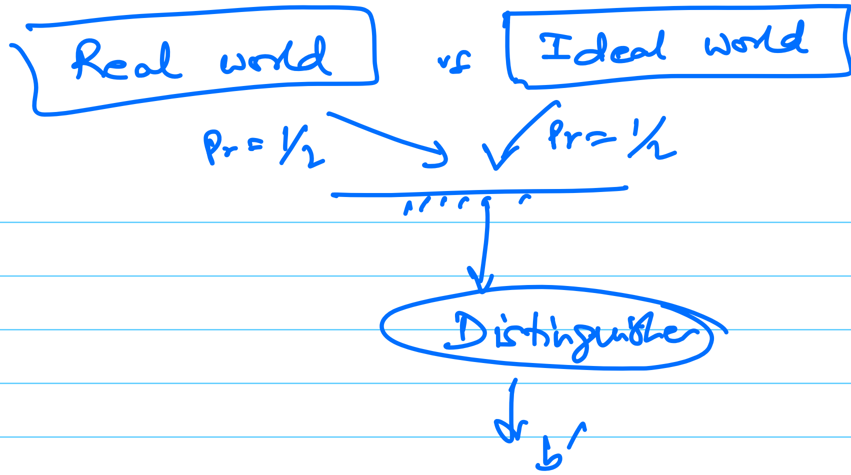
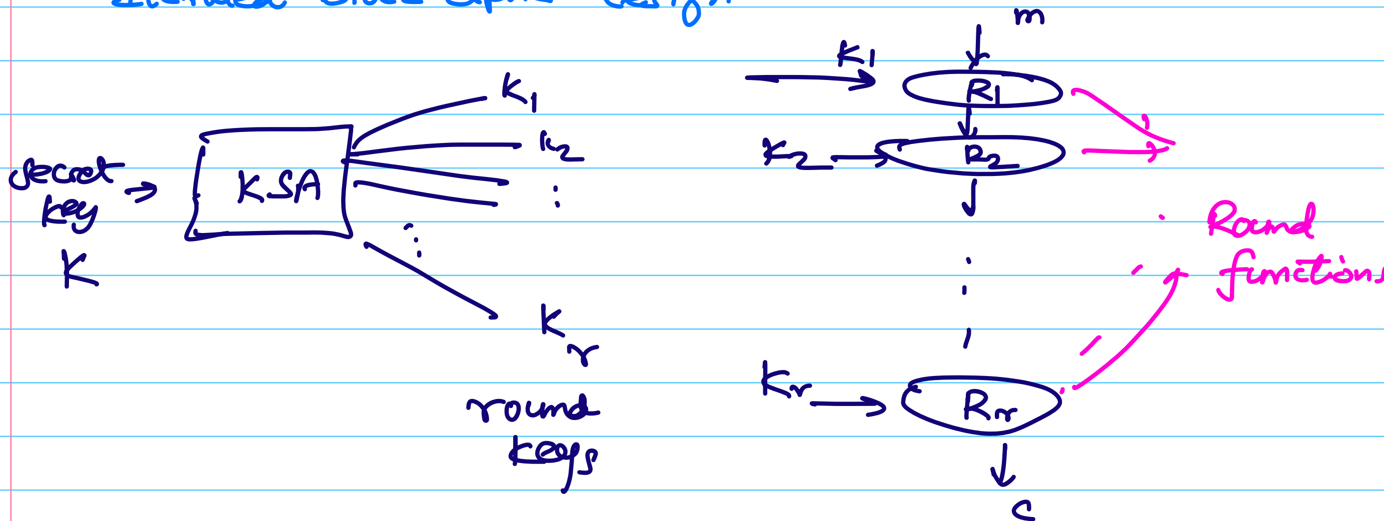
4 · feb 2025



Last class:

Iterated Block cipher design



Round function:

DES had a round function designed as a feistel Structure

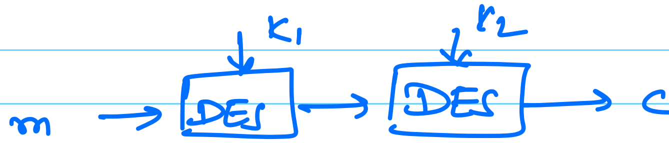
Issues with DES:

(i) hidden design – (fear of hidden trapdoors)

(ii) Small key size

(Lucifer had 128 bit keys)

Can we increase the key size?

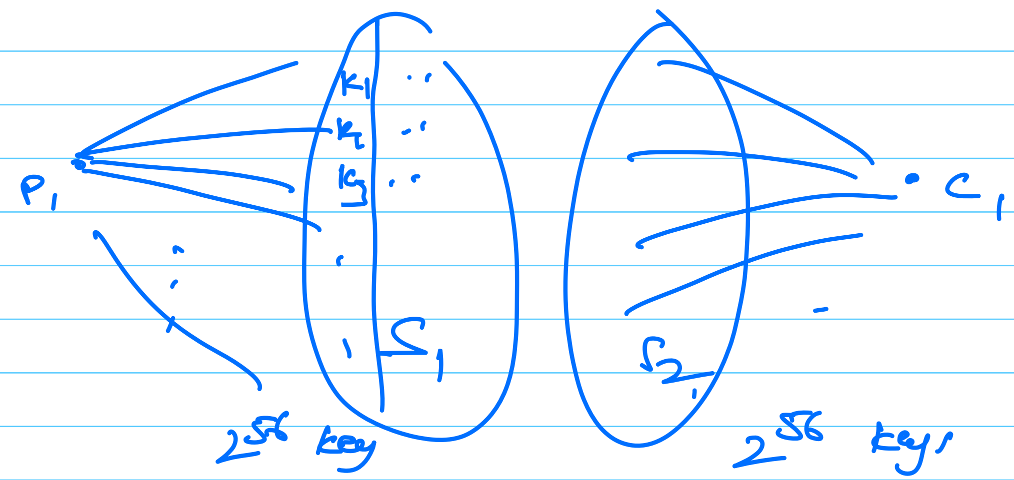


2-DES

= 112 bit key

2-DES is not 112-bit secure.

Suppose we have $(P_1, C_1), (P_2, C_2), \ldots$



Practically,

(i) create S_1 : effort $= 2^{56}$ calls to DES

(ii) Sort S_1 on ciphertext part

(iii) for loop for diff k^* $\{ \text{Dec}(k^*, c_1) \}$

if match:

$$P_1 \xrightarrow{K_1} \text{mid} \xleftarrow{K} C_1$$

$\Rightarrow$ $\boxed{\text{Potential key} = K_1 \| K_2}$

$=$ Cost $= 2^{56}$ calls to 2-DES

+ memory 2^{56} entries ($= 56 + 64$ bits)

Check the potential keys with another pair (P_2, C_2)

$\Rightarrow$ w.h.pr only 1 candidate key is left

What next? 3-DES

$$m \longrightarrow \boxed{DES}_{k_1} \longrightarrow \boxed{DES}_{k_2} \longrightarrow \boxed{DES}_{k_3} \longrightarrow c$$

make $k_1 = k_3$ $\Rightarrow$ 2 key 3-DES

$\simeq$ 112 bit security

Change management:

DES $\longrightarrow$ 3DES in individual machines

k_1, k_1^{-1}, k_2

$= k_2$

90's - trapdoor fear

NIST - call for proposal

- open to world (~ 1997)

Advanced Encryption Standard — competition

Evaluation criteria - (i) security

(ii) efficiency in both s/w & h/w

(iii) elegance & resistance to cryptanalysis

(iv) no patent

(available world-wide without any royalty)

~ 3 years of effort – public scrutiny
3 workshops

3rd round – 5 designs left

✓ (i) Rijndael – Rijmen & Daemen
(ii) Twofish
(iii) TIGER
(iv) ..
(v) ..

AES: Standard 128 bit block
key $\in \{128, 192, 256\}$
$\Rightarrow$ AES-128, AES-192, AES-256

(Rijndael supported block sizes of 128, 192, 256)

Iterated Block cipher:
Based on finite field operations

Group: Set $(S, *)$ — Abel

Additional property:
if $\forall\, a, b \in S$
$a * b = b * a$
then group is commutative

(i) closure
if $a, b \in S$, then $a * b \in S$

(ii) Associativity
if $a, b, c \in S$
then $(a * b) * c = a * (b * c)$

(iii) Identity
special element $e \in S$
s.t $\forall\, a \in S$ $a * e = a$
$e * a =$

(iv) Inverse $\quad \forall a \in S$

$\exists\ b \in S$ s.t. $\quad a * b = e$

denoted as $b = a^{-1}$

$\mathbb{Z}_p^* = \{1, 2, 3, \ldots (p-1)\}$ for a prime p

operation = $\times$ mod p

$a \times b \neq 0 \bmod p$

Inverse ?:

For any $a \in \mathbb{Z}_p^*$ $\exists\ b \in \mathbb{Z}_p^*$ s.t.

$ab \equiv 1 \bmod p$

Proof:

$\mathbb{Z}_p^* = \{\underline{1, 2, 3, \ldots (p-1)}\}$

$a \cdot \mathbb{Z}_p^* = \{\underline{a*1, a*2, a*3, \ldots a*(p-1)}$

Suppose $\quad a \cdot i = a \cdot j \bmod p$

$\Downarrow$

$a(i-j) = 0 \bmod p$ $\longrightarrow$ Impossible for distinct i, j

Finite field:

$(S, +, \cdot)$

(i) $(S, +)$ is a commutative group, with 0 as additive ident.

(ii) $(S - \{0\}, *)$ is a commutative group

(iii) $+, *$ distribute

$$a*(b+c) = (a*b)+(a*c)$$

6-feb-25

Recall: Group: $(G, *)$

Necessary

(i) closure: $\forall\, a, b \in G,\ a*b \in G$

(ii) Associativity: $\forall\, a, b, c \in G,$

$$a*(b*c) = (a*b)*c$$

(iii) Identity: $\exists\, e \in G$ s.t.

$\forall\, a \in G$

$$e*a = a*e = a$$

(iv) Inverse: $\forall\, a \in G$

$\exists\, b \in G$

s.t. $a*b = e$

Additional: (v) Commutativity

$\forall\, a, b \in G,\quad a*b = b*a$

when it is satisfied for a group G, G is called an Abelian group