

# Practical Cryptography

# Weakest Link

A Security system is  
only as strong as its  
weakest link.

# Kerckhoff's Principle

The security of the encryption scheme must depend only on the secrecy of the key  $K_e$ , and not on the secrecy of the algorithm.

# Design Rule #1

Complexity is the worst  
enemy of security.

# Block Ciphers

An encryption function for  
fix-sized blocks.

Usually

128 bits (16 Bytes)

or 256 bits (32 bytes)

# Block Ciphers

In an “ideal” block cipher, 1000 groups of text after being encrypted, would show no statistical variations in their cipher text.

# Block Ciphers

An ideal block cipher implements an independently chosen random even permutation for each of the key values.

# DES

DES starts with 64 bits of  
plaintext

32-bits are called L

32-bits are called R

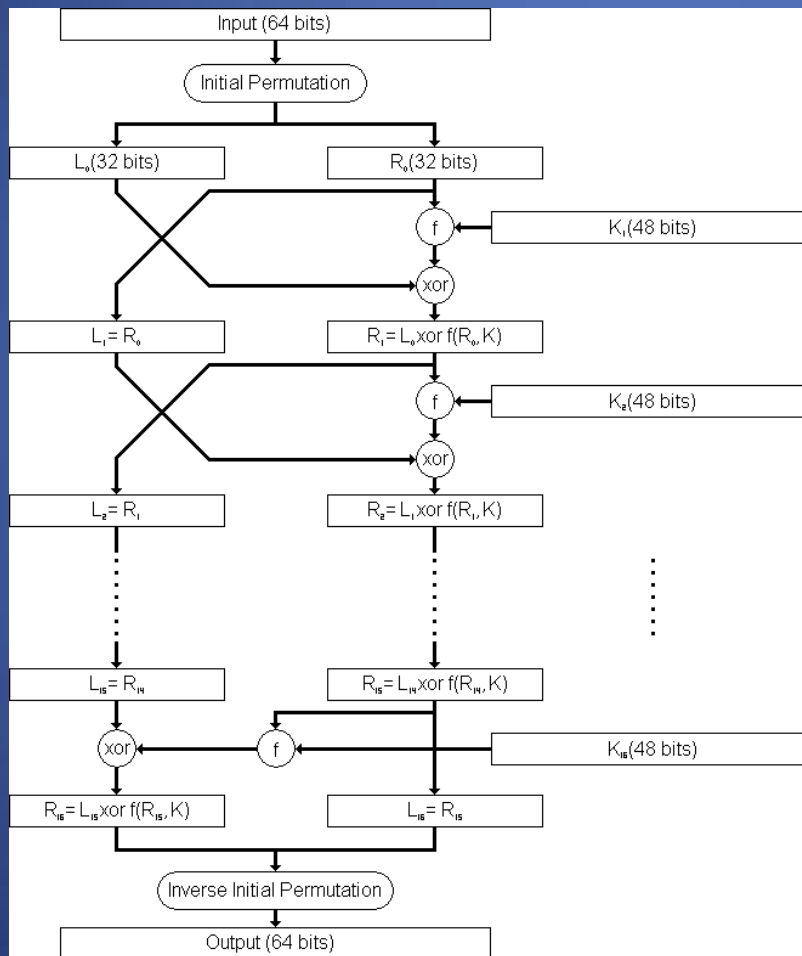
Step 1.

# DES

DES works in 16 rounds:

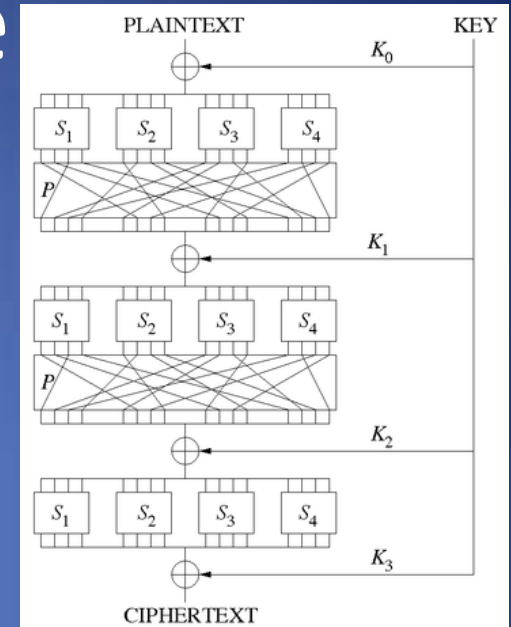
1. Create 16 “subkeys” from the 56-bit key,  $K_1 - K_{16}$
2. For each round  $i = 1-16$  do:
  - a. Take 64 bits of data, and split them into  $L_i$  and  $R_i$ .
  - b. Start with  $R_i$ , and expand by duplicating bits to a 48 bit length string.
  - c. XOR this string with the key for this round,  $K_i$
  - d. Take the resulting 48 bit string, and use a Substitution Block, replacing each 6 bits with a 4 bit string, to transform the 48 bit string into a 32 bit string
  - e. Run a “Bit shuffle” function on this 32 bit string.
  - f. Take the resulting string, and XOR with  $L_i$
  - g. The result is now  $R_{i+1}$ . The original  $R_i$  become  $L_{i+1}$
3. At the end, join the two halves,  $L_{16}$  and  $R_{16}$  together, select the next 64 bits of data, and repeat until out of data.

# DES – the Feistel Construction



# DES Family Tree

Lucifer – “substitution permutation network encryption” – 16 bit block Cipher, with 4 permutations of Substitution in 4 bit S-blocks.



DES – 64-bit block cipher. Its “substitution permutation network” is called “Feistel” and became the basis of several additional encryption algorithms.

(TripleDES, GDES, DES-X, LOKI89, ICE)

# AES

AES was the result of a  
NIST encryption  
competition.

15 proposals were  
submitted.

Five finalists were chosen  
for exhaustive testing

# AES

## Rijndael was the winner.

How do you pronounce Rijndael ? Unless you are Dutch you will say it wrong, so relax and pronounce it any way you like. – Schneier

Other finalists were Serpent, Twofish, RC6, and MARS. Serpent is very strong, but very complex to implement and slow to use. Twofish is widely used still today. It was authored by Bruce Schneier, and is Free.

# AES

AES starts with 128 bits of  
plaintext (16 bytes)

It can also use  
192, or 256 bit keys (with  
corresponding block sizes)

# AES Steps

1. XOR the 128 bits with 128 bit key.
2. For each of 10 to 14 rounds:
  - a. SubBytes - Bytes are reordered and four bytes are placed into each of four identical substitution boxes. The results are in a 2-d matrix 4x4
  - b. ShiftRows – items from each row are shifted by 0-3 positions
  - c. MixColumns - items from each column are multiplied with a fixed polynomial  $c(x)$
  - d. The resulting 128 bits are re-XORed with the key
3. In the final round, MixColumns is omitted.

# AES Diagram

