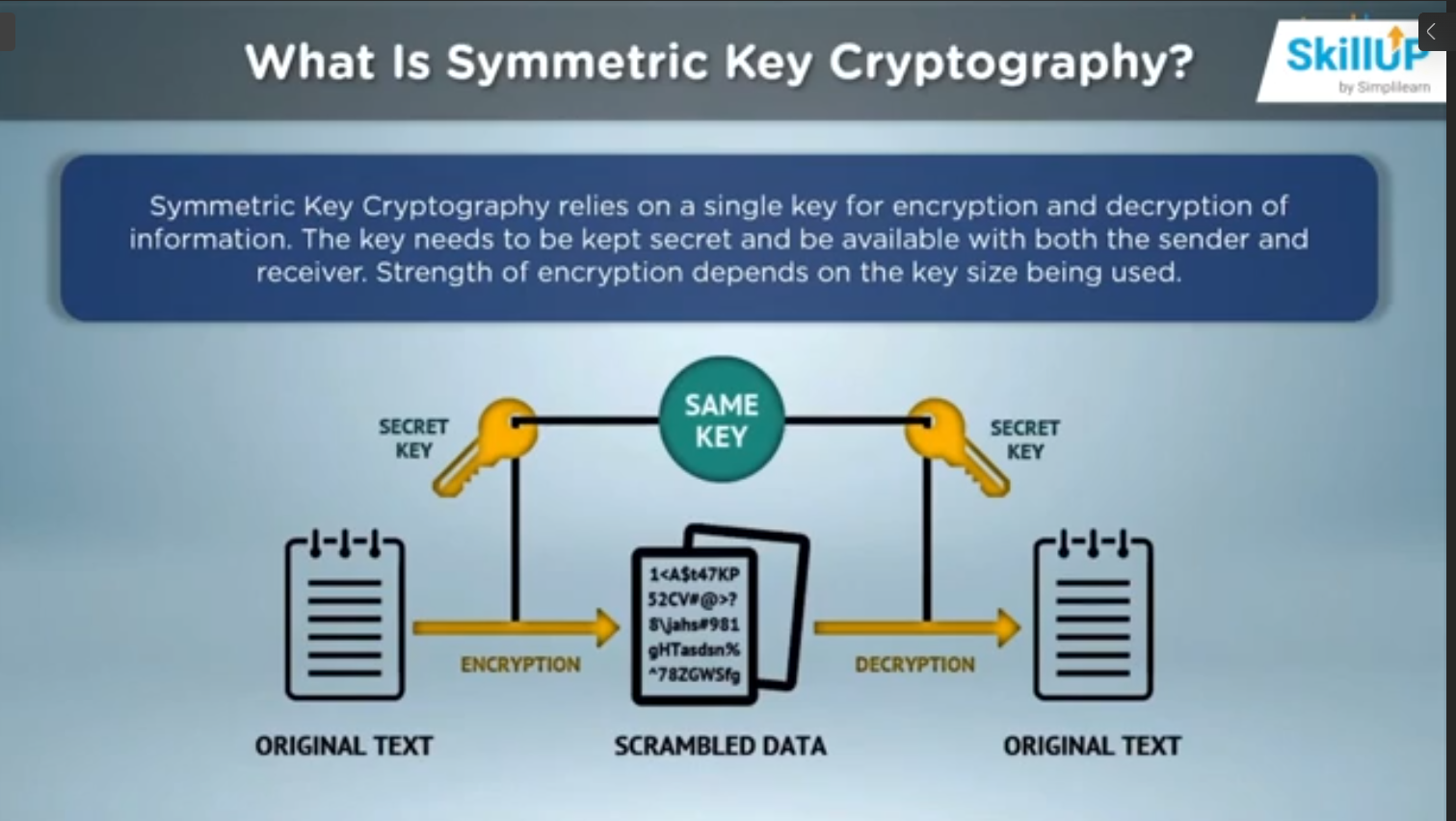
**CRYPTOGRAPHY**

* Cryptography is the science of encrypting and decrypting information to prevent unauthorized access.

Types of Cryptography

* **Symmetric Key Cryptography:**



* Same key for encryption and decryption means a single point of failure
* Key needs to be always keep secret.
* Receiver/Third party can also generate messages with the same key, so authentication issue will arise should the secret key is leaked.

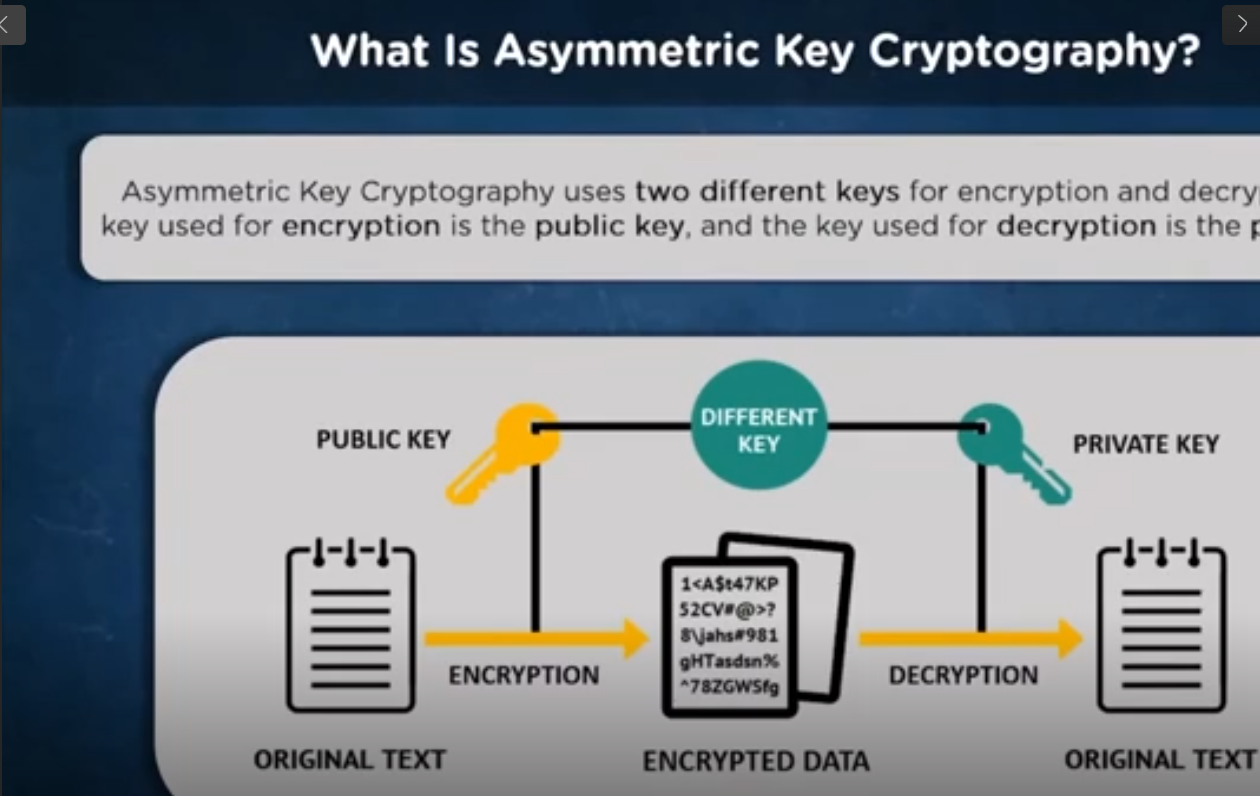
Types of Encryption:

1. Stream Ciphers:

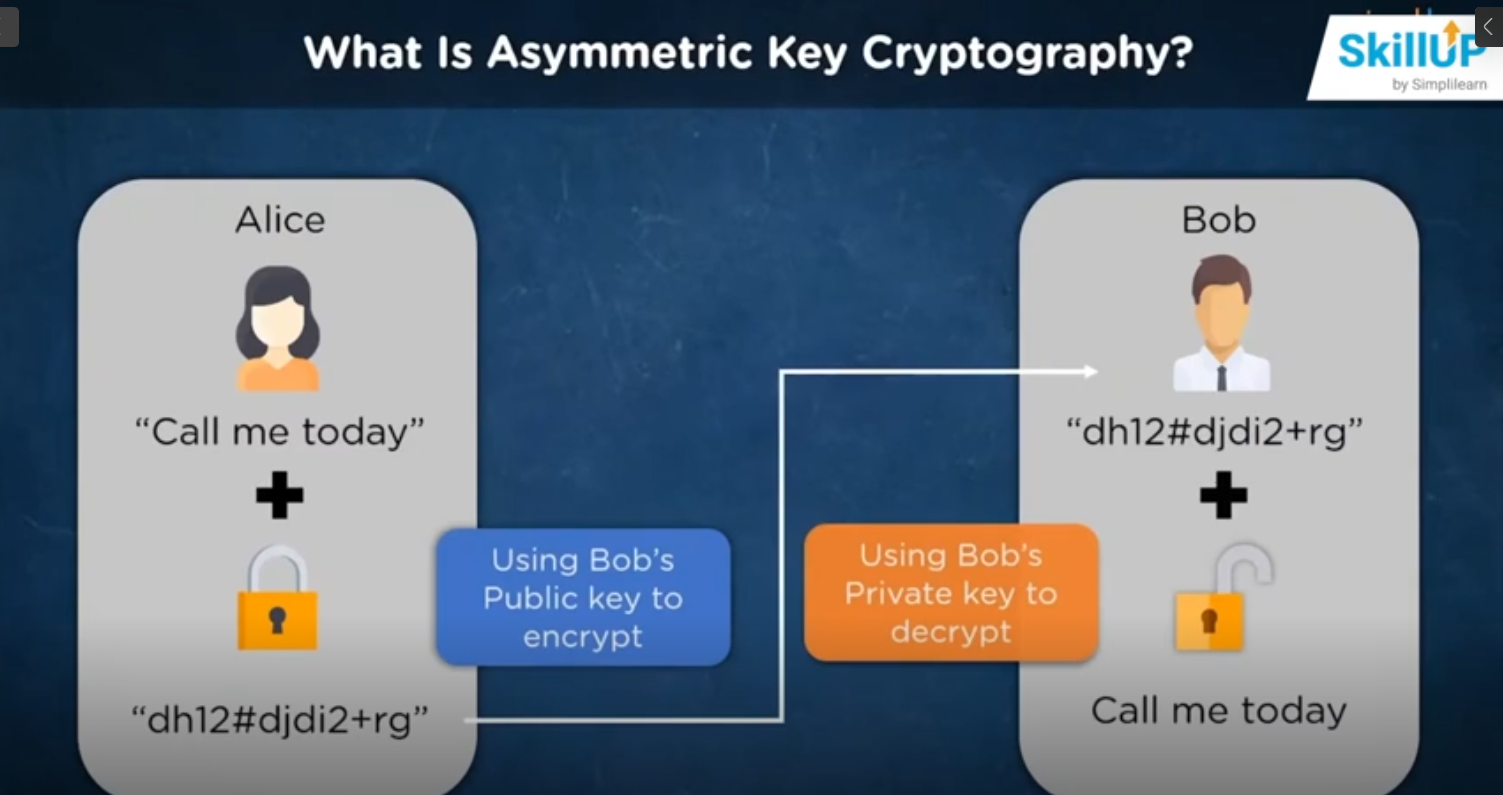
* Encrypt information one bit/byte at time.
* Quicker format of encryption.
* Data is converted to binary digits and encrypted sequentially.
* Popular algorithms – RC4, Salsa20

1. Block Ciphers

* Information broken down to chunks/books of fixed size.
* Size of block depends on key size.
* The chunks are encrypted and later chained together.
* Popular algorithms – AES, DES, 3DES
* **Assymetric Key Cryptography**



Example



**Hashing**

Hashing is the process of scrambling a piece of information or data beyond recognition. They are designed to be irreversible. We pass input through a hash function to calculate the Hash Value or Digest.

Hash Function is to store the password in the server. This hashed password is checked while login.

Hash Algorithm Digest size

MD5 ------------------------------------------------------ 128 bits

SHA-256 ------------------------------------------------------ 256 bits