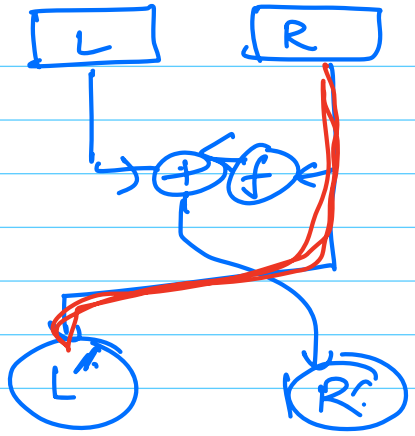
feistel round



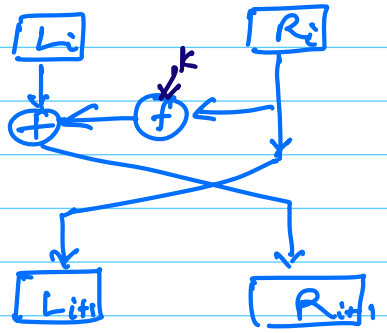
$L_{i+1} = R_i$

$R_{i+1} = L_i \oplus f(k, R_i)$

Jan 31, 2025

(Horst feistel)

1-round of feistel structure



$L_{i+1} = R_i$

$R_{i+1} = L_i \oplus f(k, R_i)$

How to invert ?

given (L_{i+1}, R_{i+1})

$R_i = L_{i+1}$

$L_i = R_{i+1} \oplus f(k, L_{i+1})$

⇒ Claim

if $f(k, .)$ is a PRF (n → n bit) then 1-Round of feistel structure is a PRP (2n → 2n bits)

Correct :

if $f(k, .)$ is a PRF then 1-round of feistel is a permutation.

Que: Prove that claim is wrong.

Proof: Supply input (L, R) → get ans (x, y)

check if $(x == R)$.

Symmetric key crypto community considers two types of PRPs -

① PRP (or weak PRP)

② SPRP (or strong PRP) → PRP ; in theory

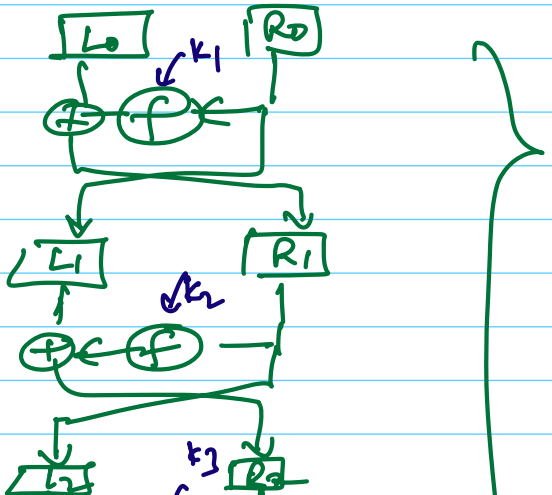
① adv gets access to only the forward computation (or the permutation only)

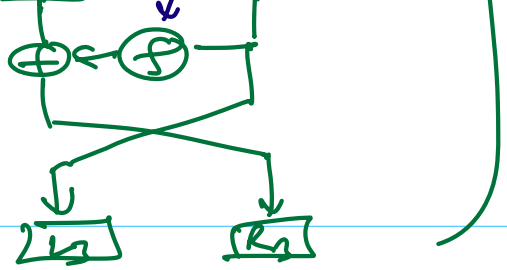
② adv gets access to both permutation as well as inverse permutation

Results:

① if each round function of feistel structure is a independent PRF then 3-rounds of feistel is a PRP

② if each round function of feistel structure is a independent PRF then 4-rounds of feistel is a SPRP.



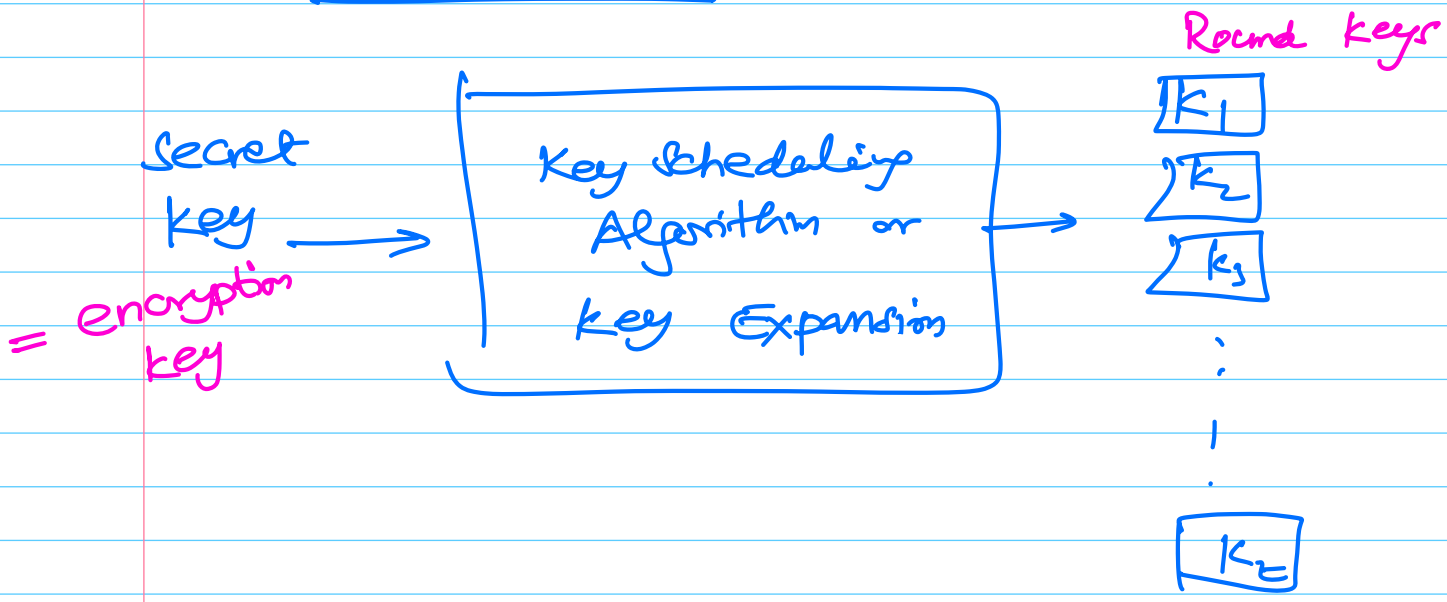


+ 1 more round
= SPRP

Most block ciphers are "iterated block ciphers"

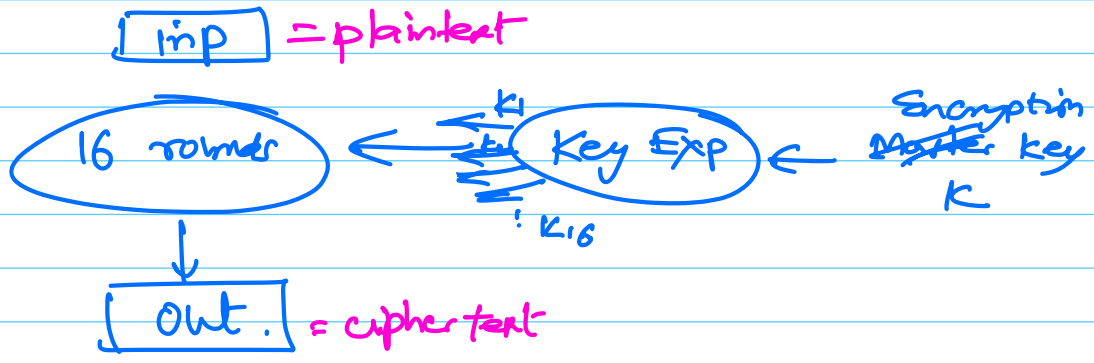
- iterate a specific structure many times

How to generate keys for PRF calls in each round?



DES is an old cipher (now deprecated)

Feistel design with 16 rounds



inp = 64 bit = out

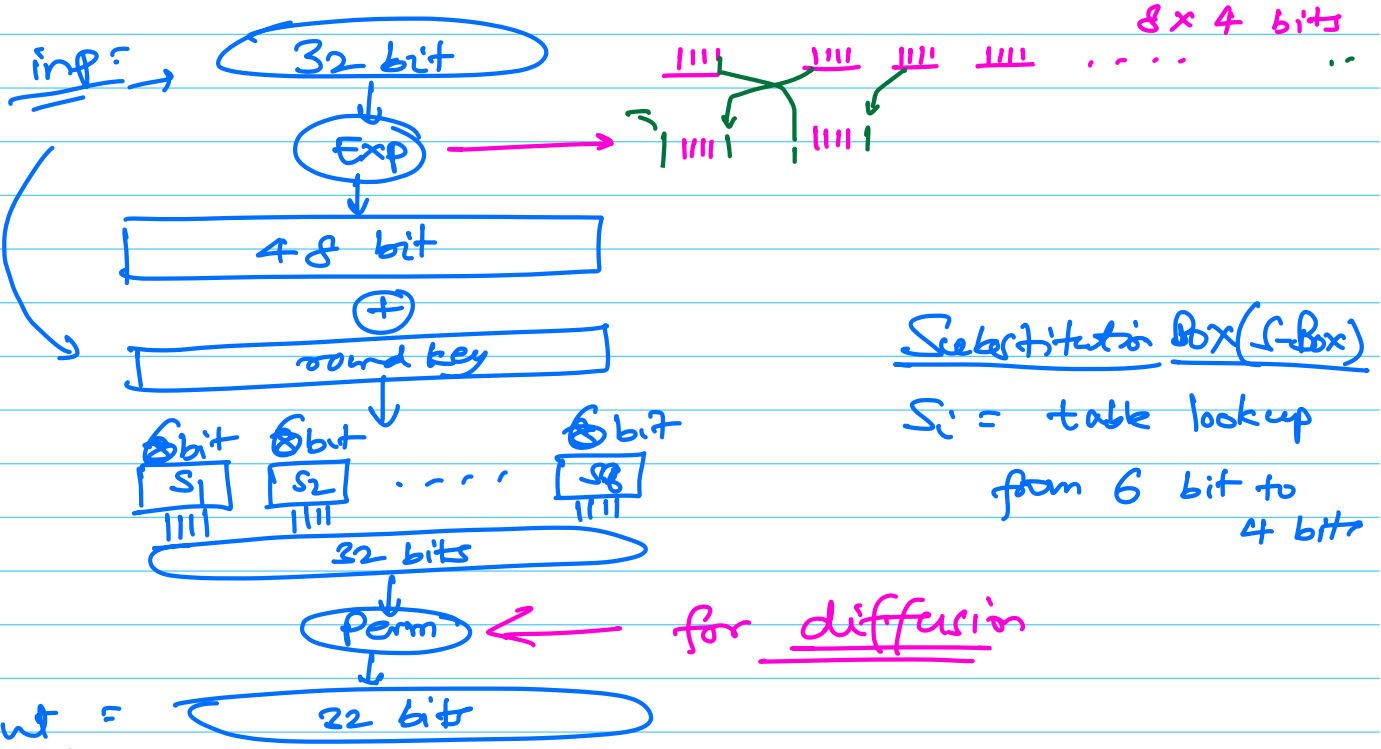
key = 56 bits

Key Expansion

56 bit → 11 round keys of 48 bits each

f function :

32 bits + 48 bits → 32 bits



f-function of DES

Substitution Box (S-Box)

S_i = table lookup from 6 bit to 4 bits

for diffusion

S-box specification : 64 input → 4 bits

bits of input

$x_1 x_2 x_3 x_4 x_5 x_6$

$x_1 x_6$ \ $x_2 x_3 x_4 x_5$	0 . . . . . f
00	
01	
10	
11	

4x16 table each entry containing a hex value

each row is a permutation of nos $\{0, 1, 2, \ldots f\}$

Differential Cryptanalysis (90's)

fix some input diff. $:= \delta \xrightarrow{\text{out}} \delta'$

pick inps $(x, x \oplus \delta)$

get outs $\downarrow y \quad \downarrow y'$

$(x, x \oplus \delta) \rightarrow (y, y')$

where $y \oplus y' = \delta'$

$\Rightarrow$ good pair

$\longrightarrow$ Secret key extraction

Biham & Shamir - applied this technique on all known block cipher at that time

LOKI, ... Broke

DES strong

~ 90's : Coppersmith et. al → "Design criteria of DES"

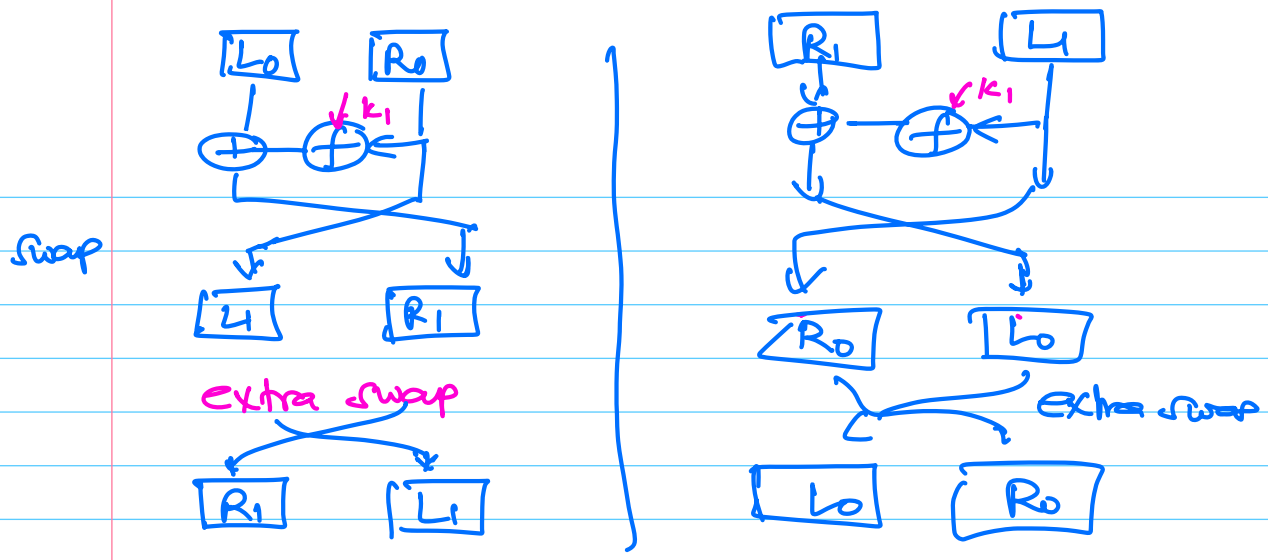
T-attack = diff. cryptanalysis

92' Cryptanalysis of DES by Biham & Shamir

full 16 rounds were broken

Requirement: 2^{47} chosen plaintexts are needed

56 bit key is recovered in $< 2^{56}$ time



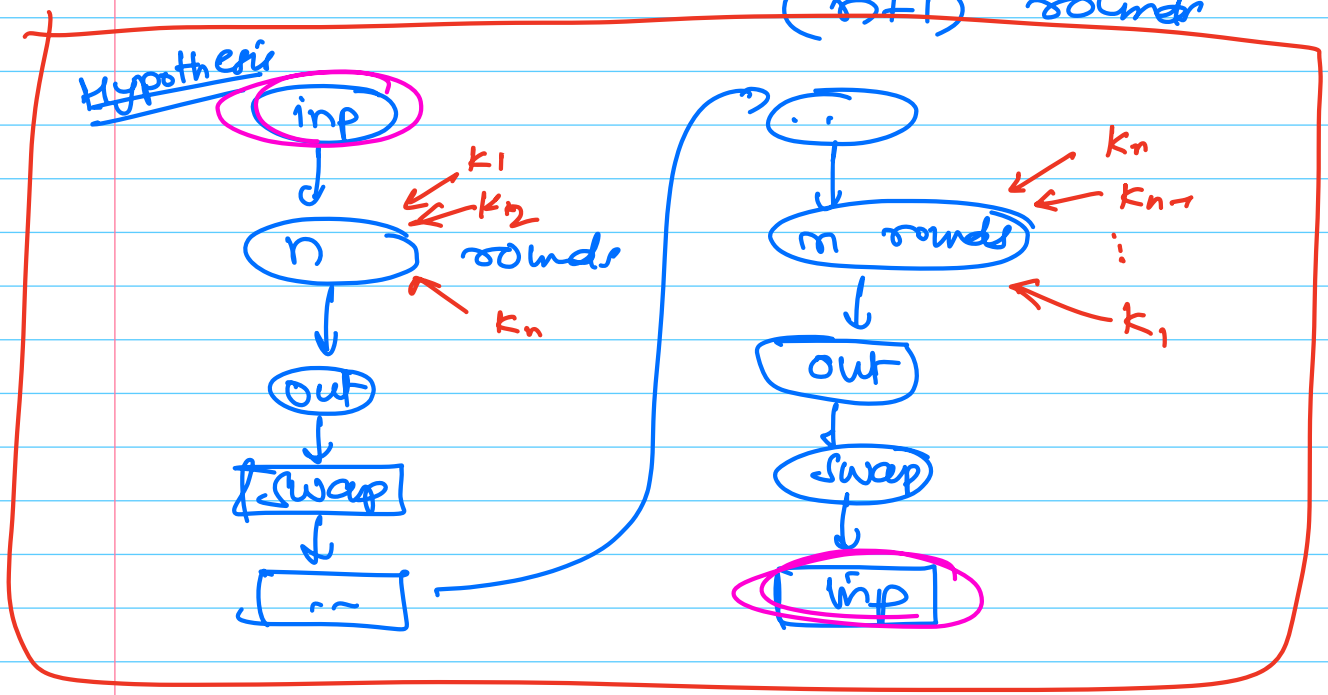
Any no. of rounds can be decrypted this way.

Proof By using Mathematical Induction:

Basis: 1 - round — we showed above

Hypothesis: Assume this works for n-rounds

Inductive step: to prove that it works for (n+1) rounds



for (n+1) rounds