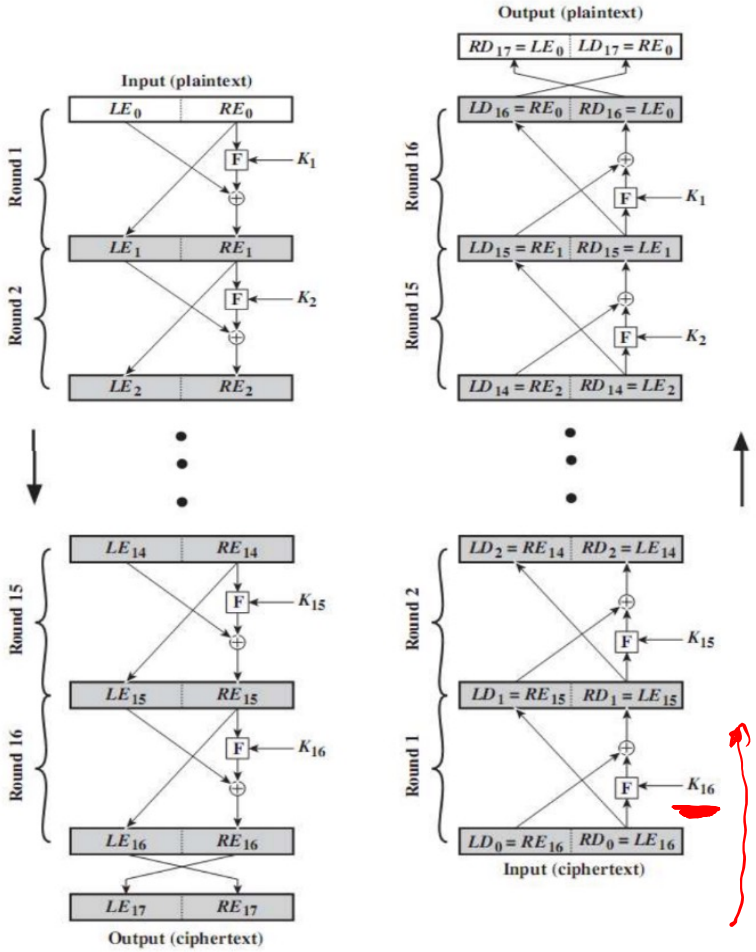
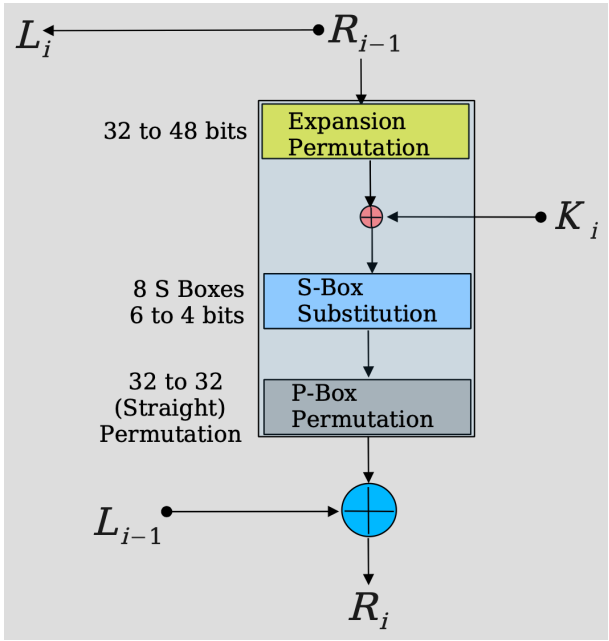
Feistel Encryption and Decryption



Encryption

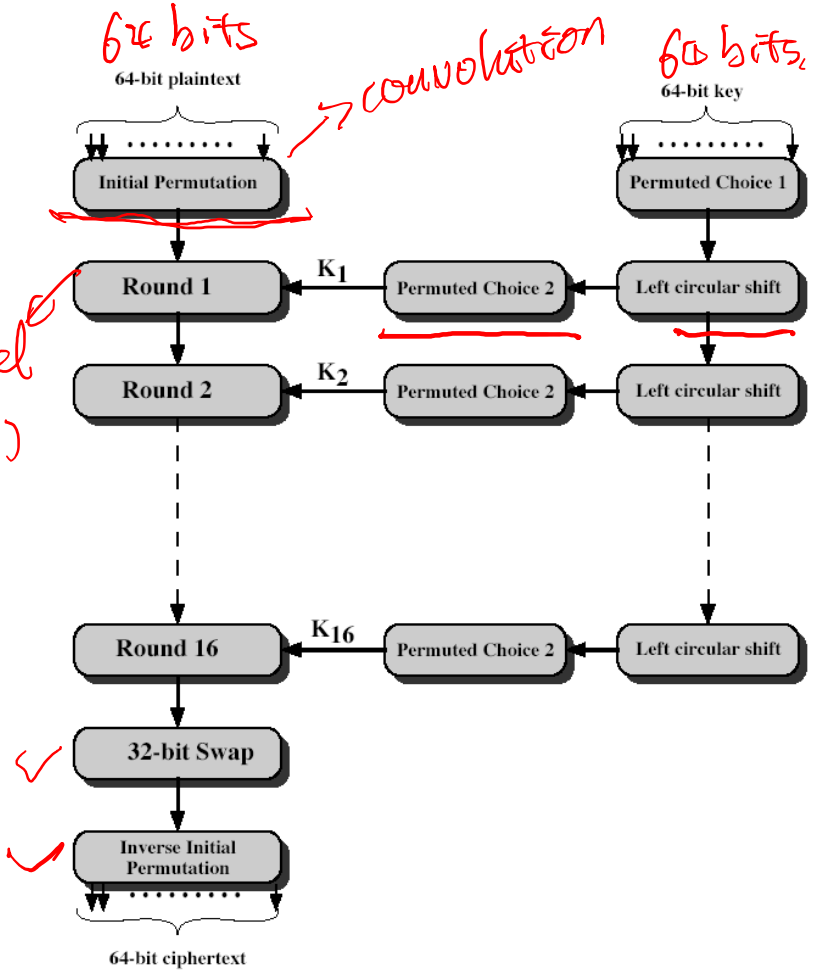
$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$



DES encryption

- 64 bits plaintext
- 56 bits effective key length

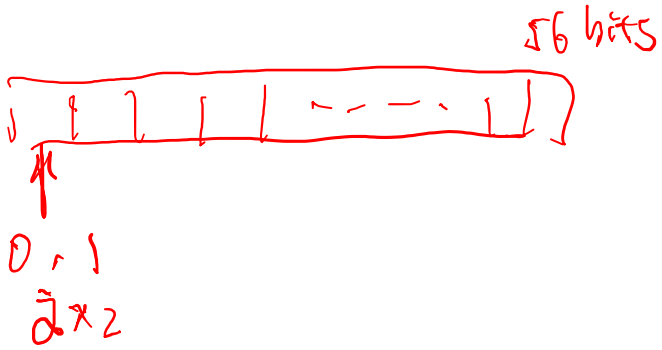


DES Weakness

try every possibity of keys

- short length key (56 bits) is not secure enough. Brutal force search takes short time.

2^{56}

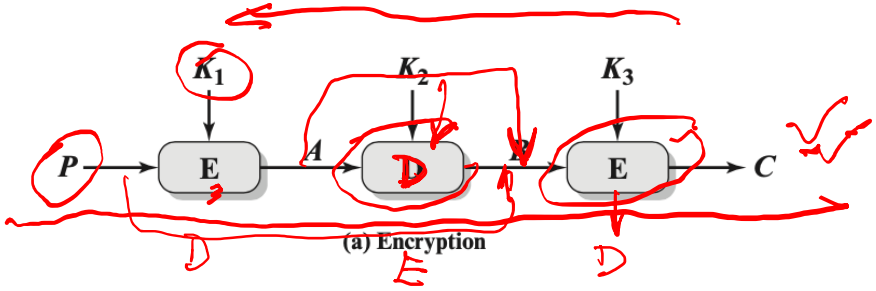


Triple DES (3DES)

$$C = E(K_3, D(K_2, E(K_1, P)))$$

where

C = ciphertext
P = plaintext
$E[K, X]$ = encryption of X using key K
$D[K, Y]$ = decryption of Y using key K



(b) Decryption

Decrypting with the wrong key will further convolute the output

3DES

- Triple DES with three different keys – brute-force complexity 2^{168}
- 3DES is the FIPS-approved symmetric encryption algorithm
- Weakness: slow speed for encryption

FIPS – Federal Information Processing Standards. The United States' Federal Information Processing Standards are publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors

AES

- clearly a replacement for DES was needed
  - have theoretical attacks that can break it
  - have demonstrated exhaustive key search attacks
- can use Triple-DES – but slow with small blocks
- US NIST issued call for ciphers in 1997
- 15 candidates accepted in Jun 98
- 5 were short-listed in Aug-99
- Rijndael was selected as the AES in Oct-2000
- issued as FIPS PUB 197 standard in Nov-2001

NIST issued calls for post quantum

review AES

key L

PKI: unsafe

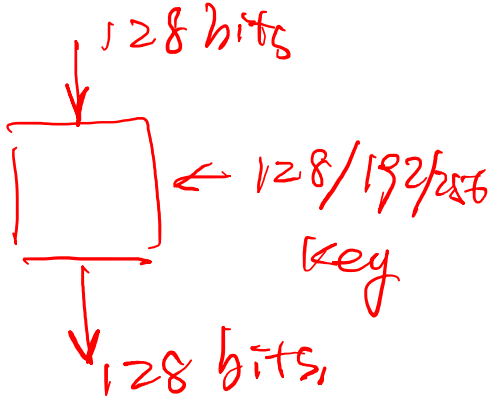
RSA & Shor

Criteria to evaluate AES

- General security
- Software implementations
- Restricted-space environments
- Hardware implementations
- Attacks on implementations
- Encryption versus decryption
- Key agility
- Other versatility and flexibility
- Potential for instruction-level parallelism

Cryptographic Standards and Guidelines | CSRC (nist.gov)

AES Specification



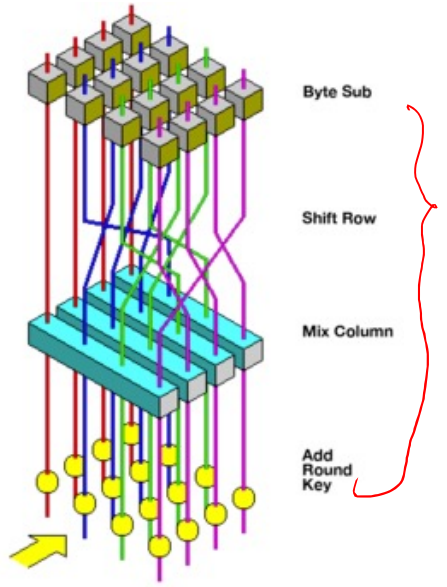
- symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- stronger & faster than Triple-DES
- provide full specification & design details
- both C & Java implementations
- NIST have released all submissions & unclassified analyses

https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/aes-development/Rijndael-ammended.pdf

The AES Cipher - Rijndael

- an **iterative** rather than **feistel** cipher
  - treats data in 4 groups of 4 bytes
  - operates an entire block in every round
- designed to be:
  - resistant against known-plaintext attacks
  - speed and code compactness on many CPUs
  - design simplicity

Rijndael



- processes data as 4 groups of 4 bytes (state) = 128 bits
- has 10/12/14 rounds in which state undergoes:
  - byte substitution (1 S-box used on every byte)
  - shift rows (permute bytes row by row)
  - mix columns (alter each byte in a column as a function of all of the bytes in the column)
  - add round key (XOR state with key material)
- 128-bit keys – 10 rounds, 192-bit keys – 12 rounds, 256-bit keys – 14 rounds