International Conference on Recent Researches and Innovations in Sciences, Management, Education and Technology
Jan Nayak Ch. Devi Lal Vidyapeeth, Barnala Road, Sirsa - Haryana, India (ICRRISMET-18)
27th-28th March, 2018 www.conferenceworld.in ISBN : 978-93-87793-16-3

QUANTUM CRYPTOGRAPHY: PERFECT ENCRYPTION FOR 21th CENTURY

Himani[1], Kanchan[2]

[1] *Student, Maharshi Dayanand University, Rohtak*

[2]*Assistant Prof. at SH. L.N. Hindu College, Rohtak*

ABSTRACT

In the present modern technology era, there is advancement in technology everywhere but security takes a back step. Since from ancient times various cryptographic techniques were used for the purpose of Military. Network wherever, whatever, private or public needs to be secured. Network security consists of services, facilities to prevent and monitor unofficial access, wrong usage, alterations, denial of computer network. The word cryptography comes from two Greek words 'Kryptos' mean hidden secrets and 'Graphein' means writing. Cryptography is step towards protection of network and data transmission. It uses coded language that appears as garbage to third party. This garbage actually is encrypted data via cryptography known as Cipher text. Cryptography includes basically encryption and decryption of data to store information securely. It is a crucial issue on World Wide Web but it is to be used correctly. It provides Confidentiality, Integrity, Accuracy. Quantum cryptography is a far more powerful and impenetrable encryption method. Quantum has the potential to affect the relation of codebreakers and code makers. Using Quantum Mechanical principles and methods for encoding and decoding of information could alter the way cybercrimes are committed. Quantum cryptography has become increasingly complex but applicable to many modern products. The use of this cryptography can be found in a wider use of products including bank cards, digital passwords and ultra-secure voting.

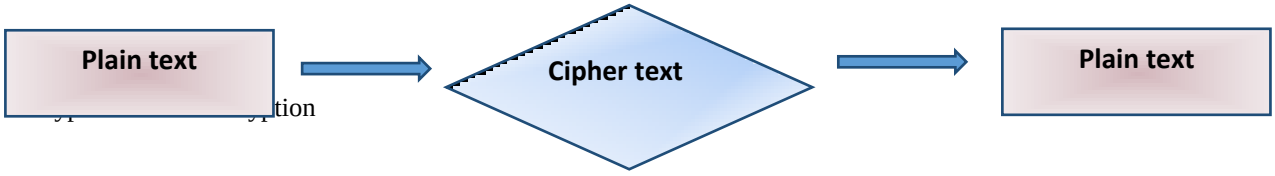
Keywords:Cipher text, Decryption, Encryption.

I. INTRODUCTION

Cryptography came into use thousands of years ago and since then has been constantly developing along with human evolution. *Cryptography*, the art and science of hidden secrets, hasplayed an important role in the history of mankind. It has significantly influence human society. Today, Cryptography has becamean important technology in internet society. In this day and age we have a lot of secrets and we are constantly having to give them away on the internet like credit card number for online shopping. But we don't even know where our information is kept. This challenge of secret keeping is a serious issue. That's why encryption or translating an information in code so that only the right people can read is very important. Now most of the focus is on improving encryption because as computer gets faster and smarter these codes becomes easier to unscramble. That's why we need to apply laws of Physics to improve encryption.Quantum cryptography is a new method for secret communications offering the ultimate security assurance of the inviolability of a Law of Nature.[1]

II. CLASSICAL CRYPTOGRAPHY

To explain the significance of Quantum Cryptography it is necessary to know the basic principle of Cryptography. If we go back up in the history of Cryptography then we saw that initially the purpose of it wasonly limited to Encryption and decryption of data. This is carried with the help of Ciphers where Cipher is the algorithm which is used to transform plaintext to cipher text.*Encryption* is the process of converting information or data into unreadable format by anyone except receiver. *Decryption* is the process to decode the cipher text back to original message.



Basic principle

There are mainly two basic principles of cryptography.

Redundancy: There must be redundancy in the cipher so that it appears as a garbage to intermediate party.

Freshness: This involves freshness of each and every letter of plaintext that within a duration of seconds or even fraction of seconds, it is observed as a code. [2]

Public and Private Keys:

Two kinds of keys are used in Cryptography.

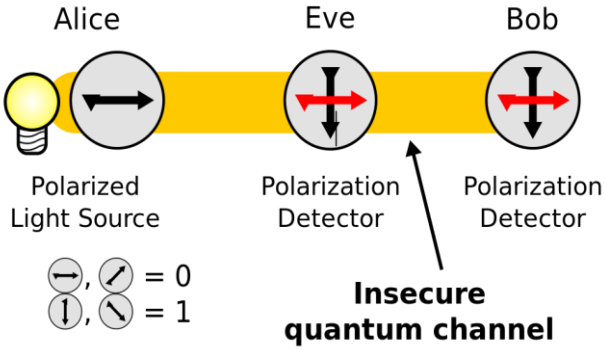
1.) Public Key: This key is used for encryption.

2.) Private Key: This key is also known as Decipher key. This key is used for both encryption and decryption.

One of the key is allocated to each person is called “public key” and is published in an open directory somewhere where anyone can easily look it up. Private is allocated only receiver.

III. Quantum cryptography

The idea of Quantum Cryptography was first proposed in 1970s. It is the method of securing key exchange over an insecure channel based on the nature of photons.Polarized photons are transmittedbetween sender and receiver to create a random string of numbers “a Quantum cryptographic key”.



It gives us perfectly secure data transfer. The first successful quantum cryptographic device could translate a secrete key over 30 centimeters using polarized light, calcite crystal and other electro-optical devices. [3]

IV. QUANTUM KEY DISTRIBUTION

Quantum Key Distribution (QKD) is very secure communication method which uses cryptographic protocols involving components of Quantum Mechanics. QKD is a means of distributing keys from one party to another, and detecting eavesdropping. [3] it enables two parties to produce a shared random secret key known only to them which can then be used to encrypt and decrypt messages. QKD exploits certain properties of various quantum states to ensure its security. QKD requires only an insecure quantum channel and authenticate classical channels, but unfortunately requires multiple rounds of back-and-froth communication between Alice and Bob. Each photon carries one "qubit" of information. Polarization can be used to represent a 0 or 1. A user cansuggest a key by sending a stream of randomly polarizedphotons. This sequence can be converted to a binary key. Ifthe key was intercepted it could be discarded and a newstream of randomly polarized photons sent. This protocol,known as BB84 after its inventors and year of publication, was originally described using photon polarization states to transmit the information. [4]

The sender (Alice) sends message in the form of series of single photons to Bob via a quantum channel.

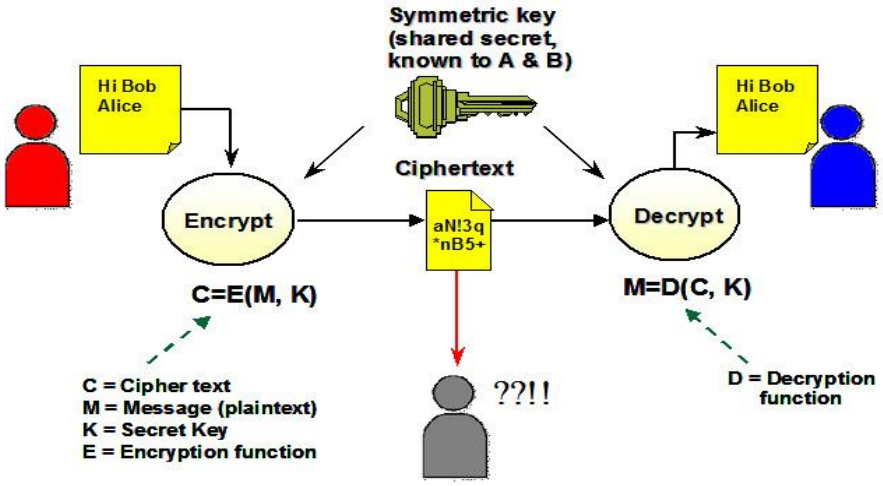
For each photon, it arbitrarily selects one oftwo possible base states, with one of them having the possible polarization directions up/down and left/right, and theother one polarization directions which are angled by 45°. In each case, the actual polarization direction is also arbitrarily selects.

The receiver (Bob) detects the polarizations of the incoming photons, also randomly selecting the base states. Then they use the result using public channel. [5]

After getting an encryption key Bob can encrypt his messages and send them by any public channel. One with the 0-90 degree basis and one with 45-135 degree basis.

Alice uses her polarizer's to send randomly photonsto Bob in one of the four possible polarizations 0,45, 90,135 degree.

Bob uses his polarizer's to measure eachpolarization of photons he receives.He can use the basis or but not bothsimultaneously.



V. CONCLUSION:

Security in digital systems consists of provisions to be made in all policies and infrastructure to protect the network and data from unauthorized access, and consistent and continuous monitoring of its effectiveness and correctness combined together. Quantum cryptography is a far more powerful and impenetrable encryption method. Quantum has the potential to affect the relation of codebreakers and code makers. Using Quantum Mechanical principles and methods for encoding and decoding of information could alter the way cybercrimes are committed.Quantum cryptography promises to reform secure communication by providing security based on the elementary laws of physics, instead of the current state of mathematical algorithms or computing technology.

REFERENCES

[1] Richard J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan and M. Schauer, Quantum Cryptography, LA-UR-95-806.

[2] Prof.Mukund R. Joshi, RenukaAvinashKarkade, Network security with Cryptography, International Journalof Computer Science and Mobile Computing, vol. 4 Issue 1 January-2015, pg. 201-204

[3] RajniGoel and AntenehGirma, Research Directions in Quantum Cryptography, conference paper April 2007, DOI: 10.1109/ITNG.2007.166.

[4] T. Rubyaet. al., A Survey on Recent Security Trends using Quantum Cryptography, (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, No. 09, 2010, 3038-3042.

[5] Miss. Payal P. Kilori and Mr.Pravin.D.Soni, Quantum Cryptography: Realizing next generation information security, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 2, February 2014.

[6] C.H. Bennett, G. Brassard and A.K. Ekert, "Quantum cryptography",Scientific American, pp. 50 – 57, October 1992.

[7] https://en.wikipedia.org/wiki/Quantum_key_distribution.