure channel that they can then use for encrypted communication. The security of the secret key depends on the hardness of the discrete logarithm problem.

2.3 Elliptic curve cryptography

Mathematical properties of elliptic curves are used to generate public and private keys.The difficulty of recovering the private key from the public key is related to the hardness of the elliptic-curve discrete logarithm problem.

2.4 Lattice-based cryptography

Security is related to the difficulty of finding the nearest point in a lattice with hundreds of spatial dimensions (where the lattice point is associated with the private key), given an random location in space (which is associated with the public key).

2.5 Code-based cryptography

The private key is associated with an error-correcting code and the public key with a scrambled and wrong version of the code. Security is based on the hardness of decoding a general linear code.

2.6 Multivariate cryptography

These schemes depend on the hardness of solving systems of multivariate polynomial equations.

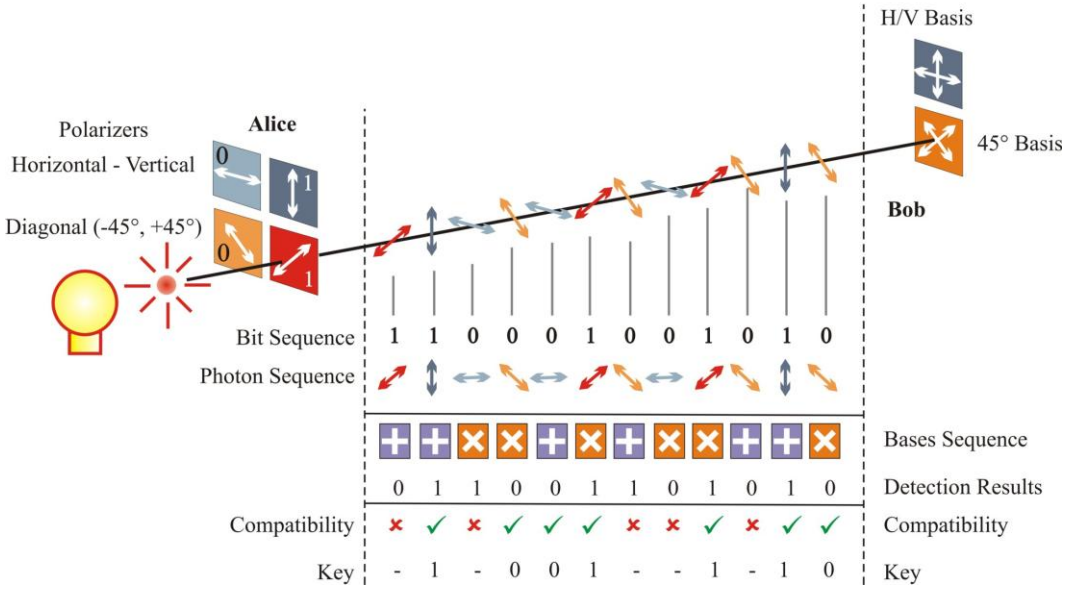

Fig.2.1 [11]

III. DATA ENCRYPTION STANDARD (DES)

A modern derivative of the original DES algorithm is the Triple DES algorithm (also called TDES, TDEA). This algorithm is based on using three DES keys consecutively in encrypt, decrypt and encrypt mode. Triple

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

DES works with either 112-bit keys (where the 1st DES key is also used as the 3rd key, called 2TDEA) or 168-bit keys (with 3 separate DES keys, called 3TDEA). Because of certain properties of the TDEA the effective key-strength of a 168-bit key is 112 bits and the effective key-strength of a 112-bit key is 80 bits. Both DES and TDES are block ciphers. For TDES the cipher block size is 64 bits (8 bytes).The algorithm also has certain properties that make it possible to very efficiently implement in hardware. It is therefore commonly used in embedded systems.

IV. ADVANCED ENCRYPTION STANDARD (AES):

The Advanced Encryption Standard (AES) [6] algorithm is a block cipher with a block size of 128 bits (16 bytes). It supports key lengths of 128, 192 and 256 bits. AES has been thoroughly screened by the cryptographic community and no significant attacks have been found to date. NIST currently believes AES to be secure beyond 2030. DES which is specifically designed for sensitive but not for secret information. But AES has been approved for use in encrypting official material marked 'SECRET' with 128, 192 and 256-bit keys and for use in encrypting official material marked 'TOP SECRET' with 192- and 256-bit keys.

V. OUR EXPLANATION ABOUT THE QUANTUM CRYPTOGRAPHY, FUTURE APPLICATIONS AND AN ALGORITHM TO SOLVE THE CODES: A NEW IDEA!

It's a big idea to cope up with the future technology and the existing ones. Obviously, big ideas have big problems too… so to conquer them, a methodological research has to be done with more ideas and assumptions. The idea of using the evolving technologies leads to greater heights in the innovations and development. It's just an implementation of the idea on this type of application i.e. cryptography. It's a subjective analysis corresponds to grasp the quantum technology into reality.

Quantum computer, which is still in the early stages of research, but they have capacitive use in cryptanalysis. By using Grover's algorithm on a quantum computer, brute-force key search can be made 4 times faster. However, this is possible only by doubling the key length. As we know that the 2048 bit-keys can safeguard the attack for a while, if Shor's and Grover's algorithm is used then the safety level gradually increases. Quantum cryptography [7] has an ability to solve the major long lasting unsolvedand advanced algorithms in shorter time; but quantum computer cannot break all types of cryptographic keys. The quantum cryptography leads to end-to-end encryption which is more securing in the bases of cloud computing, internet protocols, smart cards etc. Cryptography is also used in near field communication, VPN, cloud storage and many more.

Now, we are interested in linking this technology with the other evolving technology i.e., Internet ofthings (IOT). Internet of things deals fully with the sensors which are used everywhere in this world almost in hardware and software devices. The main use of IOT is to communicate with the sensors remotely and get back the required information to their respective person who is handling it and to analyze the data, act upon it, setting the instructions can be done. Many of the devices which are interlinked with the usage of sensors, the security for them are mainly based on the type of cryptographic code. IOT is mainly dependent on the user's confidentiality, security, safety, authentication and certification; all this is possible by the combination of three things i.e., cryptography, quantum based techniques, IOT.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

But the main dilemma in using IOT is mismatching of data or things in the bad zones of IOT. Most of the security issues in IOT are familiar, because they also exist in current internet usage system. An issue can be compared with the detailed analysis of internet. For example, false routing, message tampering, unauthorized usage, DOS attack.We also know that the cryptographic technique tends to: It does not guard against the vulnerabilities and threats that cause from the poor design of systems without security, safety. It is always vulnerable/breakable to brute force attack. Cryptography comes at cost in terms of security, safety, time and money.It depends on the secret key; if we forget the keys then we cannot recover the data back.

We need to manage the keys; generate, distribute and keep them safe and secure in precise manner,which is not always possible to do so.The major disadvantages of implementing the quantum cryptography into existence is

1. Distance and Free Space Communication
2. Lack of Digital Signatures
3. Trojan Horse Attack and many more attacks…

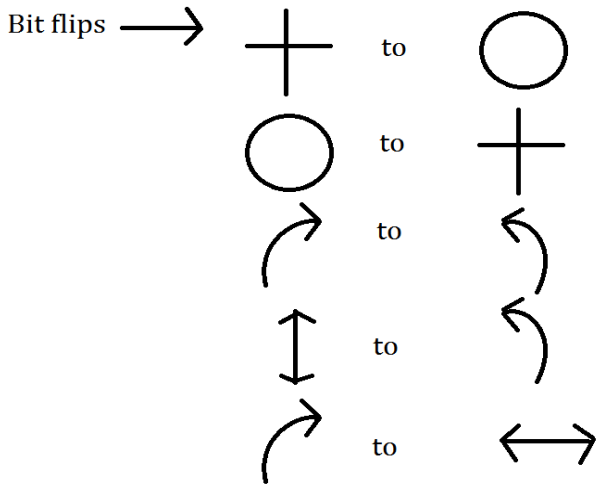

Fig.5.1

QuantumCryptography [9] has a very high weakness of the implementation and lack of algorithms. In future, we can expect that most of the implementation problems in Quantum Cryptography should overcome. It is known that algorithms cannot be implemented in Quantum Cryptography [10] without sacrificing on security.Now we are going to show a new block based symmetric cryptography algorithm. In this technique we are using a random number for generating the initial key, where this key will use for encrypting the given source file using suggested encryption algorithm with the help of encryption number. Basically, in this technique a block based substitution method will be used. In this technique it is used to provide for encrypting message multiple times. The suggested key blocks contains all possible words comprising of number 'n' characters each generated from all characters whose ASCII code is from 0 to 255 in a random order. The pattern of these key blocks will depend on text key entered by the user. Our suggested system is using 512 bit key size to encrypt a text message. It is very difficult to find out two same messages using this parameter. To decrypt any file one has to know exactly what the key blocks is

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

and to find the random blocks theoretically one has to apply 2256 trial run and which is impossible. Initially that technique is only possible for some files such as MS word file, excel file, text file.

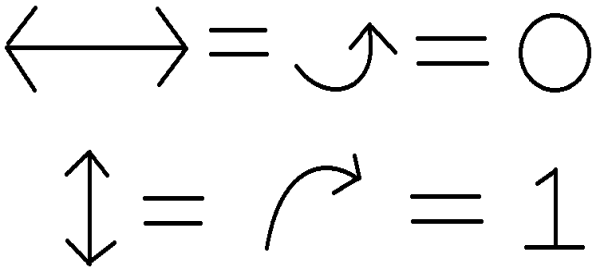

Fig.5.2

Here we are using symmetric encryption approach. We already know that symmetric encryption approach is divided in two types one is block cipher symmetric cryptography technique and another is stream cipher symmetric cryptography but here we are choosing block cipher type because it's efficient and secure. In the above suggested technique we have a common key between sender and receiver, which is known as private key. Basically private key concept is the symmetric key concepts where plain text is converting into encrypted text known as cipher text using private key where cipher text decrypted by same private key into plain text. The encryption key is related to the decryption key, in that they may be identical or there is a simple change in between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain private information. Reasons for use of Symmetric approach for Encryption and Decryption is mainly due to ease encryption process, it's simple. Security, safety is mainly dependent on the length of the key. Keys used for the symmetric-key ciphers are relatively short. Symmetric-key ciphers can be used as first to construct various cryptographic mechanisms. It can be composed to produce stronger ciphers.

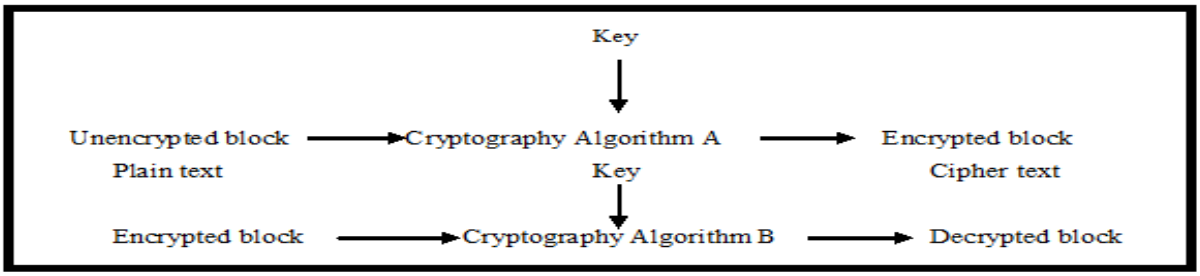

Fig.5.3

5.1. Figures and Tables

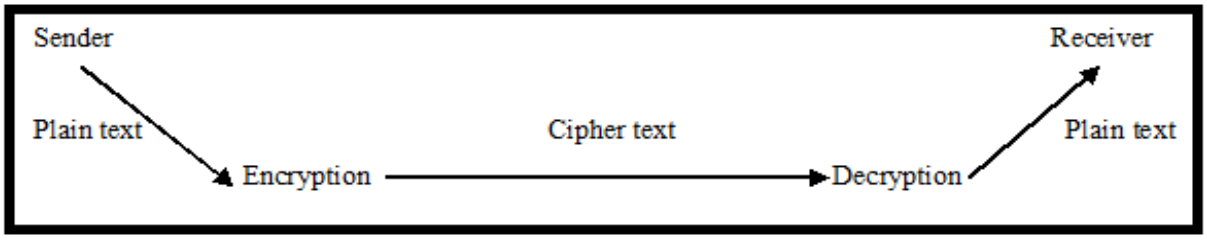

Fig.1.2

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

5.2. Symmetric Key Cryptography

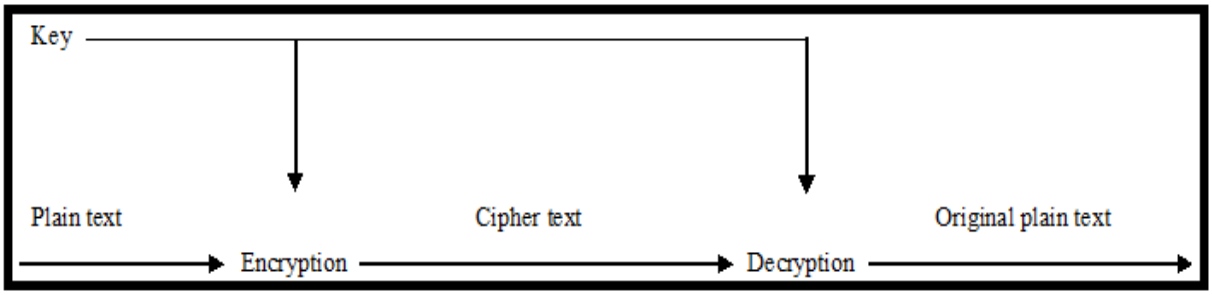

Fig.1.3

5.3.Asymmetric key cryptography

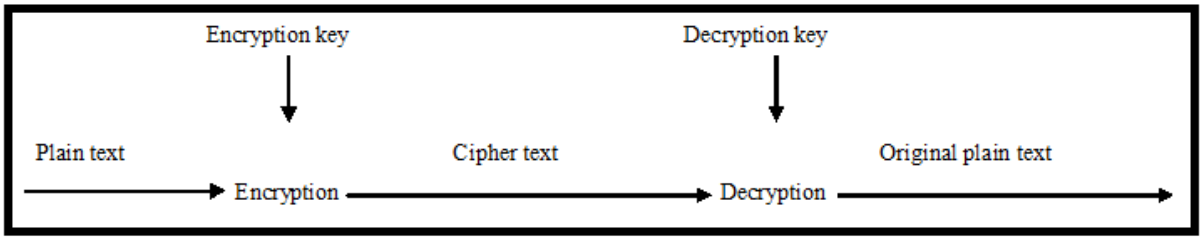

Fig.1.4

VI. CONCLUSION

Cryptography is literally everywhere. It plays an important role in many day-to-day activities; when making a telephone call using a cell phone, purchasing a new computer in a web shop or getting some cash from an ATM, cryptography does its bits to improve the security. It needs to be used correctly in order to add the security of a system. We also know the fact that if cryptography is used in improper manner leads to security disasters. Use 256-bit encryption to keep your filessafe and to trust products. It is lucid when reading thispaper and it is all about encryption (to provide privacy) is separated across many domains and applications. There is no single solution that provides end-to-end protection all the time.

Quantum cryptography is the most complicated technology in the area of quantum information. It is the first quantum concept in the process of making change from purely scientific research to an industrial application. Quantum cryptography has to become practically applicable a lot more progress has to be made to overcome the issue of single photon production, achieving long distances of transmission, understanding all possible attacks. Current key generation rate by using quantum cryptography is in the order of 1000 bits/second. This is definitely very low. This is an important area for future research and developmentand as such something to look out for in the future.Finally, it is important to stay up-to-date with currentdevelopments. Cryptographic theory is a very active field of research and many algorithms that were thought to be secure in the past have proven to bebreakable or vulnerable and are considered to be weak by modern standards and norms.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

VII. ACKNOWLEDGEMENTS

This research was supported by Dr. S. Krishna Veni (M.Tech, Ph. D, MIETE, MSEMC(I), MIE, MIEEE), ELECTRONICS & COMMUNICATION DEPT. &Neelam Siva Krishna, Asst. Prof., Basic Sciences and Humanities. We thank our professors, friends from Gayatri Vidya Parishad College for Degree and PG Courses School of Engineering who provided instigation, insight, zeal and expertise towards cryptography that greatly assisted the research to do with interests. We would also like to show our gratitude towards all the sources that helped us in any manner.

REFERENCES

[1.] http://en.wikipedia.org/wiki/Cryptography
[2.] http://en.wikipedia.org/wiki/Caesar_cipher
[3.] http://en.wikipedia.org/wiki/Cryptanalysis
[4.] http://en.wikipedia.org/wiki/Pseudorandom_number_generator
[5.] Data Encryption Standard (DES), Federal Information Processing Standard 46-3 (FIPSPUB 46-3), Reaffirmed October 1999, http://csrc.nist.gov/publications/fips/fi ps46-3/fips46-3.pdf
[6.] Encryption Standard (AES) to Protect National Security Systems and National Security InformationCNSS Policy No. 15, Fact Sheet No.1, The Committee on National Security Systems, June 2003, http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf
[7.] http://homepage.univie.ac.at/reinhold.bertlmann/pdfs/dipl_diss/PetraPajic_BA_QuantumCryptography.pdf
[8.] https://www.nsa.gov/resources/everyone/digital-media-center/publications/research papers/assets/files/optical-networking-for-quantum-key-distribution.pdf
[9.] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.220.547&rep=rep1&type=pdf
[10.] http://www.iosrjournals.org/iosr-jce/papers/Vol16-issue2/Version-11/A0162110109.pdf
[11.] http://swissquantum.idquantique.com/IMG/jpg/bb84.jpg