ciphers

By

Hafez Barghouthi

Two flavors

- Symmetric algorithms: the same key is used for encryption and decryption .
- Asymmetric algorithms: different keys are used for encryption and decryption.

Symmetric cipher

- Key has to be kept secret.
- All parties sharing the same key can read data encrypted under the key.
- Setting a private channel need a maintaining a large number of keys.
- Key Managment is a very important task.
- Example DES.(Data Encryption Standard)

Asymmetric cipher

- Also called public key algorithm.
- Public key to encrypt and private key to decrypt.
- Obviously, the two keys are algorithmically related but it should not be feasible to derive one from another.
- Example RSA (Rivest,Shamir and Adleman)

Another two

- Block cipher.
- Stream cipher.
- A **stream cipher is one that encrypts a digital data stream one bit or one byte at a** time.
- A **block cipher is one in which a block of plaintext is treated as a whole and** used to produce a cipher text block of equal length.

Block cipher

- In this course we will concern on this kind of cipher.
- So let talk a look on DES.