InfoSec Exam Prep Cheat Sheet

by Bayan (Bayan.A) via cheatography.com/122738/cs/31493/

Block Ciphers

Encrypt plaintext of given size & key

Encryption algorithm for a block

Recover plaintext from encrypted word

Knowing if given encryption allows recovery of plaintext

SP-Boxes

Substitution-Permutation Box

Encrypt single block from final permutation

Elementary calculation related to block ciphers

Assessing required resources for encryption method based on block ciphers

Calculate required size of lookup tables

Number of binary words of length n is 2n

Fiestel Encryption

What it is

How to

By **Bayan** (Bayan.A)
cheatography.com/bayan-a/

Not published yet.
Last updated 10th September, 2022.