Hello everyone! In this video, you will understand various types of cryptography techniques.

Cryptography can be broadly divided into two categories: symmetric key cryptography and asymmetric key cryptography based on the keys being used for encryption and decryption.

Let's understand the symmetric key and asymmetric key algorithms of cryptography.
In symmetric key cryptography, the sender and the receiver share the same key. The shared key is kept secret between the sender and the receiver only. Encryption and decryption operations are performed using the shared key. Few of the cryptographic algorithms using this technique are Data Encryption Standards (DES), Advanced Encryption Standards (AES) etc.
In asymmetric or public key cryptography, two types of keys are involved: a public key and a private key. While more than one party such as a sender and a receiver involve in data transmission securely and separately, they both announce their public keys to all and keep their private keys secret to themselves. The sender encrypts the message using the public key of the receiver and the receiver decrypts the cipher message using his/her private key.

Examples of the algorithms using this approach are Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC) etc.

Here is an example of using Symmetric Key Cryptography.
Alice wants to send message secretly to Bob through unsecure channel using symmetric key cryptography algorithm.
So, she sends encrypted message(C) of the Plain Text(P) using Encryption(E) algorithm, which is a symmetric key cryptography algorithm. Bob uses decryption algorithm(D) to get the original plaintext P.
It can easily be observed here that same key K is being used for encryption and decryption.
This approach provides authentication as the Secret Key (K) is known to only Alice and Bob, if Bob is able to decrypt successfully then Bob believes that message sent by Alice
Similarly this approach ensures confidentiality Since the Secret Key (K) is known to only Alice and Bob, nobody in between can decrypt it

Here is an example of using an Asymmetric key cryptography algorithm.
Alice wants to send a message secretly to Bob through insecure channel

So, she sends an encrypted message© of the Plain Text(P) using the Encryption algorithm E, which is an asymmetric key algorithm.
Where each user is having two keys. Private Key of Alice (PR_A), Public Key of Alice (PU_A), Private Key of Bob(PR_B), Public Key of Bob(PU_B). The public keys of both users are known to each other as they are distributed using public channels such as digital certificates. Alice uses Bob's public key to encrypt the message and Bob uses its private key to decrypt the message.
Asymmetric key cryptography does not ensure authentication, as anyone, with the public key of the receiver, can send the data to him.

You can get more about types of cryptography from the given links.

Thank you…