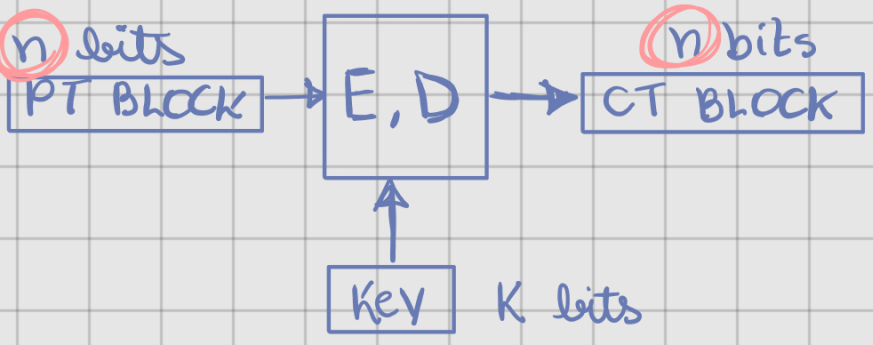
BLOCK CIPHERS

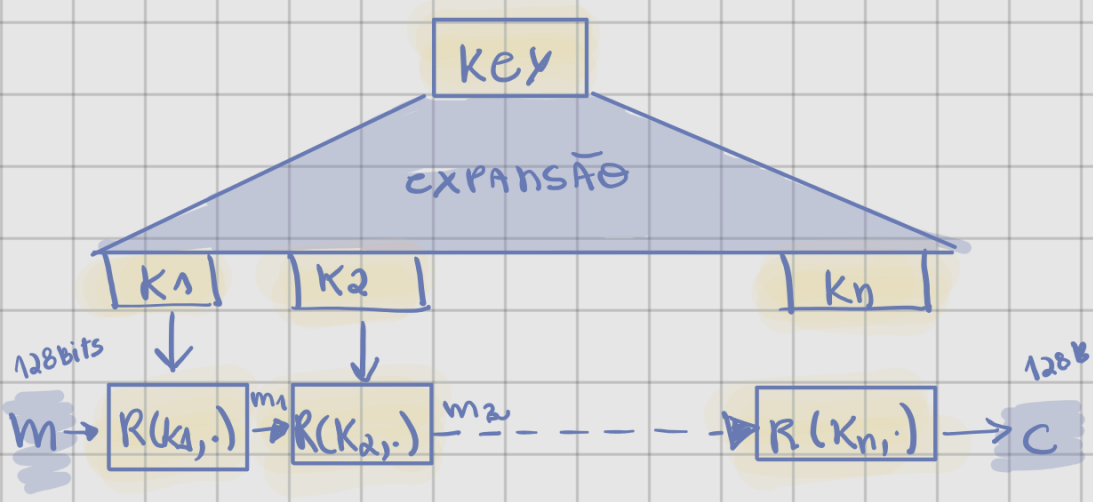


Exemplos:

I. 3DES: n = 64 bits
K = 168 bits

II. AES: n = 128 bits
K = 128, 192, 256 bits

CIFRAS DE BLOCO CONSTRUÍDAS POR ITERAÇÃO

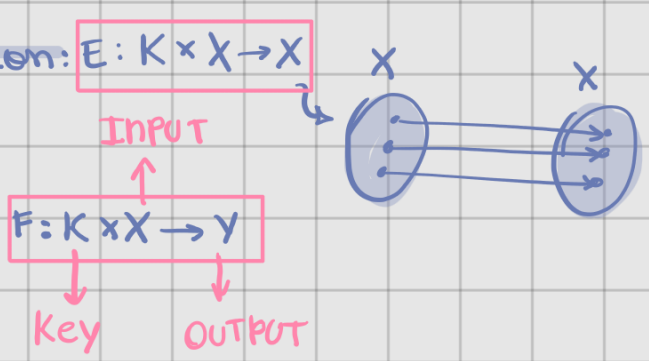


R(K,m) é a função de arredondamento → 3DES: n = 48
AES: n = 10

pseudo random permutation: $E: K \times X \to X$

PRPs e PRFs

pseudo random function: $F: K \times X \to Y$



PRF SEGURO

* Considerando $F: K \times X \to Y$ seja uma PRF

$\begin{cases} Funs[X,Y]: \text{o conjunto de todas as funções de } X \text{ para } Y \\ S_F = \{ F(K,\cdot) \text{ o qual } K \in \mathcal{K} \} \subseteq Funs[X,Y] \end{cases}$