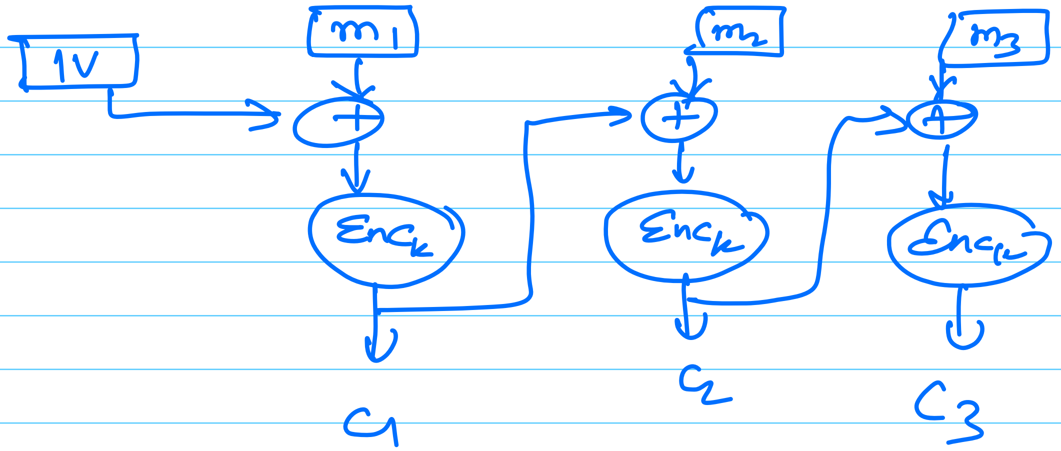
② Cipher Block Chaining (CBC)



inp = (m_1, m_2, m_3)

ciphertext = (IV, c_1, c_2, c_3)

---

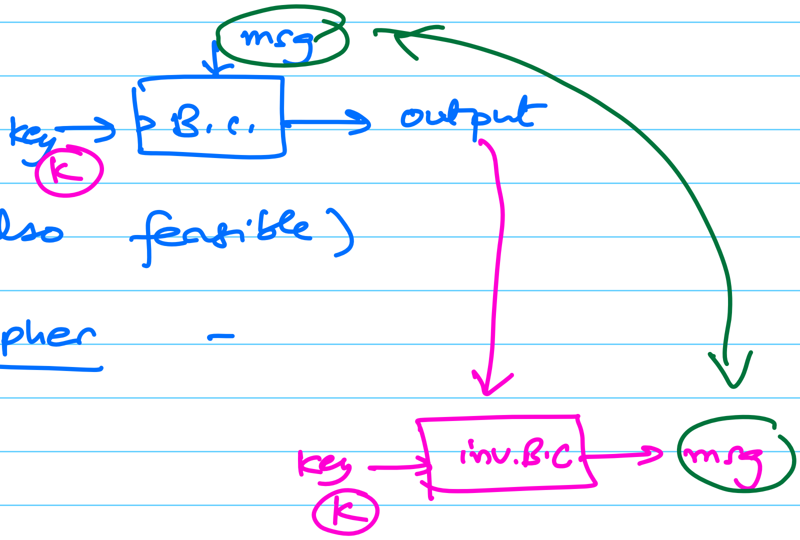
30 Jan 2025

PRF → PRP → in practice = Block Cipher

Block Cipher:

- an practical realization of a PRP
- n bit → n bit permutation
- deterministic construction

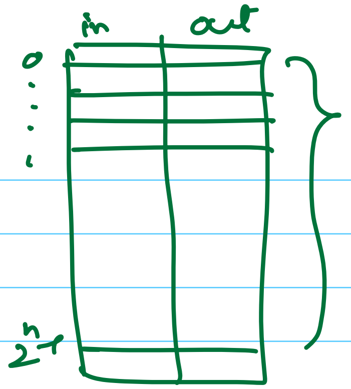
Syntax:



(inversion is also feasible)

Inverse Block cipher –

PRP:



all 2^n values exactly once

PRP $(\text{no.} = 2^k)$ $\simeq_c$ RP $\text{no.} = (2^n)!$

Security game:

Challenger | Adversary

$b \xleftarrow{\$} \{0,1\}$

if(b==0) pick a RP

else pick a random key k & setup PRP(k, ·)

interaction $\rightleftarrows$ $= \text{poly}(n)$ queries

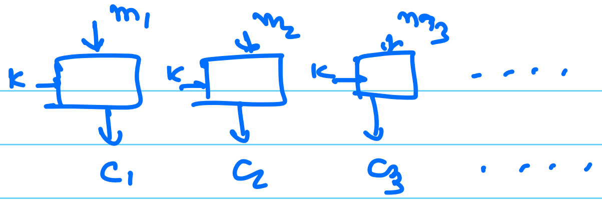
Predict b'

if $(b' == b)$. Adv wins
else she loses

Construction is a PRP if $\Pr(\text{Adv wins}) = \frac{1}{2} + \epsilon(n)$

For practical / real-life encryption scheme, we need to use a mode of operation

① ECB : (Electronic Code Book)



inp = $(m_1, m_2, m_3, \ldots)$

ciphertext = $(c_1, c_2, c_3, \ldots)$

Weaknesses : (i) deterministic construction

=> insecure

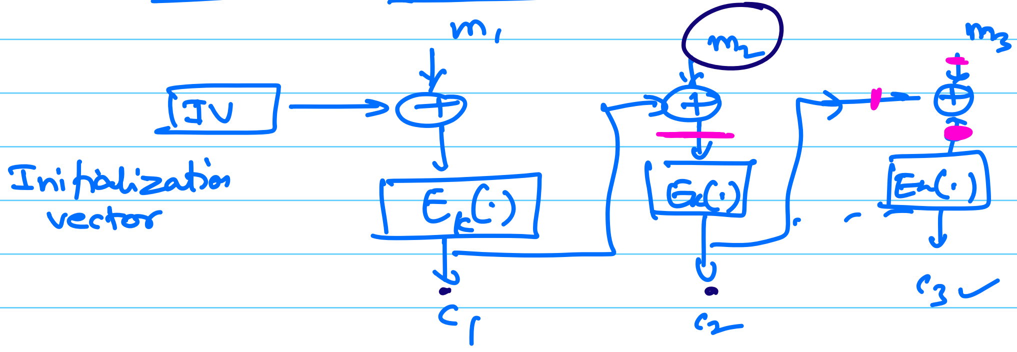
Easiest attack :

- given $(c_1, c_2, c_3) \rightarrow$ send (c_2, c_1, c_3)
- image encryption (Penguin)

useful only when encrypting 1 block

(or when used rarely with guarantee that all blocks are different)

② CBC : (very popular)



inp = $(m_1, m_2, \ldots)$

ciphertext = (IV, c_1, c_2, ...)

ciphertext length = 1 block more than plaintext

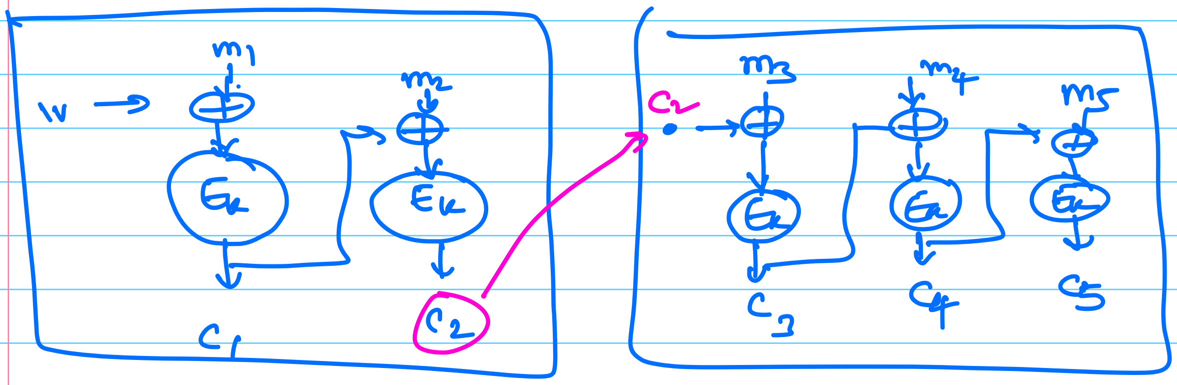
if $c_i \oplus m_{i+1} = c_j \oplus m_{j+1}$

then $c_{i+1} = c_{j+1}$

Adv (an adversary can break security property of CBC mode) $\leq$ Adv (breaking the property of block cipher) + Pr (inp- collision)

③ Chained CBC

one problem of CBC is that you need to generate an IV for every new message



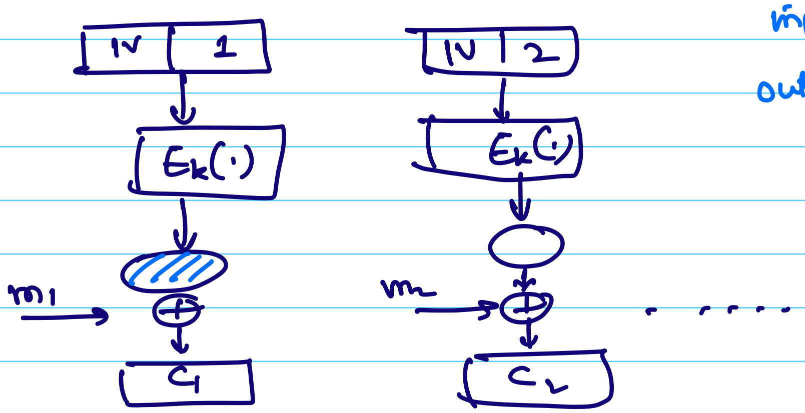
used in SSL 3.0 & TLS 1.0

④ CTR mode (Cocenter mode)

- Extremely popular

inp = $(m_1, m_2, \dots)$

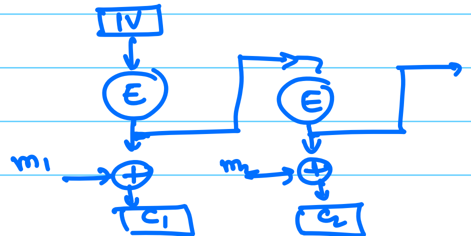
out = $(IV, c_1, c_2, \dots)$



Converts a block cipher into a stream cipher

- no decryption circuit needed
- any block can be decrypted without waiting for other blocks
- Error propagation

⑤ OFB (Output feedback mode)



How to design a block cipher ?

Computerization → banks

Lloyds bank (London)

NIST (NBS → National Bureau of Standard)
(← National Inst for Std. & Tech.)
under the dept of commerce, US govt.

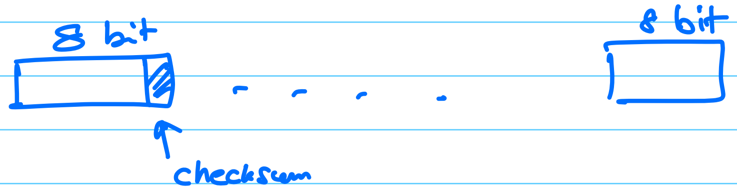
Requirements → asked for designs
revised → asked again

IBM – designed Lucifer

Don Coppersmith, Horst Feistel, ...

Revised by NSA –
→ Became Data Encryption Standard
DES (70^{s})

64 bit block cipher
56 bit secret key

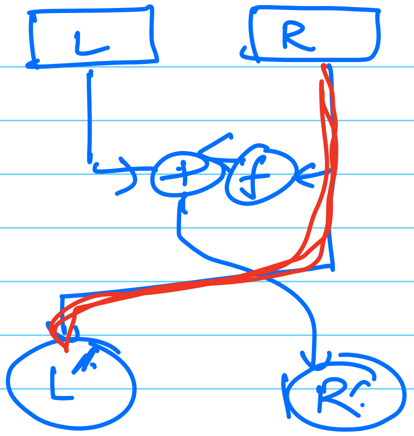


8 blocks × 7 bits
= 56 bits

(i) The biggest criticism of DES — small key size

(ii) design criteria are not public
– fear of hidden trapdoors

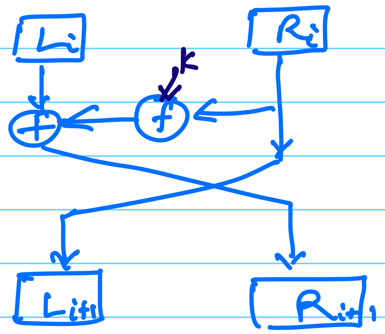
feistel round



$L_{i+1} = R_i$

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

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 $f(k, \cdot)$ is a $\overset{n \to n \text{ bit}}{\text{PRF}}$ then 1-Round of feistel structure is a $\underset{2n \to 2n \text{ bits}}{\text{PRP}}$

Correct :

if $f(k, \cdot)$ 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 $(x == R)$.