**AIM: Introduction to Information Security and Cryptography.**

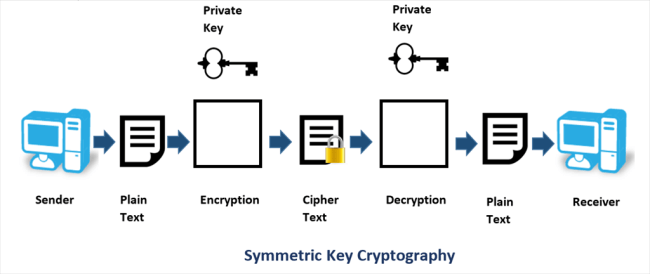
1. **What is Cryptography?**

**Ans:**

* Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.
* Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. Cryptography also aids in nonrepudiation. This means that the sender and the delivery of a message can be verified.
* Cryptography is also known as cryptology.
* Cryptography also allows senders and receivers to authenticate each other through the use of key pairs.
* Earlier cryptography was effectively synonymous with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice.
* **Modern cryptography concerns with:**

1. **Confidentiality** - Information cannot be understood by anyone
2. **Integrity** - Information cannot be altered.
3. **Non-repudiation** - Sender cannot deny his/her intentions in the transmission of the information at a later stage
4. **Authentication** - Sender and receiver can confirm each  
   Cryptography is used in many applications like banking transactions cards, computer passwords, and e- commerce transactions.

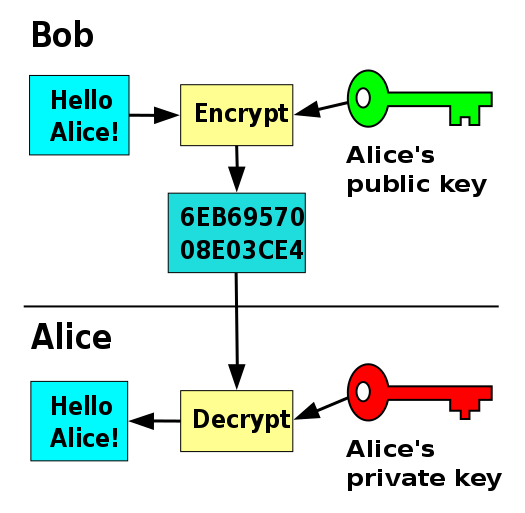
* Three types of cryptographic techniques used in general.  
    
  1. Symmetric-key cryptography  
  2. Hash functions.  
  3. Public-key cryptography



1. **What is Public Key Cryptography?**

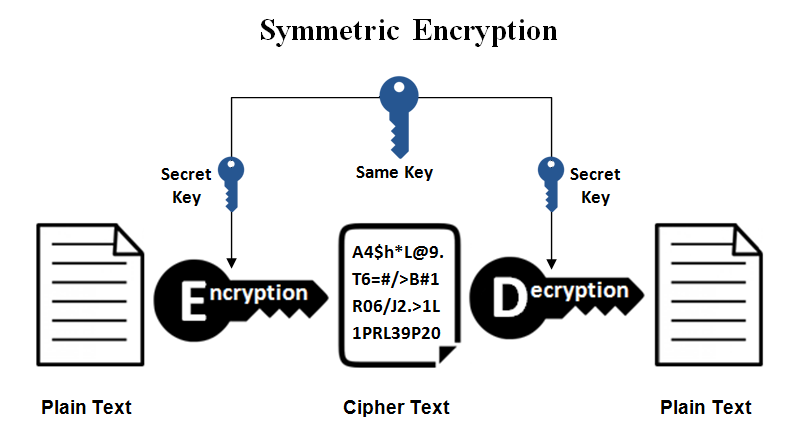
**Ans:**

* Public key cryptography (PKC) is an encryption technique that uses a paired public and private key (or asymmetric key) algorithm for secure data communication. A message sender uses a recipient's public key to encrypt a message. To decrypt the sender's message, only the recipient's private key may be used.
* PKC is also known as public key encryption, asymmetric encryption, asymmetric cryptography, asymmetric cipher, asymmetric key encryption and Diffie-Hellman encryption.
* PKC is a cryptographic algorithm and cryptosystem component implemented by a variety of internet standards, including Transport Layer Security (TLS), Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), Secure Socket Layer (SSL) and Hypertext Transfer Protocol (HTTP) websites.
* PKC facilitates secure communication through an insecure channel, which allows a message to be read by the intended recipient only. For example, A uses B's public key to encrypt a message to B, which can be decrypted using B's unique private key.
* PKC is slower than secret key cryptography (or symmetric cryptography) methods, due to high computational requirements. Unlike symmetric cryptography, PKC uses a fixed buffer size, depending on particular and small data amounts, which may only be encrypted and not chained in streams. Because a broad range of possible encryption keys are used, PKC is more robust and less susceptible to third-party security breach attempts.



1. **What is Private Key Cryptography (PKC)?**

**Ans:**

* A private key is a tiny bit of code that is paired with a public key to set off algorithms for text encryption and decryption. It is created as part of public key cryptography during asymmetric-key encryption and used to decrypt and transform a message to a readable format. Public and private keys are paired for secure communication, such as email.
* A private key is also known as a secret key.
* sending encrypted messages requires that the sender use the recipient's public key and its own private key for encryption of the digital certificate. Thus, the recipient uses its own private key for message decryption, whereas the sender's public key is used for digital certificate decryption.