Hello everyone! In this video, you will learn about two asymmetric key algorithms RSA and Elliptic curve cryptography and the difference between symmetric and asymmetric key cryptography.

RSA was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adelman at MIT
It is a public key cryptographic algorithm. The strength of RSA lies the in-integer factorization problem i.e., if we are given n, which is the product of two large primes, it is very difficult to factorize n into $p \times q$.
A pair of keys comprising of public key and the private key is used by the RSA algorithm. Public key is available to all, while private key is kept secretly by the receiver.
Suppose a sender wants to send some message M, M<n, secretly to the receiver using RSA cryptosystem. Sender computes $C=M\text{^}e \ mod \ n$ and sends C to the receiver, where e is the public key of the receiver.
On receiving C from the sender, the receiver decrypts C to M using his/her private key d. using formula M= $C\text{^}d \ mod \ n$.
the key generation process is also straight forward, as shown here.

The Elliptic Curve Cryptography (ECC) is modern family of public-key cryptosystems, which is based on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP).

ECC implements all major capabilities of the asymmetric cryptosystems: encryption, signatures and key exchange.
It's simply stronger than RSA for key sizes in use today. The typical ECC key size of 256 bits is equivalent to a 3072-bit RSA key and 10,000 times stronger than a 2048-bit RSA key.

The elliptic curve equation is given by Ep. In order to perform mathematical operation in ECC, three types of operations, point addition, point doubling and point subtraction needs to be known. Given the points P(x1, y1) and Q(x2, y2) in an elliptic curve, how to find point R(x3, y3) during point addition or point subtraction is given.

Point subtraction of P(x1, y1) and Q(x2, y2) is performed using the rule of point addition after the y2 coordinate is negated.

Here are some differences between symmetric key cryptography and asymmetric key cryptography
Symmetric-key cryptography is based on sharing secrecy while Asymmetric-key cryptography is based on personal secrecy.
In symmetric-key cryptography, symbols are permuted or substituted; in Asymmetric-key cryptography, numbers are manipulated.

Asymmetric-key and Symmetric-key ciphers will exist in parallel and continue to serve the community. They are complements of each other; the advantages of one can compensate for the disadvantages of the other.

For other details of Asymmetric key cryptography, read the books mentioned in the references.

Thank You…