UNIT V – QUANTUM CRYPTOGRAPHY AND EMERGING APPLICATIONS

Classical Cryptography Review – Public and Private Key Cryptography – Quantum Key Distribution (QKD) – BB84 Protocol – E91 Protocol – Post-Quantum Cryptography – Quantum Security Concepts – Shor's Algorithm and RSA Vulnerability – Quantum Computing in Artificial Intelligence – Quantum Machine Learning – Healthcare – Finance – Cybersecurity – Smart Manufacturing – Quantum Digital Twins – Challenges, Ethics, Sustainability and Future Trends.

Classical Cryptography and Quantum Cryptography

Cryptography is the technique that is used for secure communication between two parties in a public environment where unauthorized users and malicious attackers are present. In cryptography, there are two processes i.e. encryption and decryption performed at the sender and receiver end respectively.

Encryption is the process where simple multimedia data is combined with some additional data (known as a key) and converted into an unreadable encoded format known as a Cipher.

Decryption is the reverse method of encryption where the same or different additional data (key) is used to decode the cipher and it is converted into real multimedia data.

Cryptography techniques can be categorized according to the basic principles or protocols they follow. But here we are going to concentrate on the two types of cryptography techniques namely Classical Cryptography and Quantum Cryptography.

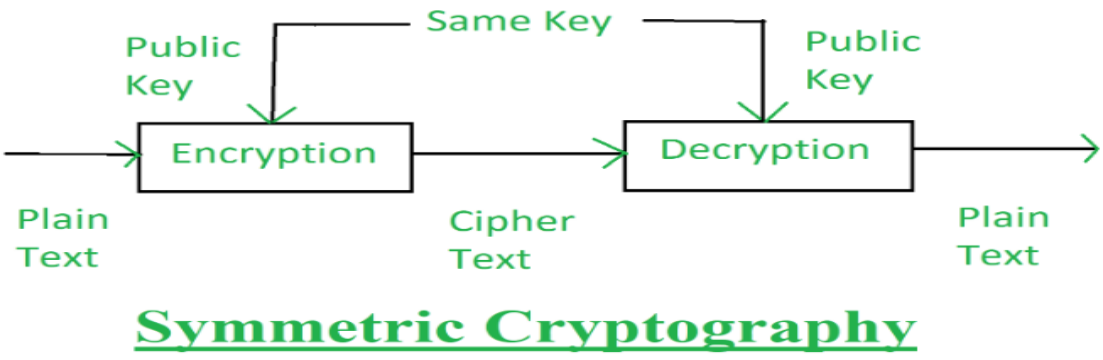
What is Classical Cryptography?

Classical cryptography is based on mathematics and it relies on the computational difficulty of factorizing large numbers. The security of classical cryptography is based on the high complexity of the mathematical problem for instance factorization of large numbers. In classical cryptography the original data i.e., the plain text is transformed into the encoded format i.e. cipher text so that we can transmit this data through insecure communication channels. A data string known as the key is used to control the transformation of the data from plain text to cipher text. This arrangement helps to keep data safe as it requires the key to extract the original information from the cipher text. Without the key, no one can read the data. In this technique, it is assumed that the only authorized receiver has the key.

Types of Classical Cryptography

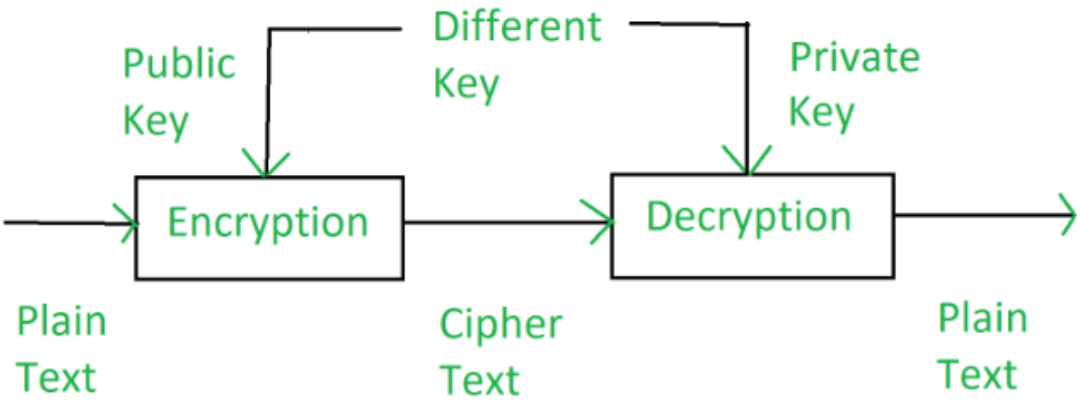
- **Symmetric Cryptography:** In symmetric cryptography, a single key is used to encrypt and decrypt data. This encryption key is the private key. This is the limitation of this encryption

technique that this private key must be distributed only among the authorized sender and receiver.



Symmetric Cryptography

- **Asymmetric Cryptography:** In **the** asymmetric cryptography a pair of key, i.e., public key and private key is used for encryption and decryption. A sender can use its public key to encrypt the data and on receiver end receiver can decrypt the data by using its private key. This technique overcomes the problem of key distribution.



Asymmetric Cryptography

Advantages of Classical Cryptography

- While employing the one-time pad, it is unbreakable.
- It is easy to do manually, no computer required.
- It protects the plain text from casual snooping.
- While employing the one-time pad, it is cumbersome and requires a personal meetup to exchange the pads.

If not employing the OTP, anyone who is even remotely interested in knowing what you wrote and knows about cryptography will be able to break the encryption.

Disadvantages of Classical Cryptography

- It has limited security, so it is vulnerable to frequency analysis and brute-force attacks which makes it inadequate for protecting against modern threats.
- Key management is challenging which requires secure distribution and management of keys, increasing the risk of interception and misuse in symmetric encryption systems.
- Scalability is also inefficient for large-scale use, as the number of unique keys needed grows exponentially with more users.
- Unsuitable for encrypting modern data formats and large datasets, which demand more advanced and versatile encryption algorithms.
- Does not provide built-in mechanisms for data integrity, authentication, or non-repudiation, essential for secure digital communications today.

What is Quantum Cryptography?

Quantum Cryptography is based on physics and it relies on the laws of quantum mechanics. It is arising technology which emphasizes the phenomena of quantum physics in which two parties can have secure communication based on the invariabilities of the laws of the quantum mechanics. Quantum mechanics is the mathematical framework or set of rules for the construction of physical theories.

There are 2 important elements of quantum mechanics on which quantum cryptography depends: **Heisenberg Uncertainty Principle** and **Photon Polarization Principle**.

- **Heisenberg Uncertainty Principle:** This principle says that if you measure one thing, you cannot measure another thing accurately. For example, if you apply this principle to human, you could measure a person's height, but you can't measure his weight. The only odd thing about this principle is that it becomes true only for the instant at which you try to measure something. This principle is applied to the photons. Photons have wave like structure and are polarized or tilted in certain direction. While measuring photon polarization, all subsequent measurements are get affected by the choice of measures that we made for polarization. This principle plays the vital role to prevent the efforts of attacker in quantum cryptography.
- **Photon Polarization Principle:** This principle refers that, an eavesdropper cannot copy the unique quantum bits, i.e., unknown quantum state, due to the no-cloning principle. If an attempt is made for measuring any properties, it will disturb the other information.

Advantages of Quantum Cryptography

- It establishes secure communication by providing security based on fundamental laws of physics instead of mathematical algorithms or computing technologies used today.
- It is virtually unhackable.
- It is simple to use.
- Less resources are needed in order to maintain it.
- It is used to detect eavesdropping in QKD (Quantum Key Distribution). This is due to the fact that it is not possible to copy the data encoded in quantum state.
- The performance of such cryptography systems is continuously improved.
- It offers perfect secrecy, meaning that the information cannot be intercepted or tampered with without detection.
- It can detect if any attempt has been made to intercept or eavesdrop on the communication, which can help prevent attacks before they occur.
- It has the potential to support large-scale, secure communication networks that are resistant to attacks by quantum computers, which could be used to break many current cryptographic systems.

Disadvantages of Quantum Cryptography

- The world wide implementation of this can take up lots of jobs and hence unemployment will increase.
- While traveling through the channel polarization of photons may change due to various causes.
- Quantum cryptography lacks many vital features such as digital signature, certified mail, etc.
- The largest distance supported by QKD is about 250 KM at a speed of 16 bps through the , guided medium.
- Quantum cryptography requires specialized equipment, including lasers and photon detectors, which can be expensive and difficult to maintain.
- It is sensitive to environmental factors, such as temperature and electromagnetic interference, which can affect the accuracy and reliability of the communication.
- It is currently limited by the distance over which secure communication can be established, which is typically less than a few hundred kilometers.

Difference between Private key and Public key cryptography

Cryptography as a field emphasizes the need to guarantee secure communication and data privacy. There are mainly two approaches available to perform this operation: – Private Key Cryptography (RIC or Symmetric Key Cryptography) and Public Key Cryptography (PKE or Asymmetric Key Cryptography). Although they are used to protect information, they work differently and have certain benefits and drawbacks. In this article, the key focus is on understanding the key aspects of a private and public key as well as the advantages and disadvantages of using them.

Cryptography is the science of secret writing to keep the data secret. Cryptography is classified into symmetric cryptography, asymmetric cryptography, and hashing.

What is a Private Key?

Private key Encryption, also termed as symmetric Key Encryption requires the key that is used to lock and the key used to unlock the message. This key must be kept concealed between the two communicating entities to have reasonable security.

Advantages of Private Key Encryption

- **Speed:** These algorithms are faster as compared to asymmetric encryption algorithms and hence used for encrypting large volumes of data.
- **Less Computational Power:** In another way, it is advantageous since it requires fewer calculations which makes it suitable for real-time use.

Limitations of Private Key Encryption

- **Key Distribution Problem:** The first and perhaps the major limitation is how to securely transfer the said key among the parties. The problem with this event is that the key is useless if it is intercepted, meaning that the security is lost.
- **Scalability Issues:** That is why as the number of the users raises key management becomes more complicated and thus it is not very scalable for large systems.

What is Public Key?

Public Key Encryption, or Asymmetric Encryption, involves a pair of keys: There is the public key that is relatively known and the private key which is kept secret. While the public key where everyone can get it from the internet is for encoding or encryption, the private key is employed for decoding, decryption.

Advantages of Public Key Encryption

- **Enhanced Security:** The application of two keys means that there is no problem of secure key distribution since with the public key anyone can encrypt the message while the private key can only be known by the recipient.
- **Digital Signatures:** The use of public key cryptography is employed to back up the concept of digital signatures hence ensuring true and complete message.

Disadvantages of Public Key Encryption

- **Slower Performance:** Asymmetric algorithms generally are slower and considerably more resource-hungry as compared to symmetric algorithms.
- **Complexity:** Another disadvantage that has been agreed upon is that the management and application of public key infrastructure can be complicated.

Which Encryption Key Type Is More Secure?

It should therefore be appreciated that there solved security of encryption methods is dependent on the application is use in. As mentioned earlier, public Key encryption is more appropriate for key distribution as well as authentications since it will be using two keys. However, the use of the private key for encryption of data proves to be secure due to the increased speed and efficiency.

Difference Between Private Key and Public Key

Private Key	Public Key
The private key is faster than the public key.	It is slower than a private key.
In this, the same key (secret key) and algorithm are used to encrypt and decrypt the message.	In public-key cryptography, two keys are used, one key is used for encryption, and the other is used for decryption.
In private key cryptography, the key is kept a secret.	In public-key cryptography, one of the two keys is kept a secret.
The private key is **Symmetrical** because there is only one key that is called a secret key.	The public key is **Asymmetrical** because there are two types of keys: private and public keys.
In this cryptography, the sender and receiver need to share the same key.	In this cryptography, the sender and receiver do not need to share the same key.
In this cryptography, the key is private.	In this cryptography, the public key can be public and a private key is private.
It is an efficient technology.	It is an inefficient technology.
It is used for large amounts of text.	It is used for only short messages.
There is the possibility of losing the key that renders the systems void.	There is less possibility of key loss, as the key is held publicly.
The private key is to be shared between two parties.	The public key can be used by anyone.
The Performance testing checks the reliability, scalability, and speed of the system.	The Load testing checks the sustainability of the system.
The private key is used in algorithms such as AES 128, AES 192 and AES 256.	The public key is used in algorithms such as RSA, DSA, etc.
The private key is kept secret.	The public key is widely distributed.
It is used to protect disk drives and other data storage devices.	It is used to secure web sessions and emails.
The recipient's private key decrypts the message.	The recipient's public key encrypts the message.

If the private key is the locking key, then the system can be used to verify documents sent by the holder of the private key.	If the public key is the locking key, then it can be used to send private communication.