Assignment for

IT Applications in Management

Institute of
Management Technology

Project

On

NETWORK SECURITY & CRYPTOGRAPHY

Course Instructor

Mr. ANIL KUMAR

Submitted By:

ROHIT BARVE 2013240

Section E

PGDM 2013-15

Table of Contents

Chapter – I

Introduction

INTRODUCTION

The present century has been one of many scientific discoveries and technological advancements. With the advent of technology came the issue of security. As computing systems became more complicated, there was an increasing need for security. Network Security is becoming more and more crucial as the volume of data being exchanged on the Internet increases. Security is a broad topic and covers a multitude of sins. Malicious people trying to gain some benefit, get attention or to harm someone intentionally cause most security problems.
Network security problems can be roughly divided into 4 closely intertwined areas. They are-

- **Privacy:**

Privacy means that the sender and the receiver expect the confidentiality. The Transmitted message should make sense to only the intended receiver and to all others it is unintelligible.

- **Authentication:**

Ensures that the sender and the receiver are who they are claiming to be

- **Data integrity:**

Ensure that data is not changed from source to destination.

- **Non-repudiation:**

Ensures that the sender has strong evidence that the receiver has received the message, and the receiver has strong evidence of the sender identity, strong enough such that the sender cannot deny that it has sent the message and the receiver cannot deny that it has received the message.

This paper deals with cryptography, which is one of the methods to provide security. It is needed to make sure that information is hidden from anyone for whom it is not intended. It involves the use of a cryptographic algorithm used in the encryption and decryption process. It works in combination with the key to encrypt the plain text. Public key cryptography provides a method to involve digital signatures, which provide authentication and data integrity. To simplify this process an improvement is the addition of hash function.

BASIC IDEA

The goal of cryptography is to make it possible that two people to exchange a message in such a way that other people cannot understand. There is no end that number of ways this can be done, but here we will be concerned with the methods of altering the text in such a way that the recipient can undo the alteration and discover the original text.

Chapter – II

ENCRYPTION

AND

DECRYPTION

ENCRYPTION AND DECRYPTION

Data that can be read and understood without any special measures is called plaintex*t* or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. We use encryption to make sure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called decryption. Figure 1 illustrates this process.

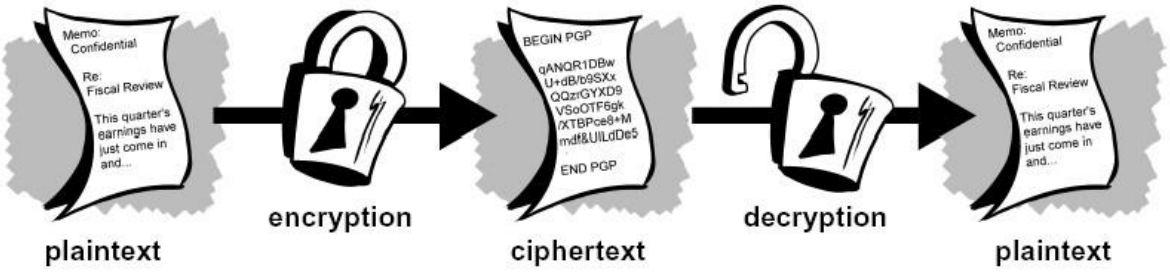


Figure 1-1- Encryption and Decryption

STRONG CRYPTOGRAPHY

Cryptography can be strong or weak, as explained above. Cryptographic strength is measured in the time and resources it would require to recover the plaintext. The result of *strong* cryptography is cipher text that is very difficult to decipher without possession of the appropriate decoding tool. How difficult? Given all of today's computing power and available time—even a billion computers doing a billion checks a second—it is not possible to decipher the result of strong cryptography before the end of the universe.

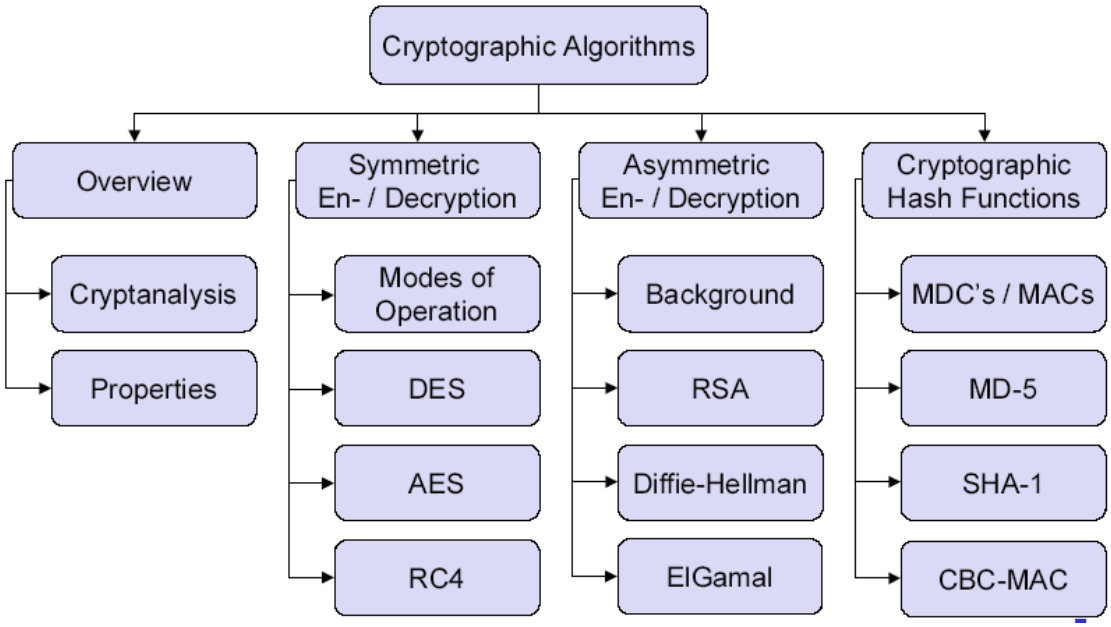
How does cryptography work?

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in Combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work, comprise a cryptosystem. PGP is a cryptosystem.

Cryptographic Algorithms:

Cryptographic algorithms can implemented either hardware (for speed), or in software (for flexibility). There are 3 classes of algorithms they are-

1. Conventional Cryptography (Symmetric algorithms, Private keys)
2. Public key Cryptography (Asymmetric algorithms, public keys)
3. Hash function algorithm.



Conventional Cryptography

In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the U.S. government. Figure 1-2 is an illustration of the conventional encryption process.

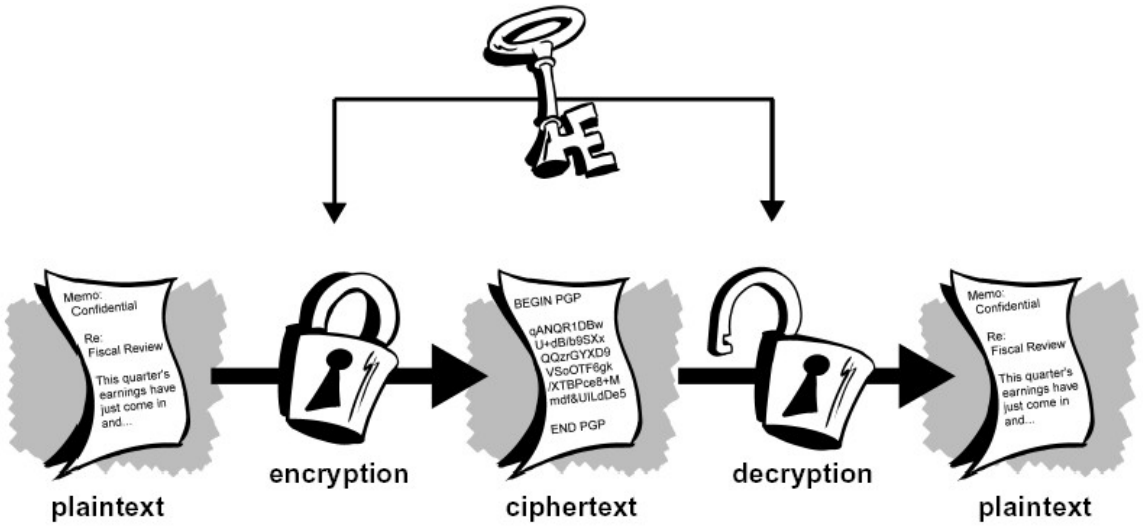


Figure 1-2. Conventional encryption

Public Key Cryptography

The problems of key distribution are solved by public key cryptography. Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private key (secret key) for decryption.

It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.

Keys

A key is a value that works with a cryptographic algorithm to produce a specific cipher text. Keys are basically really, really, really big numbers. Key size is measured in bits; the number representing a 2048-bit key is huge. In public-key cryptography, the bigger the key, the more secure the cipher text. However, public key size and conventional cryptography's secret key size are totally unrelated. A conventional 80-bit key has the equivalent strength of a 1024- bit public key.

A conventional 128-bit key is equivalent to a 3000-bit public key. Again, the bigger the key, the more secure, but the algorithms used for each type of cryptography are very different. While the public and private keys are mathematically related, it's very difficult to derive the private key given only the public key; however, deriving the private key is always possible given enough time and computing power. This makes it very important to pick keys of the right size; large enough to be secure, but small enough to be applied fairly quickly.

Larger keys will be cryptographically secure for a longer period of time. Keys are stored in encrypted form. PGP stores the keys in two files on your hard disk; one for public keys and one for private keys. These files are called key rings. If you lose your private key ring you will be unable to decrypt any information encrypted to keys on that ring.

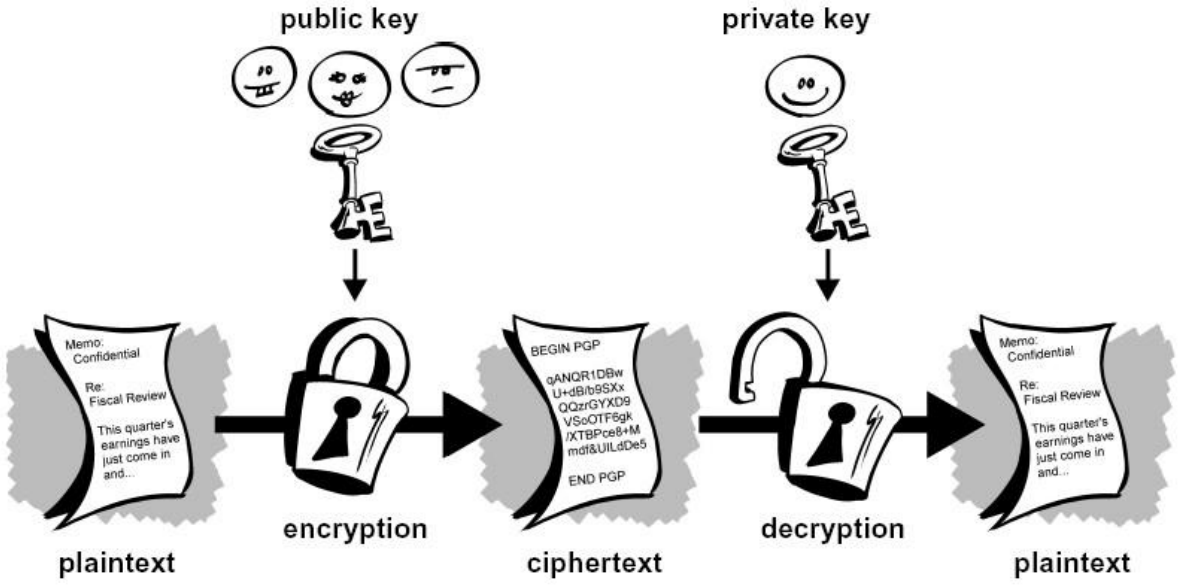


Figure 1-3. Public key encryption

The primary benefit of public key cryptography is that it allows people who have no pre-existing security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. Some examples of public-key cryptosystems are Elgamal, RSA, Diffie-Hellman and DSA, the Digital Signature Algorithm.

Digital Signatures

A major benefit of public key cryptography is that it provides a method for employing digital signatures. Digital signatures let the recipient of information verify the authenticity of the information's origin, and also verify that the information was not altered while in transit. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information. These feature share every bit as fundamental to cryptography as privacy, if not more.

A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as to the identity of the signer.

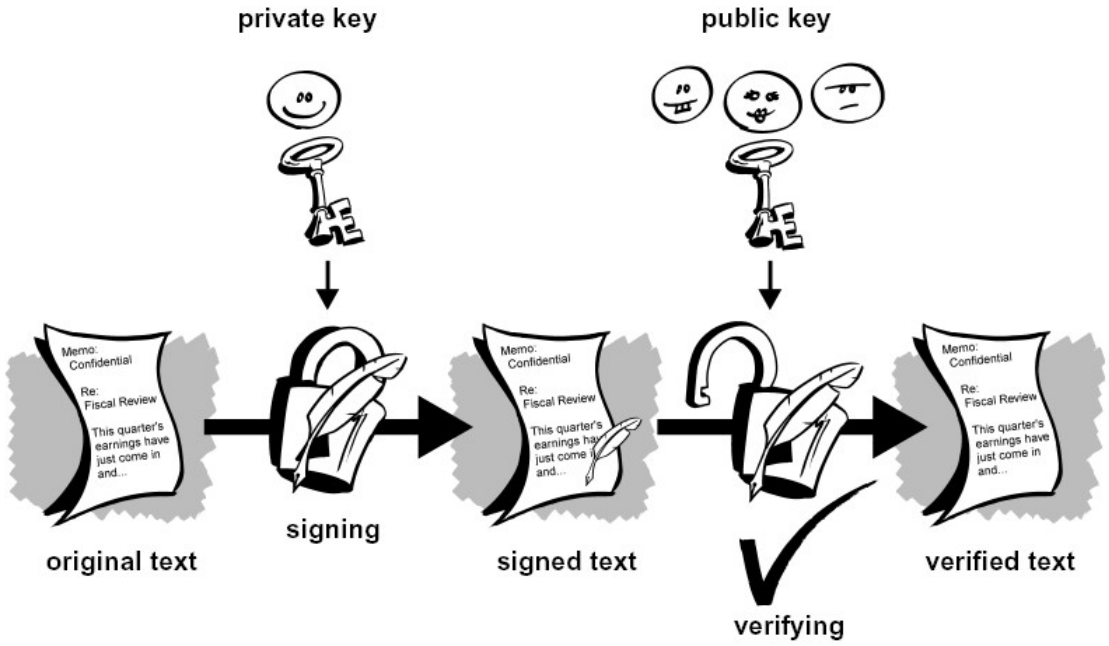


Figure 1-6. Simple digital signatures

Hash Functions

The system described above has some problems. It is slow, and it produces an enormous volume of data—at least double the size of the original information. An improvement on the above scheme is the addition of a one-way hash function in the process. A one-way hash function takes variable-length input in this case, a message of any length, even thousands or millions of bits—and produces a fixed-length output; say, 160 bits. The hash function ensures that, if the information is changed in any way—even by just one bit—an entirely different output value is produced.

PGP uses a cryptographically strong hash function on the plaintext the user is signing. This generates a fixed-length data item known as a message digest. Then PGP uses the digest and the private key to create the "signature." PGP transmits the signature and the plaintext

together. Upon receipt of the message, the recipient uses PGP to recompute the digest, thus verifying the signature. PGP can encrypt the plaintext or not; signing plaintext is useful if some of the recipients are not interested in or capable of verifying the signature.

As long as a secure hash function is used, there is no way to take someone's signature from one document and attach it to another, or to alter a signed message in any way. The slightest change to a signed document will cause the digital signature verification process to fail. Digital signatures play a major role in authenticating and validating the keys of other PGP users.

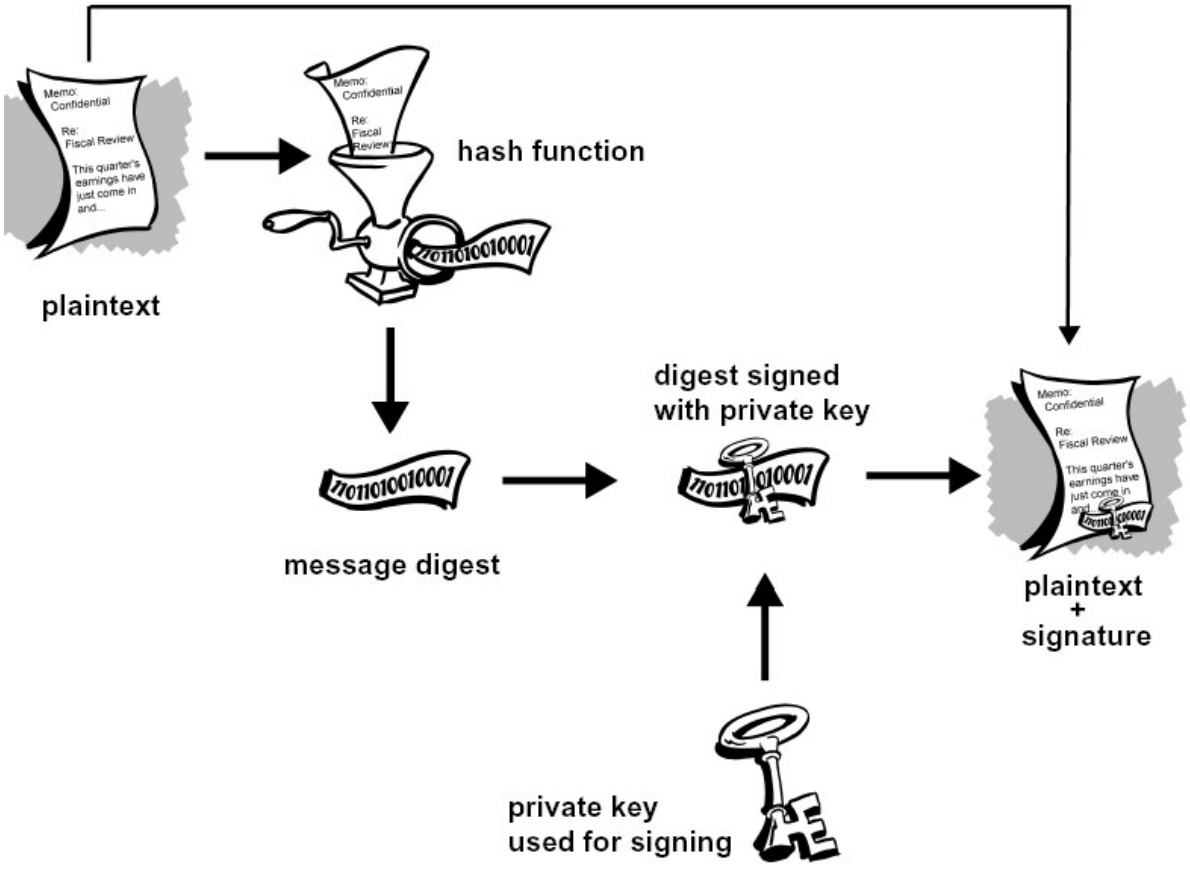
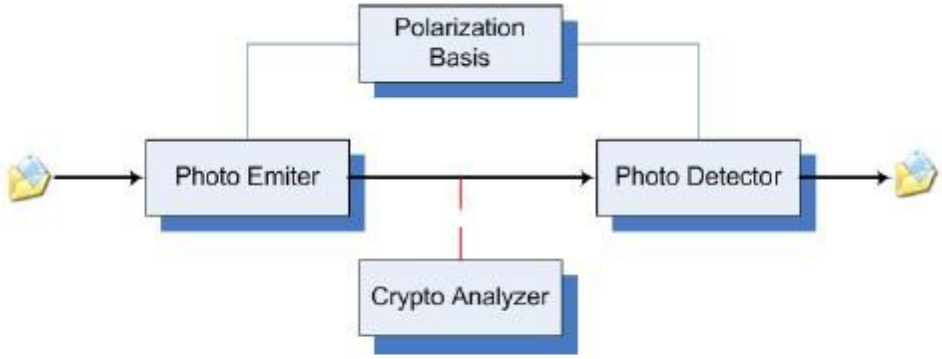


Figure 1-7. Secure digital signatures

QUANTUM CRYPTOGRAPHY - Basic Ideas

Ability to detect eaves dropping

- Detection works only after the information was taken.
- Usually requires classical information channel for effective communication.



Uses of QUANTUM CRYPTOGRAPHY

- Primarily used for key exchange for classical cryptography.
- Key doesn't have any information value.
- The receiver knows if any parts of the key are intercepted.
- Key is random, if intercepted then just generates a new one.

Data Representation:

Two bases are used:

- Vertical
- Diagonal

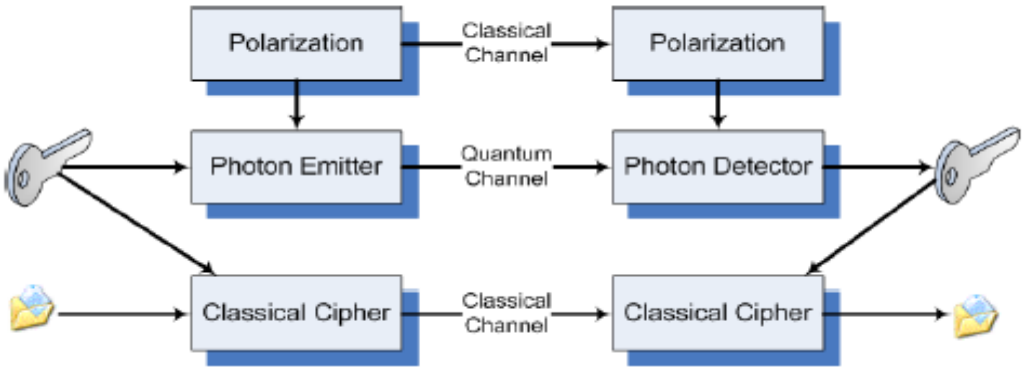
Depending on the bit value the direction on the bases is chosen.

Bit Values:

Polarization	1	0
Vertical	$\lvert\uparrow\rangle$	$\lvert\downarrow\rangle$
Diagonal	$\lvert\nearrow\rangle$	$\lvert\searrow\rangle$

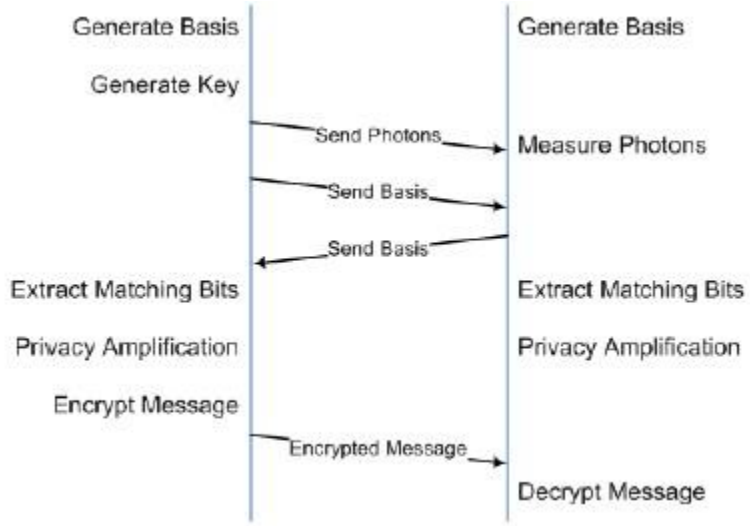
The Exchange:

- The Sequence of events:
  - A generates random key and encoding basis.
  - A sends the polarized photons to B.
  - A announces the polarization for each bit.
  - B generates random encoding basis.
  - B measures photons with random basis.
  - B announces which basis are the same as A's.



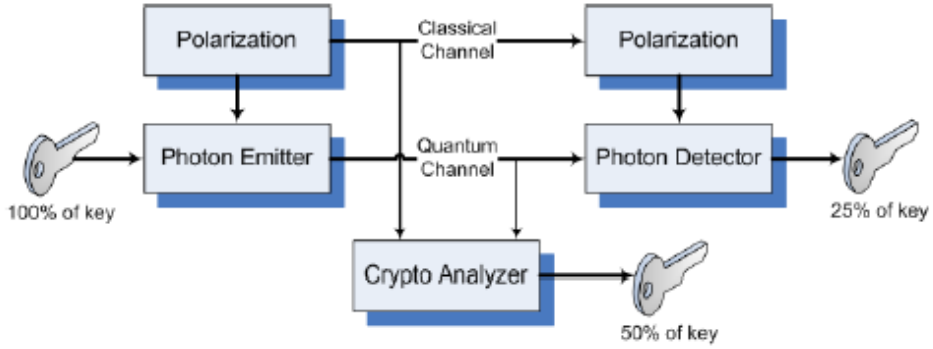
- Finally, the matching bits are used as the key for a classical channel.

Sequential View:



EAVESDROPPING

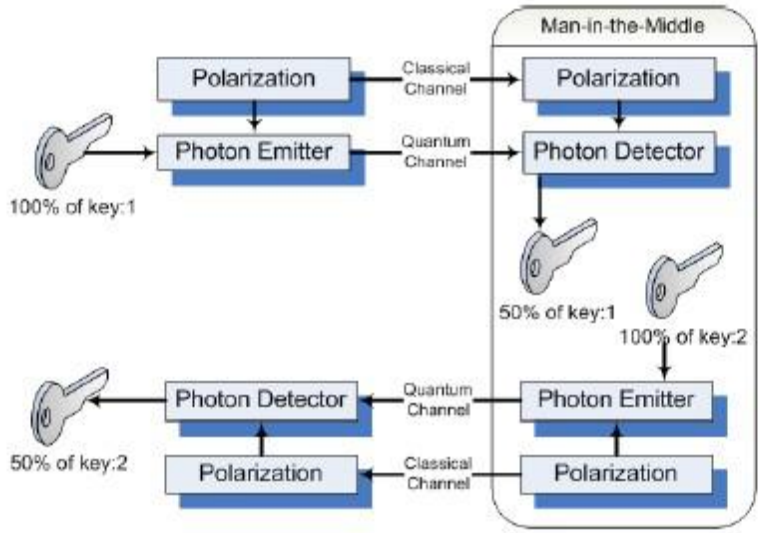
Eavesdropping on the quantum channel requires measuring the photons, therefore perturbing the system.



Eavesdropper will be required to resend the photons at random polarization; the receiver will end up with 25% of the key.

MAN - IN THE - MIDDLE ATTACK:

Requires the attacker to take over both classical and quantum channels. It can be prevented by authenticating the messages on the classical channel.



ADVANTAGES AND DISADVANTAGES:

- Based on natural quantum laws
- Computational Complexity Expires.
- There is no expiration date on the security of QC messages.
- Perfect for public communication
- Easy to detect an eavesdropper.
- Severally limited by technology
- Practical systems are limited by distance.
- Photon emitters and detectors are far from perfect, causing a lot of errors.
- Most protocols require a classical channel.

Chapter – III

CONCLUSION

AND

REFRENCES

CONCLUSION:

As the proverb says that "Even a crow can peck an elephant which is stuck in the mud". Even though we are providing high security by cryptography there are many pitfalls in it also. Nothing in the world is 100% secured. Cryptography is one of the way to provide network security but it is not only the path to achieve network security.

REFERENCES:

i. "Cryptography and Network Security, Principles and Practices" --- (Third Edition)-William Stallings.

ii. "A Method for obtaining Digital Signatures and Public Key Cryptographic Systems." ---Rivesp.R , Shamir.A and Adleman.L

iii. "Multiuser Cryptography Techniques." -- Diffie.W and Hellman.M

iv. www.rsasecurity.com/rslab/intro.html

v. www.howstuffworks.com

vi. www.wikipedia.com