

## 1. List all symmetric key Algorithms

There are two types of symmetric key algorithms:

1. Block algorithm

Set lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks.

2. Stream algorithms

\* AES (Advanced Encryption Standard)

\* DES (Data Encryption Standard)

\* IDEA (International Data Encryption Algorithm)

\* Blowfish (Drop-in replacement for DES or IDEA)

\* RC4 (Rivest Cipher 4)

\* RC5 (Rivest cipher 5)

\* RC6 (Rivest cipher 6)

## List all asymmetric key algorithms

Asymmetric cryptography is a branch of cryptography where a secret key can be divided into two parts, a public key and a private key.

\* Ed25519 signing

\* X25519 key exchange

\* Ed448 signing

\* X448 key exchange.

\* Elliptic curve cryptography

\* RSA

\* Diffie-Hellman key exchange

\* DSA

\* key serialization

\* Asymmetric Utilities



3 List the algorithms for message digest

→ The MD5 Message-digest algorithm is a widely used hash function producing a 128-bit hash value.

→ Although MD5 was initially designed to be used as a cryptographic hash function

### List of Message Digest Algorithm

\* MD2 ÷ The MD2 message digest Algorithm as define in RFC 1319.

\* MD5 ÷ The MD5 Message digest Algorithm as define in RFC 1321

\* SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256

\* SHA3-224, SHA3-256, SHA3-284, SHA3-512