iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** III **Month of publication:** March 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Performance Enhancement of Computer Network Security with Quantum Cryptography

Raj Kumar[1], Ms. Sandhya Rathore[2]
[1]Associate Professor, [2]Phd Scholar
[1]Dept. of computer Science, Dr. B. R. Ambedkar University, Agra
[2]Department of CS, Himalayan University, India

Abstract: Quantum cryptography uses the law of quantum physics for unconditionally secure data communications. This is a main achievement because the cryptography currently in use, known as conventional cryptography, relies completely on the hardness of a mathematical equation.The advances in quantum computing has threatened the computational security of classical cryptography, which in theory can efficiently compute the hard mathematical problems classical cryptography relies on.This paper makes a comparison between classical cryptography and quantum cryptography and outlines the increased security level provided by quantum cryptography
Keywords: Classical Cryptography, Quantum Cryptography, Shor's Algorithm, Secured Quantum, Cryptography Algorithm

I. INTRODUCTION

Securely transporting messages has been a goal of all major civilizations. The Mesopotamians, ancient Greeks, ancient Chinese, and the Spartans are just a few of the ancient civilizations that used some form of cryptography to keep their messages secret [12].
The ciphers used by these civilizations were advanced at the time, but were certainly not unbreakable. Cryptography has evolved over the years to a much more advanced state that our brains alone are incapable of breaking. The most advanced cryptography to date is quantum cryptography. It was first introduced by Stephen Wiesner in the 1970's, but the paper was not published until 1983 [15].
Quantum cryptography is currently a widely researched topic because of breakthroughs in quantum computing. These breakthroughs in quantum computing threaten the most widely used key distribution systems used today.
Classical cryptography is directly affected by these breakthroughs because it relies solely on the hardness of computing a mathematical problem that cannot be solved by current computers in polynomial time, but theoretically can be solved on a quantum computer.
This realization is what spurred the research in quantum cryptography because quantum cryptography does not rely on computational security, but rather on the laws of quantum physics.
This paper will first give a brief history of classical cryptography and discuss its different kinds. Then quantum cryptography and. the most famous quantum key distribution protocol is taken into account along with a description of what eavesdropping is and how quantum cryptography defends against it.
Finally an overview of the various quantum computing algorithms is given that ends with the introduction of a secured quantum cryptography algorithm proposed by our study.

II. CLASSICAL CRYPTOGRAPHY

Cryptography is the practice and study of hiding information. It manages secret knowledge by taking a message in plaintext and converting it to an unintelligible message to any prying eyes. The need for cryptography is growing exponentially with the number of users that are relying on the internet for a multitude of things, with some of the most prominent uses being E-commerce and online banking.
There are a number of security services that should be addressed by cryptography, with the most important being confidentiality, authenticity, and accountability. Confidentiality protects against unauthorized release of the message, authenticity assures the recipient of the message that the sender is who they say they are, and accountability ensures the sender of the message is accountable for the contents.
These goals are achieved by combining a plaintext message with a key Navleen Kaur et al. and creating cipher text. This cipher text will be unusable to anyone unless they have the key to decode the message. Classical cryptography systems are based on the NP-

hardness of certain mathematical problems, such as factoring two large primes.

These problems are said to be trapdoor functions because it is easy to compute the function one way, but extremely taxing to compute the reverse without some special information, known as the trapdoor [8].

Classical key cryptography relies on the NP-hardness of mathematical problems and does not offer theoretical security, but rather computational security. This poses a great security risk because a breakthrough in mathematics could potentially nullify public key cryptography, which would make transporting symmetric keys with asymmetric cryptography unsecure.

This is a major concern considering most e-commerce and authentication services currently implemented use asymmetric cryptography to transfer the secret key to setup a secure connection between a client and a web server.

III. QUANTUMCRYPTOGRAPHY

Quantum cryptography describes the use of quantum mechanical effects to perform cryptographic tasks or to break cryptographic systems. It offers perfectly secure data transmission because it relies on the laws of physics that we believe to be true, rather than relying on an unproven mathematic problem.

The idea was first proposed in the 1970's but was not applied to information security until the early 1990's. Quantum cryptography is only used to solve the key distribution problem, not actually transmit any useful data. It does so by transmitting photons of light through either fiber optics or free space [2]. These photons of light adhere to the Heisenberg uncertainty principle or quantum entanglement.

The Heisenberg uncertainty principle is when special information is encoded into the properties of a photon so that any attempt to monitor the photon will change the properties and will be detectable. It relies on quantum theory that suggests certain pairs of physical properties are complementary so that measuring one will change the other.

Quantum entanglement is a state of two or more photons that are strongly correlated physically even though they are separated spatially. This means even though they are separated, measurements performed on one system will appear to instantaneously influence the other systems that are strongly correlated [9].

A. Bennett-Brassard (BB84) Protocol

BB84 was the first quantum key distribution protocol and was developed by Charles Bennett and Gilles Brassard in 1984 [3]. Mayer's proof proves that BB84 is unconditionally secure from an attacker that performs any operation allowed under quantum physics [9].

Mayer's proof guarantees the security of BB84 even in the event of a future development in quantum computing, which is a great advantage over all classical key distribution systems. A Vernam one-time pad is most often used in conjunction with the BB84 protocol because the one-time pad is a well known perfectly secure cryptosystem [11][14].

Although BB84 is mathematically proven secure, an implementation of the protocol is not. Problems may arise at the implementation level that will be impossible to foresee in the design level because the protocol may rely on some idealized piece of hardware that simply is not feasible at the time of implementation.

B. Eavesdropping

Eavesdropping is the act of an unintended receiver intercepting and reading a message between two communicating parties. Preventing eavesdropping is one of the main priorities of any key distribution system and quantum key distribution systems have an advantage.

Quantum theory has a principle called the Heisenberg uncertainty principle that guarantees any effort to monitor the communication will disturb it in some detectable way. Although this does not prevent eavesdropping, it will allow the communicating parties to know if someone is eavesdropping.

If someone is detected eavesdropping, the communicating parties can disregard the current key and not lose anything significant since it was a randomly generated key [2].

IV. EXISTING APPROACHES IN CLASSICAL CRYPTOGRAPHY

There are two kinds of cryptosystems: *symmetric* and *asymmetric*. Symmetric cryptosystems use the same key (the secret key) to encrypt and decrypt a message, and asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it.

Symmetric cryptosystems are also called as ***private key*** cryptosystems and asymmetric cryptosystems are also called as ***public key*** cryptosystems. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are the common approaches that come under symmetric key cryptography. RSA, after the name of its inventors (Rivest, Shamir and Adleman) belongs to asymmetric cryptosystems.

It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. But all these techniques of classical cryptography suffer from problems of less security and more complexity.

V. ENHANCING CLASSICAL CRYPTOGRAPHY

A. Quantum Computers

The most widely used public key system is RSA, which relies on the fact that factoring two large prime numbers is an NP hard problem [1]. Factoring a number that is hundreds of digits long will take millions of years using even the fastest supercomputer.

Relying on the hardness of mathematical problems has been the crutch of classical cryptography because whenever computers make gains in terms of computing power, classical cryptography can simply increase the key length, which effectively doubles the key space with each bit.

A newly conceived computer, called a quantum computer, uses the laws of quantum physics and could possibly be able to crack any of the most sophisticated encryptions in use today in a year rather than millions of years. The main difference between quantum computers and classical computers is how information is stored.

In a normal digital computer, information is stored in a bit and encoded as either a 1 or a 0. This means that an n-length word is stored as an n-length string of either 1's or 0's. Quantum computers on the other hand store information in quantum bits (qubits) which can be in a state of 0, 1, or most importantly exist simultaneously as 0 and 1.

This means that n qubits actually requires 2n numbers [13]. Quantum computers have the ability to be immensely powerful because of two major properties: it can be in multiple states at once as well as act on all of its states simultaneously.

A quantum computer, in theory, could perform multiple operations at once on a single processing unit. In November 2007, a company named D-Wave Systems Incorporated unveiled the most powerful quantum computer to date. The quantum computer contained 28-qubits and was running an image matching application [6].

B. Shor's Algorithm

Shor's algorithm, proposed by Peter Shor in 1994, is a quantum algorithm used to factor an integer and can be applied to cracking RSA. Shor's algorithm consists of two parts: First is a reduction, which can be done on a classical computer, of the factoring problem to the problem of order-finding. Second part defines a quantum algorithm to solve the order-finding problem.

The first efficient algorithm to attack the factoring of the product of two large prime numbers, Shor's algorithm sparked a great deal of interest among the scientific community in the quantum computing field.

C. Grover's Algorithm

Grover's algorithm is a quantum algorithm for searching an unsorted database with N entries in $O(N1/2)$ time and using $O(\log N)$ storage space (see big O notation). It was invented by Lov Grover in 1996.

In models of classical computation, searching an unsorted database cannot be done in less than linear time. Grover's algorithm illustrates that in the quantum model searching can be done faster than this; in fact its time complexity $O(N1/2)$ is asymptotically the fastest possible for searching an unsorted database in the quantum model.

It provides a quadratic speedup, unlike other quantum algorithms, which may provide exponential speedup over their classical counterparts.

D. Deutsch–Jozsa algorithm

The Deutsch–Jozsa algorithm, proposed by David Deutsch and Richard Jozsa in 1992 with improvements by Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca in 1998. In the Deutsch-Jozsa problem, we are given a black box quantum computer known as an oracle that implements the function.

We are promised that the function is either constant (0 on all inputs or 1 on all inputs) or *balanced* (returns 1 for half of the input

domain and 0 for the other half); the task then is to determine if *f* is constant or balanced by using the oracle.

VI. SECURED QUANTUM CRYPTOGRAPHY ALGORITHM (SQCA)

Because of the limitations of Classical Cryptography, a new algorithm has been proposed in this paper, SQCA (Secured Quantum Cryptography Algorithm). This algorithm incorporates the effects of Quantum Cryptography and assures more security as compared to any other classical cryptography algorithm studied so far.

In SQCA, we have combined the effects of quantum computing with the classical cryptography. It results into a fast cryptosystem then can't be cracked easily. Here, along with classical Cryptography Algorithm (RSA), we have added the fast speed effect of Shor's algorithm which results in an efficient, secure and faster algorithm.

The complexity of SQCA is O(logN), which is faster and efficient than any classical algorithm(here, RSA). The maximum number of bits that can be supported by this algorithm is also higher as it supports 2N qubits.

Random attacks are not possible in SQCA algorithm and for brute force attack, the maximum key size than can be broken in SQCA is quite large i.e. 1024 bits. The maximum key size than SQCA supports is also large i.e. 256.

TABLE 1 shows a comparison between Classical cryptography and Quantum Cryptography.

Property	RSA	SHOR'S	SQCA
Complexity	*O*(*Nk*)	O((log*N*)3)	O(logN)
No. of bits	N	2N	2N
Key size	512	512	1024
Brute Force Attack	Largest broken 512 bit	Value Largest Broken 512 bit	Value Largest broken1024 bit
Random Attack	2.2 months	< 1 second	Not Possible

A. *Simulation of Secured Quantum Cryptography Algorithm (SQCA)*

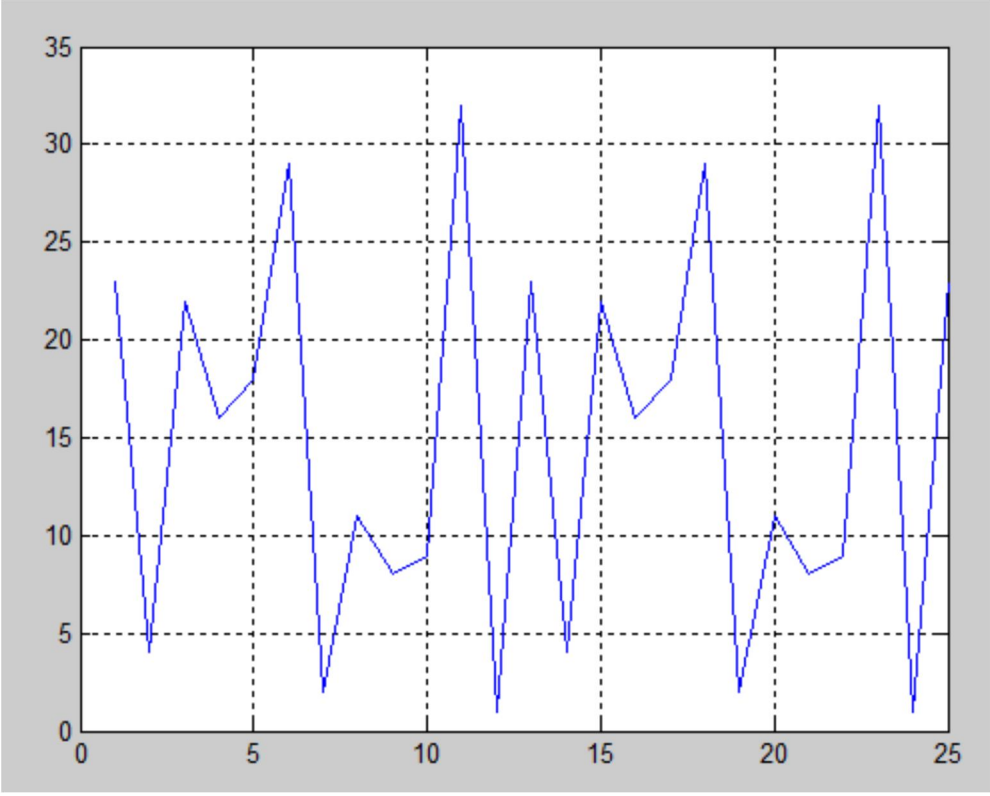


Figure1: Simulation results for SQCA Algorithm

As it is already discussed, the power of any cryptosystem depends on the difficulty that an eavesdropper faces in breaking it. But

with the arrival of Quantum Computing, it becomes easy to crack any cryptosystem.

So, classical cryptography is no longer a secure communication method. Instead of using classical cryptography, now days quantum cryptography is preferred because of its higher security level. All the algorithms which are based on the quantum computing are studied in this paper, starting from Shor's algorithm to the Deutsch-Jozsa algorithm and a new algorithm is proposed i.e. SQCA which utilizes quantum mechanics effects to provide a secure quantum communication channel. SQCA is developed on the quantum entanglement principle of quantum physics.

Quantum Entanglement is a nonlocal property that allows a set of qubits to express higher correlation than is possible in classical systems. In the Figure 1, n shows the number of qubits taken and e shows the interpolation due to quantum entanglement. Simulation of the SQCA clearly shows that with the increase in the number of the qubit selected, corresponding interpolation also get effected and hence the chances of the eavesdropper reduced.

The intruder cannot easily crack the data and if he tries for the random attack then it is almost impossible in the case of SQCA. Brute force attack, however, is possible but it also takes years to achieve it and with the increase in the number of qubits, it reaches next to impossible. SQCA results into a more secured quantum key distribution that is difficult to break. Hence, it ensures a more secured data transfer without any intrusion. Secured Quantum Cryptography Algorithm has some disadvantages also.

It is difficult to implement SQCA algorithm because of the decoherence problem faced by quantum mechanics. Also, the hardware required to implement this algorithm is not available properly. In spite of these disadvantages, it cannot be considered as a failure because its advantages overpower its disadvantages.

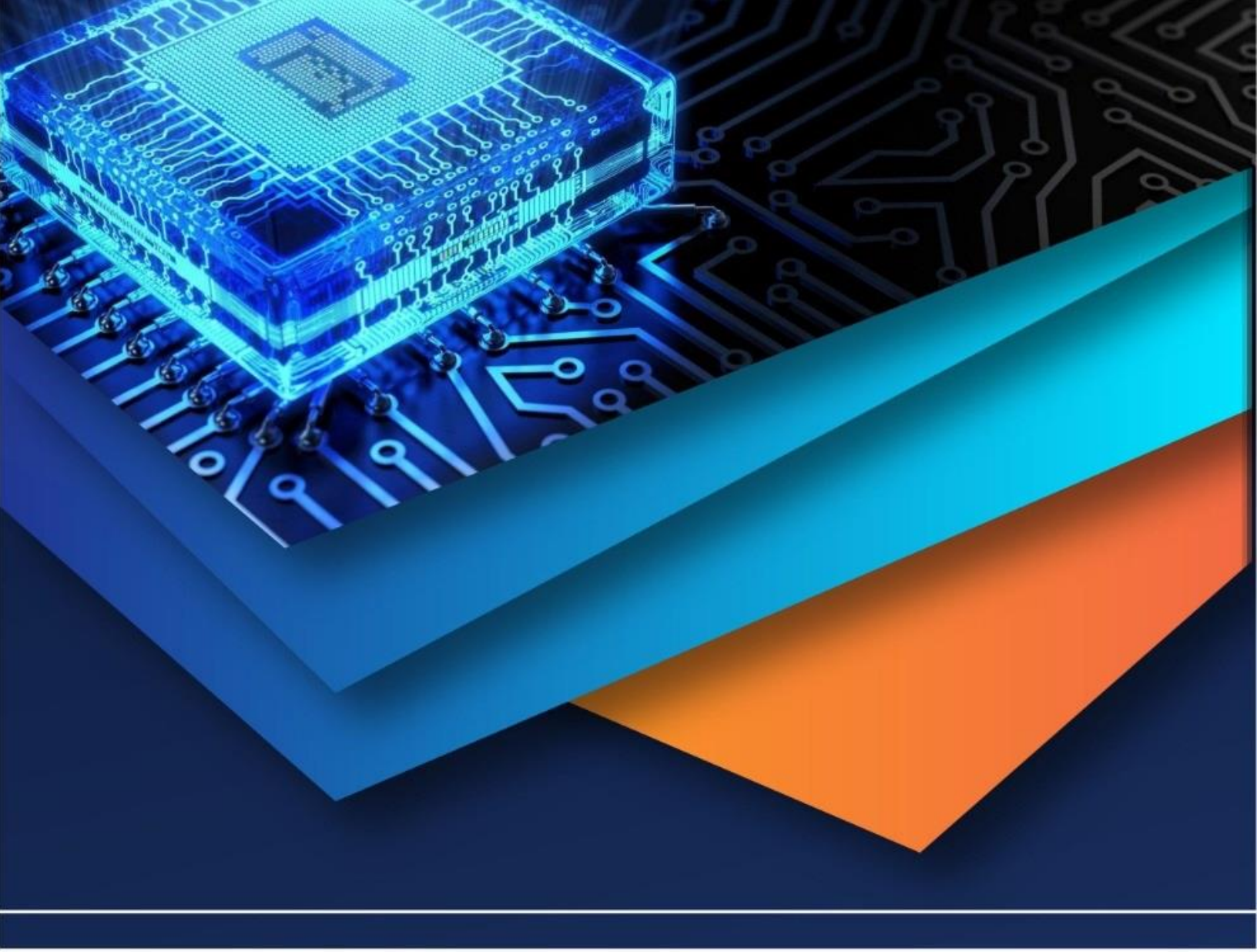
VII. CONCLUSION

Securing data and data communication is a top priority because the consequences of unsecure data can have grave effects on both the economy and national security. Classical key distribution systems are protected only by the limitations of the currently available computing power.

But with the increased computing power of Quantum Computers, classical cryptography is no longer a fully secured communication method. Quantum Cryptography provides more security level then any classical cryptosystem as quantum computing works according to the laws of quantum physics and does not depend on hard mathematical functions. Hence, the resulting Quantum Cryptosystem is more secure and cannot be cracked easily.

REFERENCES

[1] Adleman, L., Rivest, R., Shamir, A 1978., "A method for obtaining digital signatures and public key cryptosystems", Communications of the Association for Computing Machinery.
[2] Bennett, C. H.1992, "Quantum cryptography using any two non orthogonal states", Physical Review Letters, 68, (21), 3121–3124.
[3] Bennett, C. H., Brassard. G. 1984, "Quantum cryptography: public key distribution and coin tossing", Proceedings IEEE international conference on computers, systems, and signal processing.
[4] Bennett, C. H., Brassard, G., Crepeau, C., Maurer, U. M. 1995, "Generalized privacy amplification", IEEE Transactions on Information Theory.
[5] Breyta, G., Chuang, I. L., Sherwood, M. H., Steffen, M., Vandersypen, L. M. K., Yannoni, S. 2001, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance", Nature, 414.
[6] Burnette, E. 2007, "D-Wave demonstrates latest quantum computer prototype at SC07", http://blogs.zdnet.com/Burnette/?p=456.
[7] Choi, K. S., Chou, C. W., Deng, H., Felinto, D., Kimble, H. J., Laurat, J.,Riedmatten, H. 2007, 'Functional quantum nodes for entanglement distribution over scalable quantum networks".
[8] Diffie, W., Hellman, M.E. 1976, "New Directions in Cryptography", IEEE Transactions on Information Theory.
[9] Goel, R., Garuba, M., Girma, A. 2007, "Research directions in quantum cryptography", Information Technology 2007 ITNG '07 Fourth International Conference, 779-784.
[10] Hiskett, P., Hughes R., Lita, E., Miller A., Nam, S., Miller, A., Nordholt, J., Rosenberg, D.2006, " Long-distance quantum key distribution in optical fibre", New Journal Of Physics, 8, (193).
[11] Inoue, K. 2006, "Quantum Key Distribution Technologies", IEEE journal of selected topics in quantum electronics, 12, (4), 888 - 896 .
[12] Kartalopoulos, S.V. 2006, "A primer on cryptography in communications", IEEE Communications Magazine, 44, (4), 146 - 151.
[13] Phaneendra, H.D., Shivakumar, M.S., Vidya, R.C. 2006, "Quantum algorithms and hard problems", 5th IEEE International Conference on Cognitive Informatics, 2, 783 -787,
[14] Vernam, G.S. 1926, "Cipher printing telegraph systems for secret wire and radio telegraphic communications", Journal of the IEEE, 55, 109 – 115.
[15] Wiesner, S. 1983, "Conjugate Coding", Sigact News, 15, (1), 78 – 88 Navleen Kaur et al. / International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3 No. 5 May 2011 1964



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY