28 Jan 2025

PRF : $\{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$

fixing a key, fixes the function

Table

inp	out

gets determined completely

indexed functions

↳ indexing is by the key

Enc. a message of size n-bits

$f(k,\cdot)$

$f_k(\cdot)$ = PRF obtained by fixing the key to be k.

$$Enc_k(m) = (r, f_k(r) \oplus m)$$

PRP - Pseudo-Random Permutation

$$\{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$$

index → $\{0,1\}^k$

restriction from PRF case: the new object is a permutation.

inp	out
↓	↓
all 2^n values	"

PRF vs PRP

(i) toss a coin — choose either a PRF or a PRP

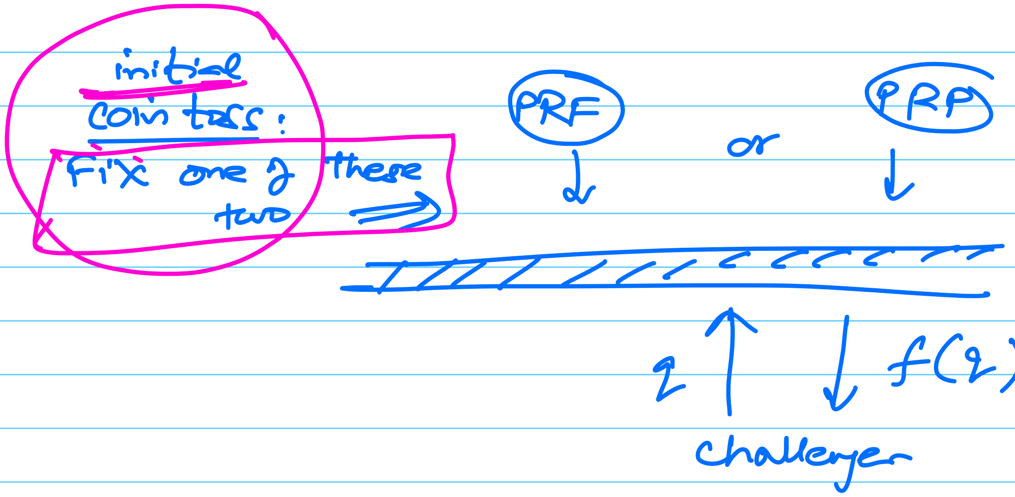
(ii) challenger is given oracle access

(iii) goal is to find out which one ?

Suppose challenger has q queries,
what is the pr. that the challenger distinguishes ?

What happens if a query is repeated ?

- Because answers are consistent, challenger doesn't benefit
- hence all queries should be distinct (to benefit challenger)



Pr of (distinguishing) = Pr (of two distinct queries outputs colliding)

PRP–PRF switching lemma:

$$\Pr\left(\begin{array}{l}\text{distinguish a PRP} \\ \quad\text{\& a PRF with} \\ q \text{ queries}\end{array}\right) \le \frac{q^2}{2 \cdot 2^n}$$

Out of q queries $\rightarrow$ ${}^{q}C_{2}$ pairs

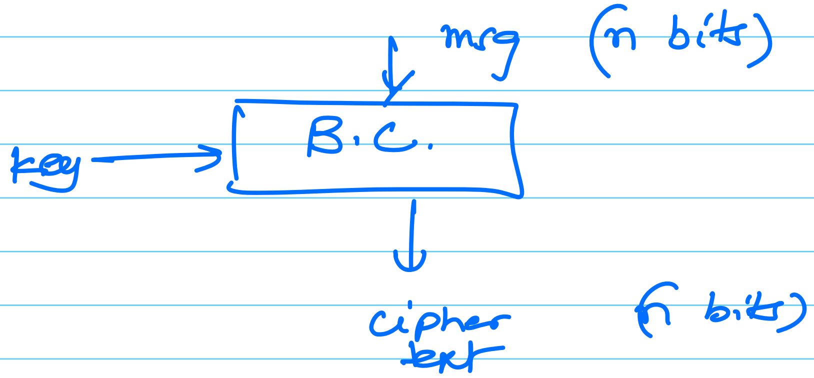
$$= \frac{q(q-1)}{2} \sim \frac{q^2}{2}$$

if $q = poly(n)$ then $\boxed{\cdots \le negl(n)}$

PRP^s are realized in practice by a construction known as Block Cipher

alternately,

Block cipher = PRP in practice



This is a deterministic construction

$\Rightarrow$ Should not be used for encryption in a direct manner.

Triangle inequality

objects O_1, O_2, O_3

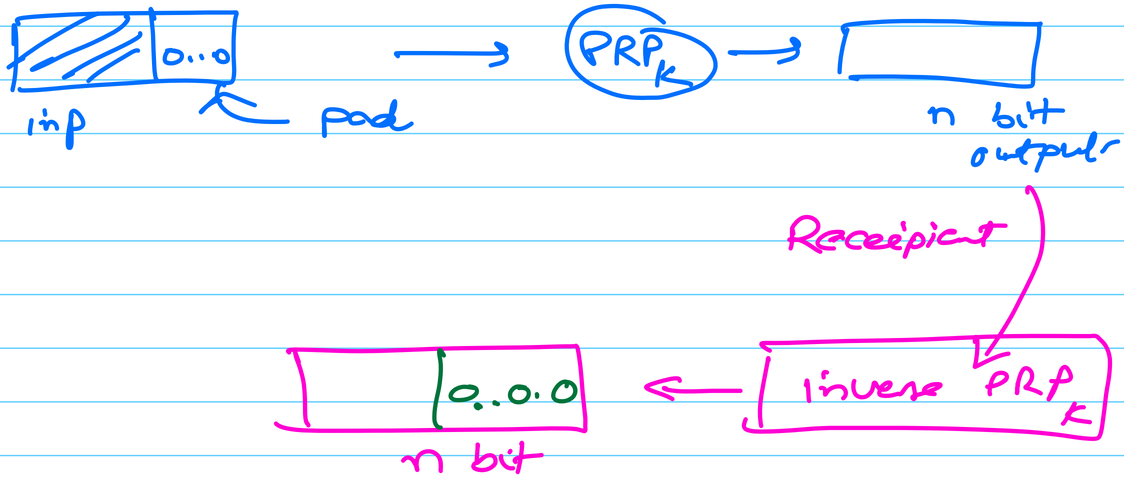
$$\text{Prob.}\begin{pmatrix}\text{to distinguish}\\ \text{between } O_1 \,\&\, O_3\end{pmatrix} \leq \Pr\begin{pmatrix}\text{distinguish between}\\ O_1 \,\&\, O_2\end{pmatrix} + \Pr\begin{pmatrix}\text{dist. between}\\ O_2 \,\&\, O_3\end{pmatrix}$$

$$RF \xrightarrow[\epsilon(n)]{} PRF \xrightarrow[q^2/2^{n+1}]{} PRP$$

How to encrypt messages which are not of n-bits?

(how to evaluate PRP on inputs of length ≠ n.)

1. if message is small → do some padding

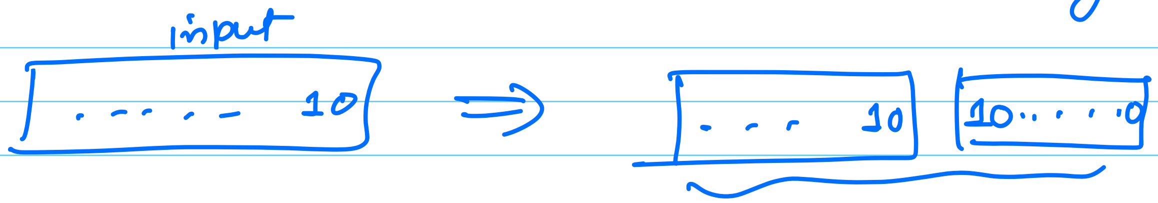


0^* padding does not work

Usual: 10^*

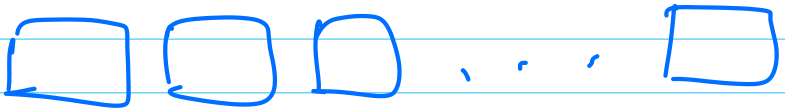
Any invertible padding is fine

2. if padding is used — then it is required to be used always



3. when message length is > n

use padding + enough to make it a multiple of n bits

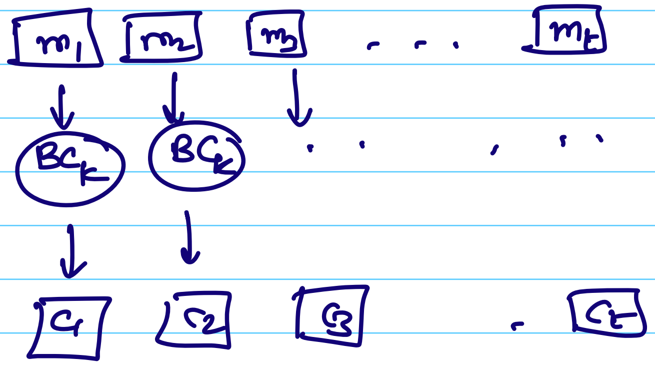


Blocks of sizes n-bits will be processed by a block cipher

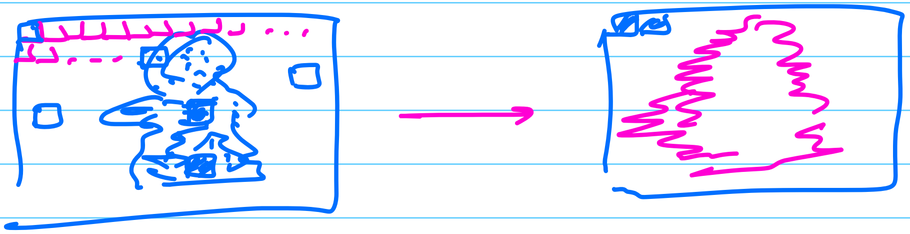
Mode of Operation

method for domain extension of a block cipher

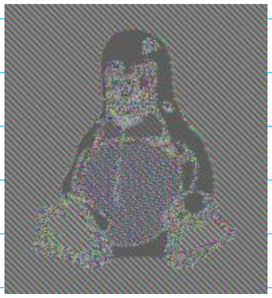
① ECB (Electronic Code Book)



Reordering ciphertext → reordering of plaintext



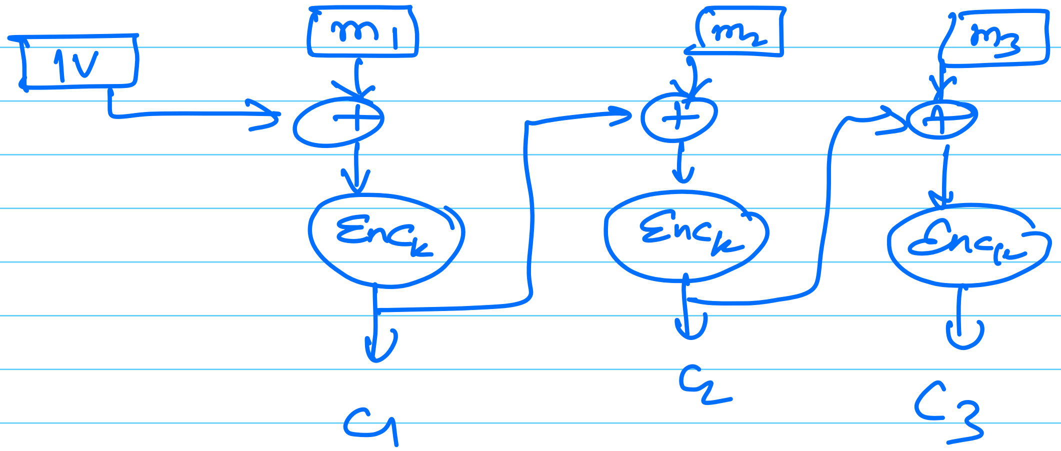
Penguin



ECB penguin

Masterkey → session key_1, session key_2, ... used in practice

② Cipher Block Chaining (CBC)



$inp = (m_1, m_2, m_3)$

$ciphertext = (IV, c_1, c_2, c_3)$

---

30 Jan 2025

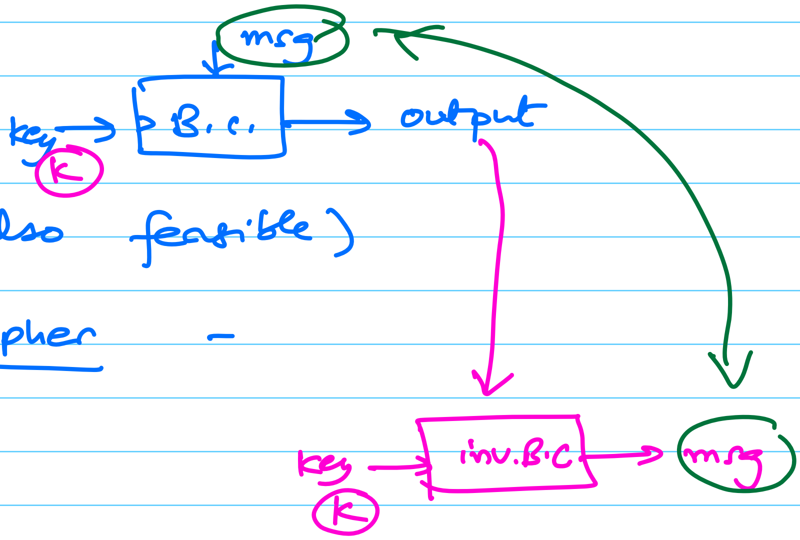
PRF → PRP

→ 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 –