DES 9/24/25

Early 1970s

Competition to find a Standard for Symmetric key encryption.

↳ 2 people communicating share a private key.

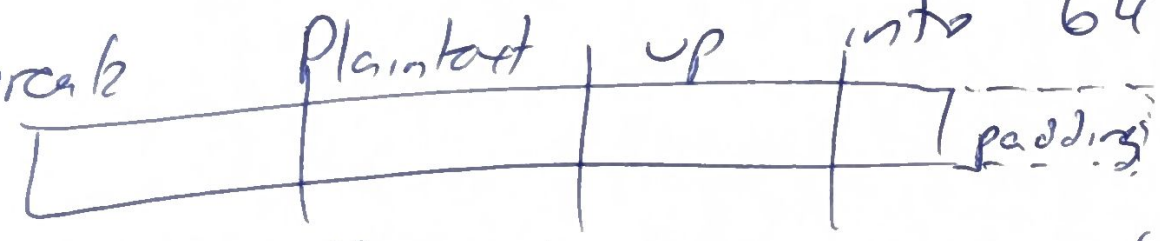
Winning System: Lucifer used internally @ IBM
Horst Feistel

↳ NSA took the original algorithm + modified it.
adopted ~ 1977ish
was sort standard from 70s to 1999

Best Paper Found a chosen plaintext-attack of size 2^{48} to find a key of 56 bits.

Block Cipher

Break plaintext up into 64 bit blocks



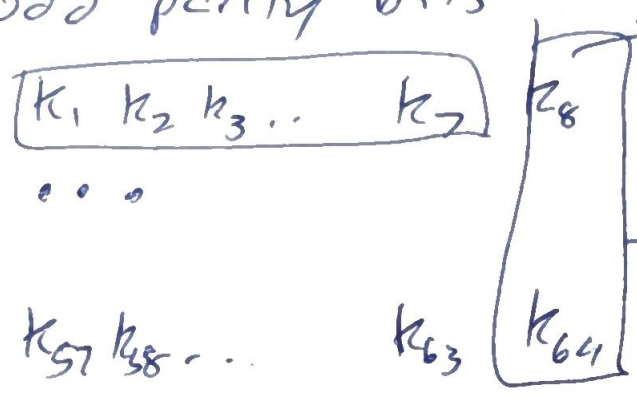
Several "Modes" of running block cipher.

Only talk about encrypting 1 block with a key.

Input Plaintext is 64 bits

key is 56 bits but is transmitted with

8 odd parity bits



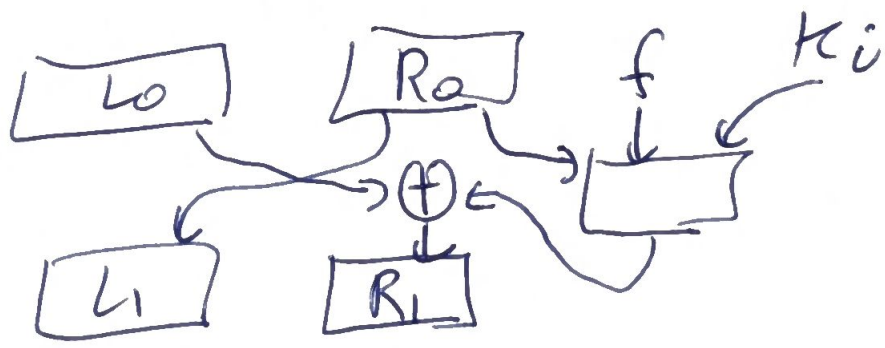
High Level

1. $X \rightarrow IP(X)$, IP is a permutation of bits → Published
   $= L_0 R_0$] L_0 is left 32 bits, R_0 is right 32 bits
2. for $i = 1$ to (16) #Rounds

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

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

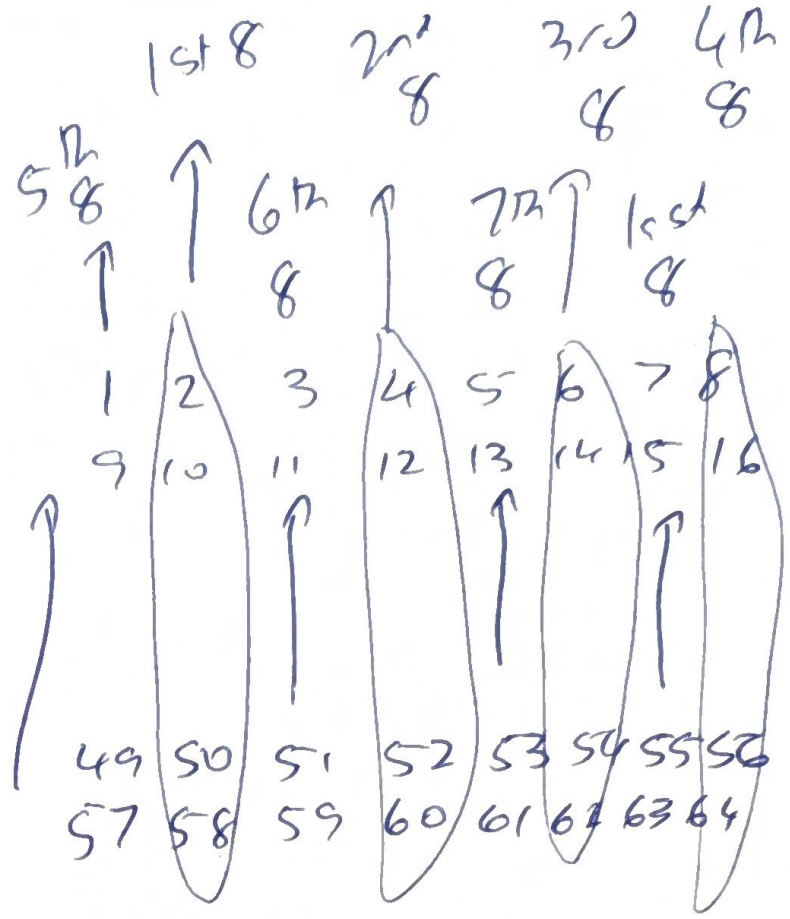
48 bit Round key generated from 56 bit key



3. $IP^{-1}(R_{16} L_{16})$

IP Patterns

58	50 ...	2
60	52 ...	4
62	54 ...	6
64	56 ..	8
57	49 ..	1
59	51 ...	3
61	53 ..	5
63	55 ..	7



Definition of Inverse Function

$f^{-1}(f(x)) = x$

f^{-1}: Decrypting; $f(x)$: Encrypting

$f(R_{i-1}, K_i)$ — 32 bits, 48 bits

1. $E(R_{i-1})$ // (Expansion Matrix) → 48 bits
2. $K_i \oplus E(R_{i-1})$ — 6 bits, 6 bits, ..., 6 bit
3. Let $K_i \oplus E(R_{i-1}) = b_1 b_2 b_3 b_4 \ldots b_8$
   Break these 48 bits into 8 6-bit blocks
   Output $c_i = S_i(b_i)$ for $i = 1$ to 8
   (c_i: 4 bits; b_i: 6 bits)
   Only non-linear part of alg.