CloudFolks HUB

Amazon S3
Simple Storage Service

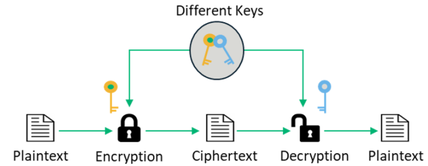
# Symmetric V/S Asymmetric Encryption

1


Symmetric Encryption

1. There's a single shared key that's used for encryption and decryption.
2. Generally faster and more efficient for encrypting large amounts of data (like S3 objects)
3. Requires a secure way to share the key with anyone who needs to decrypt the data
4. Symmetric Encryption Examples
   1. AES (Advanced Encryption Standard)
      1. AES-128
      2. AES-192
      3. AES-256
         1. AES-256 is generally considered the most secure
         2. It is the default encryption standard used by AWS S3
   2. DES (Data Encryption Standard
   3. 3DES (Triple DES)

2




Asymmetric Encryption

1. It involves the use of two mathematically related keys.
   1. The public key (the one that's known to everybody)
   2. private key (which is only known by you) are required for encrypting and decrypting the message.
2. Offers stronger security due to the separation of keys. Even if someone intercepts the encrypted data and the public key, they cannot decrypt it without the private key.
3. Slower than symmetric encryption, especially for large amounts of data
4. Asymmetric Encryption Examples
   1. RSA (Rivest-Shamir-Adleman)
   2. ECC (Elliptic Curve Cryptography)
   3. Diffie-Hellman key exchange