Block Ciphers + DES

**Phân biệt Block cipher và Stream cipher:**

1 block cipher là 1 khối plaintext được mã hóa tạo ra ciphertext có độ dài bằng nhau. 1block thường 64 hoặc 128 bits.

1 stream cipher là mã hóa dữ liệu số dòng 1bit hoặc 1byte tại 1 thời điểm.

**Nguyên lý Block Cipher:**

Dựa vào a Feistel Cipher Structure.

Cần thiết vì phải giải mã ciphertext để khôi phục tin nhắn hiệu quả.

Giống như thay thế trên vùng rộng lớn.

Cần 264 entries cho 64-bit block.

DES sinh ra từ năm 1977.

DES sử dụng 64bits-block nhưng khóa 56bits-key + 8 bit khác có thể được sử dụng như là các bit chẵn lẻ hoặc chỉ đơn giản là thiết lập tùy tiện.

Sử dụng 16 Round cho mã hóa.

Ngày nay, thì AES thay thế cho DES.