Feistel Ciphers

Michelle Lu & Katherine Hlaing

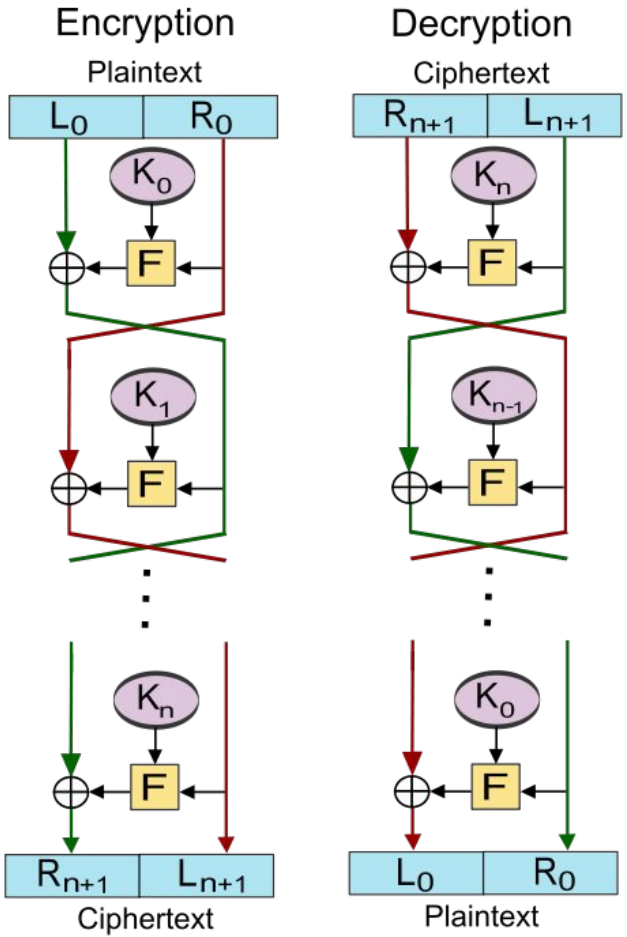
Explanation

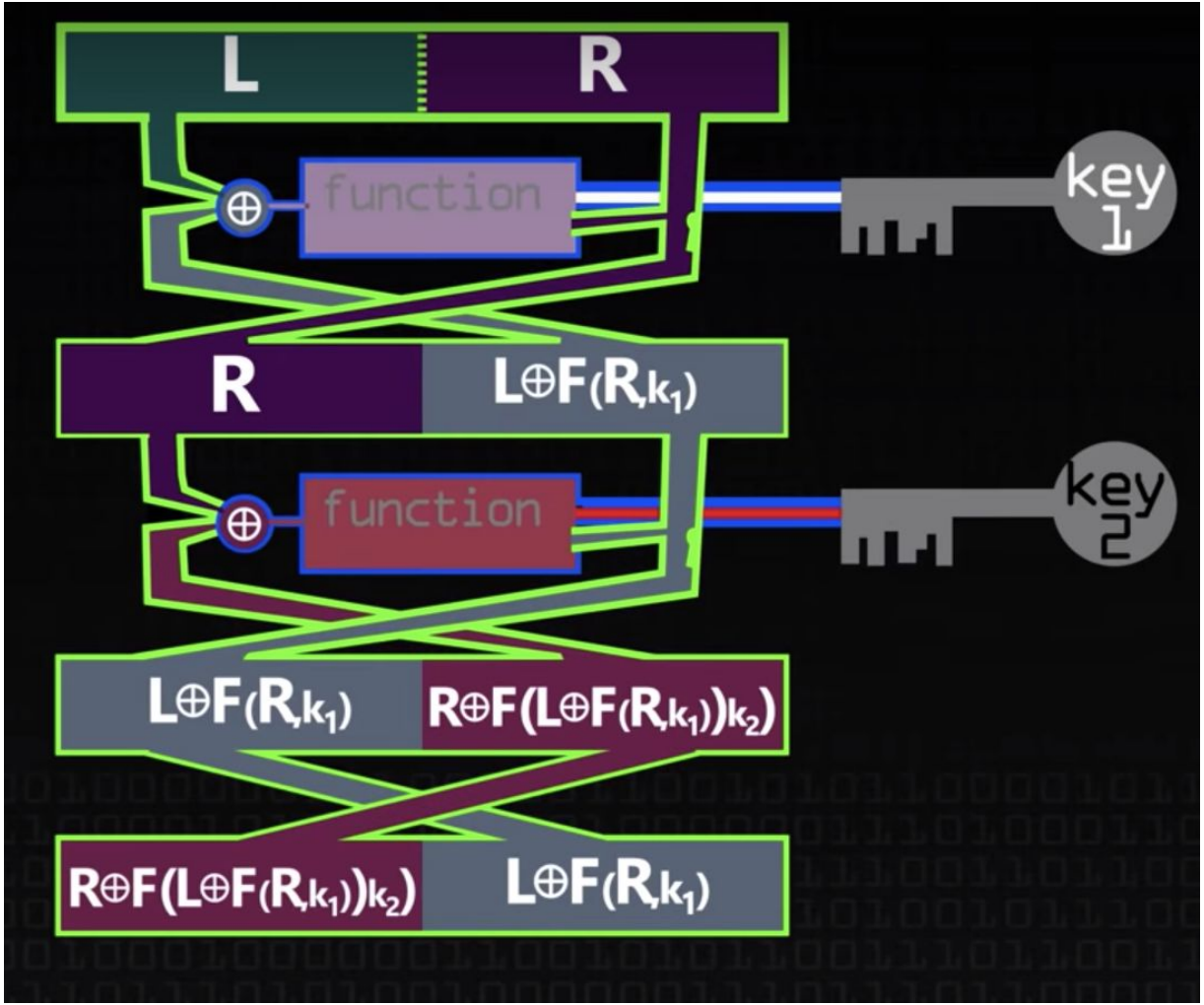
History:

- Named after the German-born physicist and cryptographer Horst Feistel
- Many modern symmetric block ciphers are based on Feistel networks
- Feistel networks were first seen commercially in IBM's Lucifer cipher in 1973.
- They gained respectability when the U.S. Federal Government adopted the DES (a cipher based on Lucifer, with changes made by the NSA) in 1976. The iterative nature of the Feistel construction makes implementing the cryptosystem in hardware easier.

What is a Feistel Cipher?

- AKA the Luby-Rackoff Block Cipher
- A design model or structure (not an actual block cipher)
- Made up of:
  - A round function (takes two inputs)
  - A data block
  - A subkey
- Returns one output the same size of the data block
- Requires multiple rounds of encryption
- Feistel ciphers can always be decrypted regardless of if the round function is invertible


Encryption
Plaintext
L0
R0
K0
F
K1
F
Kn
F
Rn+1
Ln+1
Ciphertext
Decryption
Ciphertext
Rn+1
Ln+1
Kn
F
Kn-1
F
K0
F
L0
R0
Plaintext


L
R
function
key 1
R
L⊕F(R,k1)
function
key 2
L⊕F(R,k1)
R⊕F(L⊕F(R,k1))k2
R⊕F(L⊕F(R,k1))k2
L⊕F(R,k1)

Computerphile Explanation

Examples/Uses in Cybersecurity

DES - Data Encryption Standard

- Used by the US government to encrypt information
- Requires the sender and receiver to have the correct private keys to encrypt and decrypt data
- Feistel F function is not invertible (but it's okay! The Feistel cipher can decrypt using invertible functions)
    - Biham and Shamir's cryptanalysis attack on DES took advantage that a pair of 32-bit inputs will often result in the same output using the DES Feistel F function
- 64-bit encryption algorithm made up of 64-bit key (8-bit used to determine parity)
    - Parity confirms accurate data transmission
- DES encrypts 64-bits at a time (this is the block size)
- 16 rounds
- Replaced by AES
    - 3 different key lengths: 128, 192, 256
    - Block size = 128-bits
    - Based off the Rijndael algorithm
    - More secure than DES (which took 84 days to break using brute force in the DES I Contest (1997))
    - AES is faster, more secure, and capable of encrypting larger files in shorter times than DES

Blowfish

- Designed by Bruce Scheire in 1993
- The encryption rate on a 32-bit microprocessor is 26 clock cycles per bytes
  - One clock cycle is the electric pulse for a CPU
- Uses less than 5KB of memory
- Uses primitive operations: XOR, addition -> simple
- Key length has a maximum of 448-bit and minimum of 32-bit
  - Flexible, secure, variety
- Encrypts 64-bit blocks
- 16 rounds
- Encryption & Key Schedule (it takes a secret key and uses an algorithm to generate 18 sub-keys and 4 S-boxes)
- Public domain (free to use)
- Relatively fast block cipher (simple round function; small number of rounds)
- Time consuming key schedule is protection against brute-force attacks
- Small block size vulnerable to birthday attacks (compared to 128 bits by AES)
  - Birthday attack: cryptographic attack which takes advantage of the math behind the birthday probability theory
  - The probability that paired people in a set of n (randomly chosen) will have the same birthday

Twofish

- Designed by Bruce Schneier, John Kelsey, Chris Hall, Niels Ferguson, David Wagner, Doug Whiting
- Based off Blowfish (improved version)
- Block size of 128 bits; key size up to 256 bits
- Half of the key is used as the encryption key and the other half is used to modify the encryption algorithm
- One of the finalists against AES (for standard); bit slower than AES
- 16 rounds
- Encryption runs faster than Blowfish (more variety in key -> no weak keys)
- Faster in key setup
- USES: Password management (Password Safe, KeePass), email encryption (PGP: Pretty Good Privacy), file encryption (TrueCrypt)