Digital Content Security with Quantum Cryptography

Dr. Pushpendra Verma
Assistant Professor, Department of CS, Swami Vivekanand Subharti University, Meerut, U.P., India.
EMAIL - dr.pkverma81@gmail.com

Abstract: *The only perfect cryptographic algorithm that cannot be solved is the One-Time Pad. This algorithm was found in 1917 by Major Joseph Mauborgne. Cipher is included into the group symmetry algorithm. One-time pad system cannot be solved due to two reasons, the first random key sequence added to the plaintext message that does not randomly generate ciphertext completely random, and the second a few rows of the key used to decrypt the ciphertext possible produce the plaintext message that has a meaning, so the cryptanalyst had no way to plaintext determine which one is correct. Even so the algorithm is not used universally in cryptographic applications. The reason is that in terms of practicality, the first since the length of the key should be the same the length of the message, because it is only suitable for short messages. Second, because the key randomly generated must be sent from the sender to the recipient via a network. Key delivery is very vulnerable to attack cryptanalyst. There is a solution that can solve the problem, namely the technology of quantum mechanics also called quantum cryptography. The protocol for this technology is in accordance with the name BB84 maker and the year of publication (Bennett and Brassard, 1984).*

Key Words: *: cryptography, one-time pad, quantum cryptography.*

1. INTRODUCTION:

Cryptography and cryptanalysis are part of a mathematical science called cryptology, where encryption is responsible for encrypting or encoding a message so that only the legitimate recipient is able to decrypt the message content being unreadable to third [1]. Cryptanalysis is the inverse function of encryption, and is responsible for decoding; decipher an encrypted message in order to get access to content. Encryption is the study of mathematical techniques related to aspects of information security, such as, confidentiality, data integrity, and authentication and non - repudiation [2]

Currently encryption is used worldwide in all sectors computerized, using algorithms from simple to very complex algorithms. The safety of these messages It depends on the encryption technique used to encode and decode the message and the size the cryptographic key used. Complex algorithms are required that even with the aid of computers are difficult to decipher. Modern algorithms can be classified into symmetric key algorithms or Asymmetrical where symmetric algorithms are those that use a shared key between transmitter and receiver to be able to encrypt and decrypt the messages, since the algorithms asymmetric, use a key to encrypt messages and one to decrypt them, these algorithms are also known as key algorithms public and private key. Current algorithms are considered safe due to the key size and if basing on mathematical operations that are easy to solve by a path and very complex in reverse, but with the evolution of computing this process of factorization can become simple and easy to solve, and timely research on quantum computing have proven it is possible to factor large prime numbers in a short time. Another major problem is in the process of distribution of keys is currently entrusted to a CDC (Key Distribution Center) that can be vulnerable for failures human, purposeful or accidental. For these reasons researchers are always looking for new forms of encryption to order to achieve always guarantee the security of information, a method that has shown good results is the method of using quantum mechanics to encrypt data, called quantum cryptography.

2. ENCRYPTION:

The encryption that for many years was considered an art is almost as old as the own writing and its origin comes from the Greek alphabet which means hidden writing, but currently the encryption is considered a science that studies how to write secret messages using for this mathematical algorithms and information technology Cryptography is the study of mathematical techniques related to aspects of safety information such as confidentiality, data integrity, authentication and non - repudiation [2].

The main purpose of encryption is to allow the transmission of messages not channels safe using mathematical techniques to make the contents of the message to restricted legitimate recipient [1]. There are two different ways to hide the messages. In the form of steganography, that is, hiding the existence of the message, or encryption which is to make the message unreadable and the party responsible for making the clear text again is cryptanalysis which has the function to decode these hidden or unreadable messages. All cryptographic process obeys certain rules defined, called cryptosystem or cryptographic algorithm [3]. Currently steganography is widely used in the areas of monetary and safety document authentication. Encryption in turn is divided into two major groups: codes

and ciphers, and the figures are divided into transposition and substitution. In the technique transpose the message and the characters of the original message remains intact, only They change places, as the replacement technique some letters or parts of them are changed. Already cryptanalysis has the important task of deciphering "break" cryptosystems to make readable encrypted messages. Encryption also is using cryptographic keys in Most of the figures, which are a kind of password, you have to specify function as transposition or replacement shall be completed [3]. With the popularization of Internet and banking options, shopping, messages, photos, movies the Internet and so many new developments that are constantly emerging encryption evolved along with these systems to make them viable so you could, for example, access your account banking over the Internet without revealing your electronic password to anyone. Encryption turn this divided into symmetric encryption and asymmetric encryption

2.1 Asymmetric encryption

Asymmetric encryption is also called public key cryptography, because the encryption algorithms of this type use a public key and a private key, the key public ensures that everyone who wants to communicate with the receiver may encrypt a message and send it to communication, since the message recipient must have a secret key only he has access, called private key, this key is used to decrypt the original message and so only the legitimate receiver may have access to content. The same happens if the receiver of this message please sends an answer to those who sent this message he must have the public key of the message sender and the sender must have a secret key to decrypt the message response. Asymmetric encryption to ensure the security of your messages uses calculations very complex easy to be solved with the correct secret key, but extremely difficult if not You have the private key. Due to this fact the asymmetric encryption requires processing most of the machine. The encryption or asymmetric public key uses two related keys by mathematical function and the public key encrypts data and decrypts the private key, but these same keys related to each other should be significantly different [1].

Although for this relationship occurs, the encryption algorithm (E) and the algorithm decryption (D) must meet three requirements [1].

- D (E (M)) = M, where M would be the message;
- It is extremely difficult to deduce D E;
- E cannot be deciphered through the plaintext attack chosen

The first requirement states that the decryption algorithm (D) is applied to the cryptogram (E(M)), we obtain the original message (M).

The second requirement is that it will be extremely difficult to deduce the algorithm decryption (D) encryption algorithm (E). The third requirement shows that any personnel may access and analyze the algorithm Cryptography (E) without compromising the confidentiality of the message (M) [1]

2.2 RSA Algorithm

The RSA algorithm was invented by Ronald L. Rivest, Adi Shamir and Leonard Adleman in 1998 is a public key algorithm used in the encryption and extremely systems world. The RSA algorithm is based on the computational difficulty of factoring integers cousins [4].

This algorithm has the feature of using modular arithmetic, a set of keys of at least 128 bit to ensure the security of the cryptosystem. The RSA encryption is very simple to be understood, it uses three mathematical formulas to generate the keys, the first formula is used for choosing prime numbers, the second to the process to generate the data encryption key and the third to generate the decryption key of data.

The RSA algorithm is based on the computational difficulty of Logarithm Problem Discrete, ie, given a prime integers p g t: 0 <g t <p, calculating an integer such that s = T gs mod p, or when p is relatively large is extremely difficult to solve this operation even supercomputers [4]

Example:

p = 17, G = 7, t = 10 s calculate a such that 10 = 7 mod 17, the answer is s = 9. When p is relatively long, this problem is computationally infeasible to be resolved even using supercomputers [4]. To generate the cryptographic keys should follow the following steps: First we have two integers, cousins, random and called distinct p and q. For this choice the process is simple, but it is very difficult to find large integers that meet these conditions, especially if we speak of over 128 bit keys. After this process will begin the process of generating the message encryption key.

Message encryption key

- The public key consists of two numbers and ne. The next step is to use the generated numbers p and q to compute the value of n, where (n = p * q).
- Now use the value of Euler function Φ (n): Φ (n) = Φ (p * q) = Φ (p) Φ (q) = (p-1) (q-1)
- For integer and we must choose a number that satisfies the condition 1 <and <Φ (n) and MDC (and Φ (n)) = 1.

Message decryption key

The private key and also composed of two numbers of n. To generate the key Private already have the number n, now we need only calculate the integer d, for this, We must meet the following two conditions:

1st Condition: 1 <d <Φ (n)

2nd Condition: d * and ≡ 1 (mod Φ (n)).

- The generated keys are:

the public key: (e, n).
the private key: (d, n).

After these processes finalized, we can continue the process of message encoding.

Encoding the message

- To send a message called P, in cryptosystems usually messages are transformed into bit blocks of such fixed, Therefore P is an integer of maximum size known. A condition for this the whole process is that no public key should be greater than Q.
- The message encoding process, called C, is simple and should

satisfy the condition $1 \leq C \leq n$ such that $C \equiv P$ and (mod n).

- This process should be performed in all fixed - size blocks divided above, the encoding process should be applied block by block made it the message is already coded.

Decoding the message

- This process should be performed in all fixed - size blocks divided above, the encoding process should be applied block by block made it the message is already coded.
- The last step is the decoding of the message by the receiver, which should apply private key block to block to decode the original message.

To this must be calculated the following equation: C d (mod n)

- Applying equation block to block, the receiver recovers the original message encrypted by the sender.

3. ENCRYPTION SYMMETRIC:

Symmetric key algorithms, also known as private key algorithms, They have a single key to encrypt and decriptograr messages, thus, both receiver and the sender of the messages must first know the secret key for the process of encoding and decoding can happen. Among the types of encryption symmetric encryption did the first type of encryption exist. It works by translating a text into an encrypted message using a key for it secret used to encrypt and decrypt the clear text [5]. Symmetric encryption is widely used due to its high performance, put in However their problem is that not only the originator of the message must know the key more secret also [5] receiver. Encryption converts data into readable gibberish, with the ability to recover the original data from these data meaningless. This kind of encryption key is called symmetrical. In this approach, an algorithm uses a key to convert the information on what that looks like random bits. Thus the same algorithm uses the same key to retrieve the original data [6

Some cryptographic algorithms safe and efficient, called secret key algorithms (or symmetric) in Alice, with the key K, encrypt a readable text x getting another text Unreadable fK (x) = y. The y text is transmitted to the computer-destination Be to where y is decrypted by the inverse algorithm fK-1 (y) to obtain x if and only if the recipient Bob knows the key K. For those unaware of the key K is computationally difficult to get ya From the knowledge of x, the algorithm is well designed, that is, if it is safe. They are called also symmetric algorithms because the same key K is for Alice and Bob [4

4. ALGORITHM ONE TIME PAD:

The One Time Pad algorithm was invented in 1917 by Gilbert Vernam, this algorithm consists of performing an XOR (exclusive OR), the table below shows an example of this application.

ORIGINAL MESSAGE 0 1 1 0 1

KEY : 1 0 0 0 1

ENCRYPTED MESSAGE:
1 1 1 0 0

It is advisable to use a cryptographic key always greater than the size of the original message to be encrypted, for security reasons, because with a lower key, algorithm can have vulnerabilities, which an experienced cryptanalyst can explore. The number One Time Pad to be considered secure the encryption key must meet four requirements [4]:

i. It must be completely random;
ii. Should be secret and the knowledge of the sender and receiver;
iii. It must be at least the same size as the original message;
iv. It must be used only once;

Given these cryptographic algorithm requirements it becomes almost indecipherable The One Time Pad algorithm despite being extremely safe is difficult to implemented, it is not known to build a generator algorithm truly random keys. The known algorithms generate numbers which are only pseudo-random [4].

5. QUANTUM ENCRYPTION:

Because it is based on the principles of quantum mechanics to quantum cryptography has a unconditional security and establish protocols to exchange keys without communication secret prior [7].

Encryption systems based on mathematical and computational problems managed as acceptable level of secrecy of the decryption exceeds the cost in most cases, the value of information to be discovered. But the way they were designed, are about to become obsolete by new technologies based on quantum theory. also according the principles of quantum only the fact that we observe an object is enough to modify their status and therefore its characteristics [8].

The foundations of quantum cryptography have signed the natural laws of physics, such as mechanics Quantum and not in mathematical difficulties. Quantum mechanics offers unlimited basis for secure key exchange between sender and receiver through the use of photons [5].

Based on this idea quantum communication allows us whenever a person does not authorized interfering with communication are notified because of the change that the intruder cause, this is due to the principle of Heiserberg of uncertainty and the transmission of the change to that the legitimate owners of information from learning occurs by quantum entanglement.

Principles of Quantum Mechanics

Unlike computer that is based on the laws of classical mechanics, computing Quantum is based on quantum mechanics, namely, while the current bit computers may take the value '0' or '1'e only one of these values, quantum computing or quantum bits qubits as they are called, can assume such values '0' and '1' and also the overlapping of the two at the same time.

But what quantum computing can improve the processing machines theoretically threaten the cryptosystems based on complex mathematical operations is related to the registers, for example, a classic register holds 8 bits to store numbers from 0 to 255. Already a register of 8 qubits can not only store the same Numbers from 0 to 255 as well as all of them at the same time, ie a register of n qubits You can store 2n distinct values.

This is a characteristic known as quantum parallelism which shows that the memory a quantum computer would be exponentially larger than the memory of a computer classic, which would promote exponential gain in processing speed of computers.

An algorithm showing these applications is the Shor algorithm that can theoretically decipher the current encryption in a short time [8].

Number length to be factored into *bits.*	**Time to an algorithm classic**	**Time Shor algorithm**
512	4 days.	34 Seconds.
1024	100,000 years.	4.5 minutes.
2048	100 000 billion years.	36 minutes

"Quantum mechanics in further says that light has both a corpuscular nature as wave. Experiments such as the photoelectric effect (Einstein) and Thermal Radiation Blackbody radiator (Planck) showing the particulate nature of light, the light is showing that the formed by photons, elementary and indivisible particles whose mass is equal to zero [7]. " The smallest unit is the light photon which can be set to an electromagnetic field oscillating infinitesimal. The direction of oscillation is known as polarization of the photons [1]

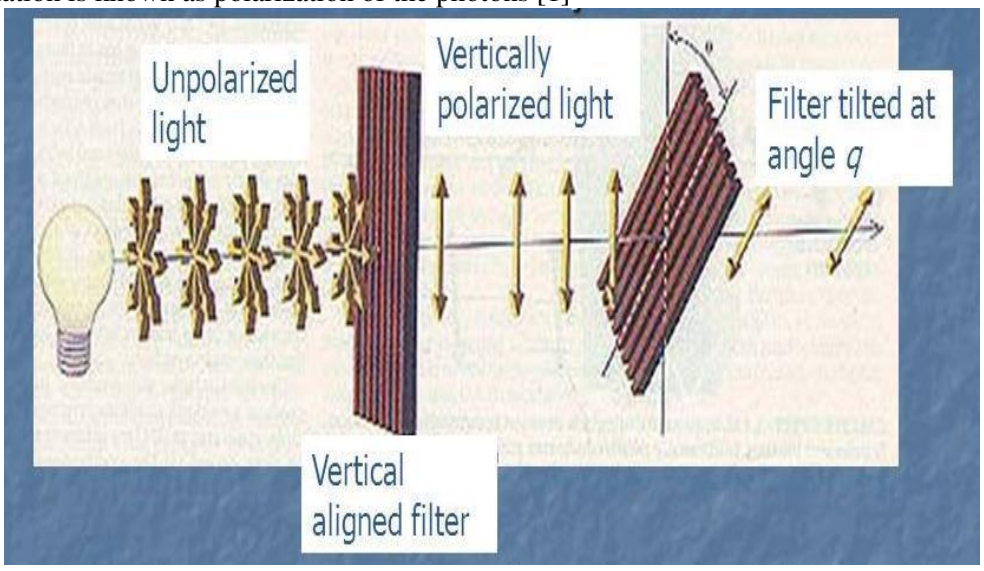
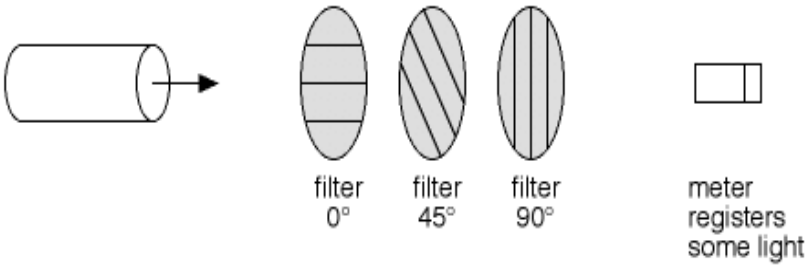


Fig.1

In this figure is represented a source of unpolarized light which in passing by the first filter is absorbed a certain amount of light and the remainder is polarized vertically, in the second filter some amount of light is absorbed and the remainder is polarized at the angle a. The image above shows that given a photon, can change its polarization with use of polarizing filters, such as calcite crystals. Polaroid filters let through photons whose plane of polarization is the same as the "crack" of the filter and absorb photons whose plan polarization is perpendicular to this. "If the photon θ presents a generic bias in relation to the slot of the polarizer, the probability of the photon pass is P = cos2θ, expression known as Reduction Postulate Von Newman. And if it passes, its polarization will be the same as the polarizer. Per example, if θ = 45˚, the probability is 50% of the photon passing polarization and gain equal to the slit polarizer [7]. "

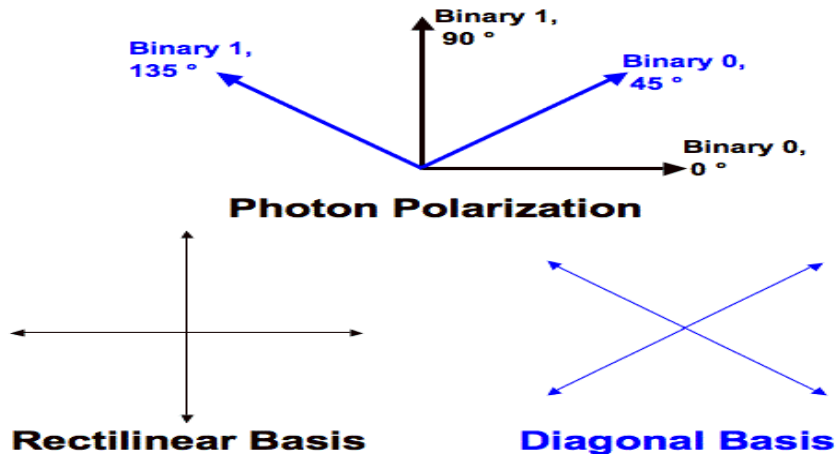


That is, we cannot know exactly the polarization of a photon as to obtain some information on it we will have to use a polarizing filter and still the only information we have of it is, if a photon passes through the filter we can conclude that the photon was polarized parallel to the slot position of the polarizer otherwise conclude that the photon was polarized perpendicular to the slit, if the photon is in any other position there is a probability of the same pass or fail visor slit, this deduction is based on the principle of Heisenberg uncertainty which states that you cannot measure a particle at the subatomic scale without causing disruption to one of its states.

5.1 PROTOCOL BB84 (Bennett and Brassard, 1984)

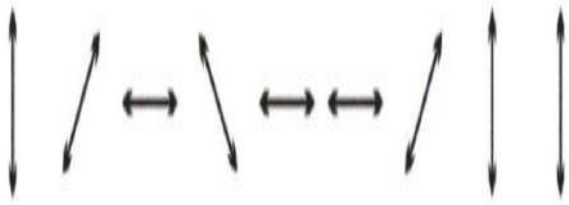
The quantum protocols unlike traditional encryption models need two communications channels with an audience and a quantum channel, for carrying out the encryption. The idea is to use the quantum channel to generate the encryption key and the public channel the encrypted message would be transmitted using, for example, that One Time Pad algorithm. The use of protocols for quantum key distribution can make a high-level security tool and a great help and importance in the process generation of cryptographic keys.

The BB84 protocol, first presents the idea that quantum mechanics can be used to achieve one of the main goals of cryptography, the distribution of a key encryption between two parties (Alice and Bob) who initially do not share any secret information. For this, Alice and Bob must have not only a quantum channel, but also a classical communication channel. The latter can be monitored passively but not actively by external agent (Eva). Through this key, Alice and Bob can with absolute sure to communicate securely. Assuming that Alice and Bob want to communicate and use it for the cryptosystem One Time Pad along as the BB84 protocol, for this they need two channels, and the first is a quantum channel and a public channel the second, Alice sends the quantum channel polarized photons to Bob, using a polarizer to measure them. The public channel they publish messages required for determining the key, but even if these messages intercepted by a third party did not affect the security of communication. They use four polarizations 0 ° and 45 ° (representing bit 0), 90 ° and 135 ° (representing bit 1), as shown below [7].



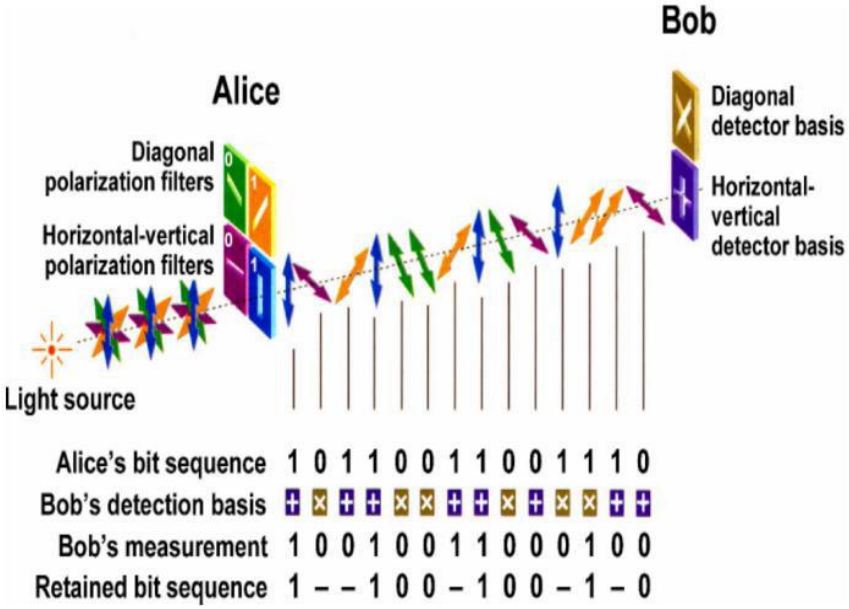
1) Via Quantum Channel (one way communication)

Step 1: Alice randomly chooses polarize photon (measure as bit) to generate photons and send them to Bob using Quantum Channel.



Step 2: Bob receives those photons with randomly chosen polarizes either to use diagonal or rectilinear basis.

2) Via Public Channel (two way communication)
Step 1: Alice will use public channel to tell Bob the polarization she choose for every bit she sent without disclosing the bit value she sent.
Step 2: Bob will compare the list of polarization he got from Alice with the one he generated when receiving.
Step 3: The union of these list can be used as their raw key, which is considered not fully secret, bits maybe tampered by Eve during the transmission.
Step 4: This communication is still continue in public channel and can be divided further in 4 main phases as below in order to obtain the correct key:
- Sifting Raw Key
- Error Estimation
- Error Correction
- Privacy Amplification



6. CONCLUSION:

Given the research presented in this paper, one can know the types of encryption existing and verify the characteristics of each. In general no encryption may be considered safe hundred percent, but both symmetric encryption and asymmetric encryption can be benefited from the inclusion of Cryptographic methods that use protocols for quantum key generation process encryption, making this process much safer as presented in this paper. The RSA algorithm, which has its main problem in the key distribution method, could use quantum protocols to assist in this process, but also if we use the quantum channel for messaging can prevent the intrusion as seen in research is a third attempt to intercept messages immediately the receiver and the transmitter They would know, making it much safer system. But the One Time Pad algorithm, could benefit in the form of generating your keys is point that prevents it from becoming widely used before the quantum protocols had not been invented any algorithm that could generate

cryptographic keys and random bits independent, and with the help of the BB84 protocol that can now become possible. Additionally, the quantum cryptography and quantum computers represent but a threat to current encryption methods, but with the use of these technologies for improvement of known encryption methods can be thought of as quantum cryptography improves security and opportunity in encryption methods and not an imminent threat. Quantum cryptography is becoming a reality and we have to evolve along this process not to let our systems become obsolete and easy to be invaded, it is known that it is too expensive and difficult to implement these systems, and the problem of signal amplification that in certain distances is not feasible, but with the rapid development of technology does not tend to be long to be able to carry out this process. As seen at work research on quantum cryptography are advancing and show very promising with great potential to help us encryption methods, but it is impossible to tell whether the current encryption will be replaced in part or fully by quantum, if worked together, or if the current encryption continued in use without intervention of quantum cryptography. What we predict that the computation is evolve both point encryption become obsolete already have a possible successor quantum cryptography.

REFERENCES:

1. Ergűn GűműŞ, G.Zeynep Aydin and M.Ali Aydin, “Quantum Cryptography and Comparison of Quantum Key Distribution Protocol”, Journal of Electrical & electronics Engineering, vol.8, no.1, 2008, pp. 503-510.
2. Vladimir L. Kurochkin and Igor G. Neizvestny, “Quantum Cryptography”, 10th International Conference And Seminar Edm'2009, Section Iii, July 1-6, Erlagol.
3. D. Mayers, “Unconditional Security in Quantum Cryptography”, Journal of the ACM, Vol. 48, 1998, pp. 351.
4. H.K. Lo, and H.F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances", Science, Vol. 283, 1999.
5. Thi Mai Trang Nguyen, Mohamed Ali Sfaxi and Solange Ghernaouti-Hélie, “802.11i Encryption Key Distribution Using Quantum Cryptography”, Journal Of Networks, vol. 1, no. 5, September/October 2006.
6. IEEE 802.11 Wireless LAN Standards, IEEE 802.11 working group, Task Group I, URL: http://grouper.ieee.org/groups/802/11, March 2006.
7. Nicolas Sklavos, Xinmiao Zhang, “Wireless security and cryptography: specifications and implementations”,2007.
8. B. Schneier, Applied Cryptography, John Wiley & Son, 1996.
9. Xu Huang and Dharmendra Sharma, “Quantum Key Distribution for Wi-Fi Network Security”, IEEE, 2008.
10. C.H. Bennett et al., "Experimental Quantum Cryptography," J.Cryptology, vol. 5, no. 1, 1992, pp. 3–28.
11. J. Postel,” User Datagram Protocol”, RFC 768, 28 August 1980.

Author’s Biography:

Dr. Pushpendra Kumar Verma is working as Assistant Professor in department of Computer science in Swami Viveknand Subharti University Meerut UP INDIA.