cifrari a blocchi.

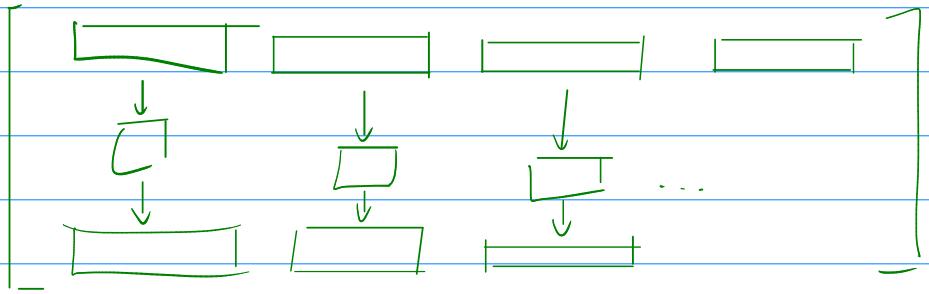
3DES K_1, K_2 $56 \times 2 = 112$ bits di chiave

b = 64

N.B DES non è usato per codificare un solo blocco!

Ha senso cifrarsi con la medesima chiave come vengono codificati blocchi differenti.

ECB



"cifrario monoalfabetico dove l'alfabeto consta di N i blocchi di 64 bits → ALFABETO DI 2^{64} CARATTERI.

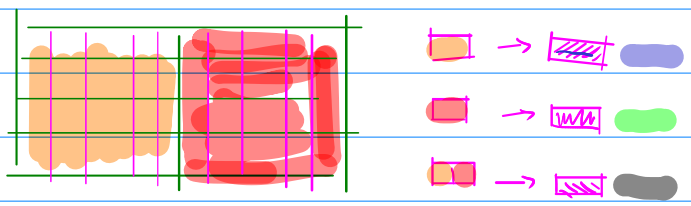
ECB → electronic codebook (mode)

sostituzioni possibili → $2^{64}!$

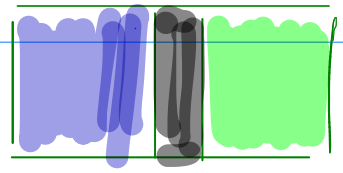
possibili sostituzioni che nascono dalle chiavi di DES

2^{56}

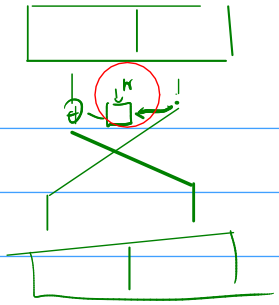
3DES $2^{112} << 2^{64}!$



encoding con ECB

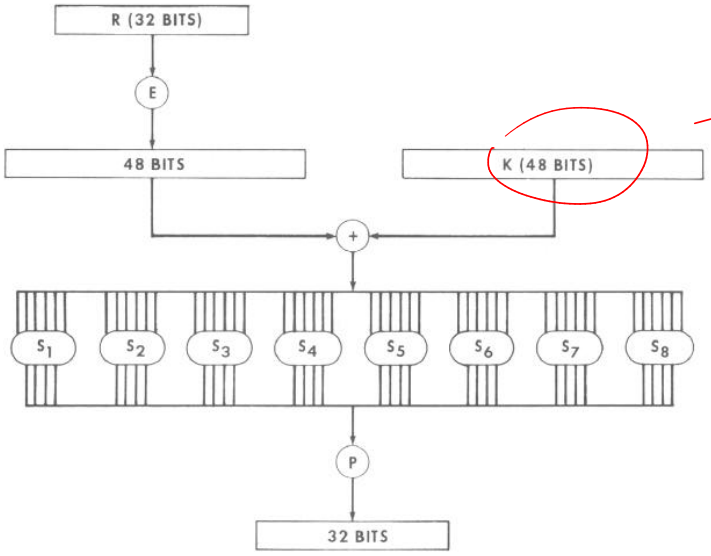


DES: architettura iterata



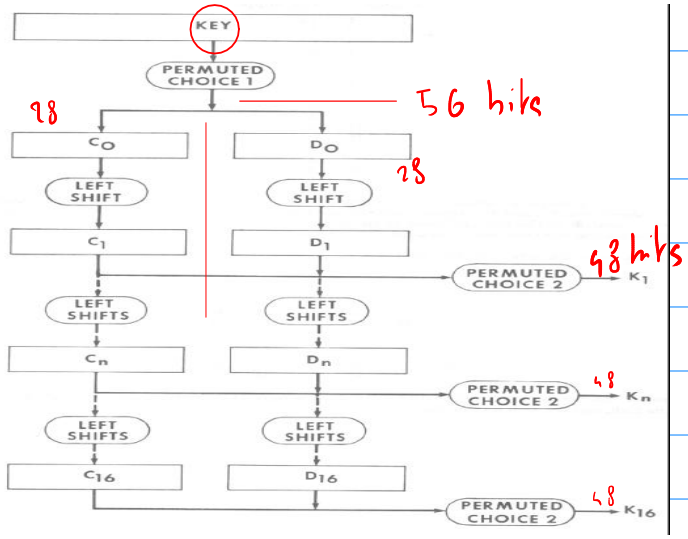
S-boxes

Ad ogni ciclo si inserisce una sottochiave k_i



→ k_i derivata da k

Ad ogni ciclo si inserisce una sottochiave differente (i.e. 48 bits derivati dalla chiave in modo diverso).



key = k k 64 bit

Idealmente le sottochiavi dovrebbero nascere da una sorta di stream cipher.

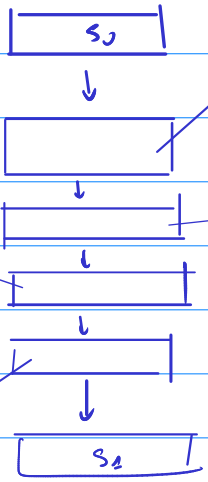
key scheduling = generazione delle sottochiavi

Limite DES → non è facile da estendere.

Architettura di AES

Abbiamo uno stato interno → rappresentato da una matrice 4x4 con bytes come entrate. (elementi di un campo finito)

→ Su questo stato si applicano una successione di operazioni invertibili.



AddRoundKey.
$S \oplus K_i$

subbytes (lavora a livello di bytes ed è una sostituzione monoalfabetica)

shiftrows
↓
fa scorrere le righe mescola le entrate in colonne diverse

mixcolumns.
→ ↓
fa interagire fra loro entrate in righe diverse

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
   byte  state[4,Nb]

   state = in

   AddRoundKey(state, w[0, Nb-1])                  // See Sec. 5.1.4

   for round = 1 step 1 to Nr-1
      SubBytes(state)                              // See Sec. 5.1.1
      ShiftRows(state)                             // See Sec. 5.1.2
      MixColumns(state)                            // See Sec. 5.1.3
      AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
   end for

   SubBytes(state)
   ShiftRows(state)
   AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

   out = state
end
```

bytes ← righe → colonne

bit

Figure 5. Pseudo Code for the Cipher.[1]

le operazioni sono fatte bit per bit mentre subbytes.

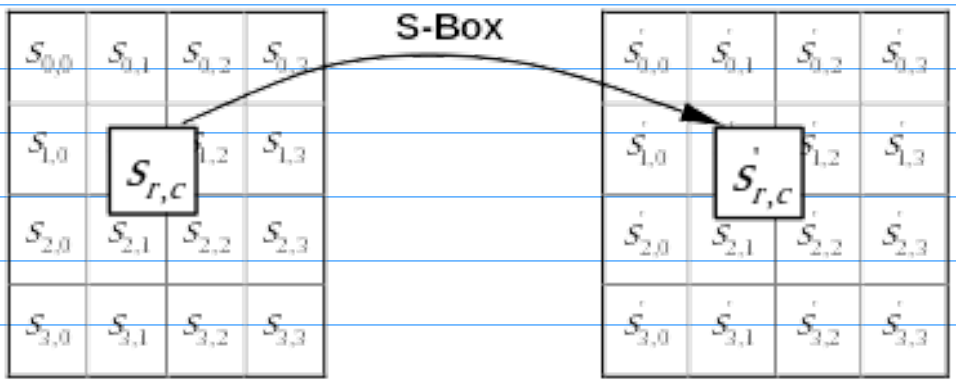


Figure 6. SubBytes( ) applies the S-box to each byte of the State.

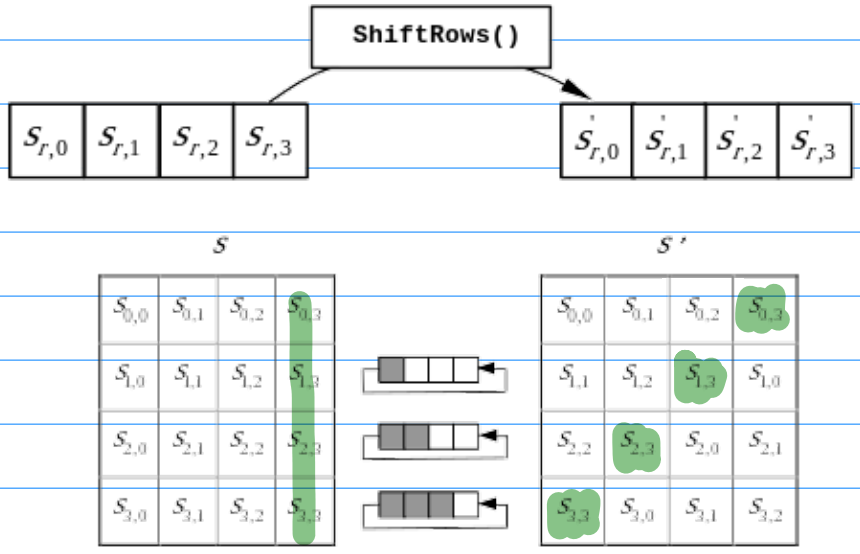


Figure 8. ShiftRows( ) cyclically shifts the last three rows in the State.

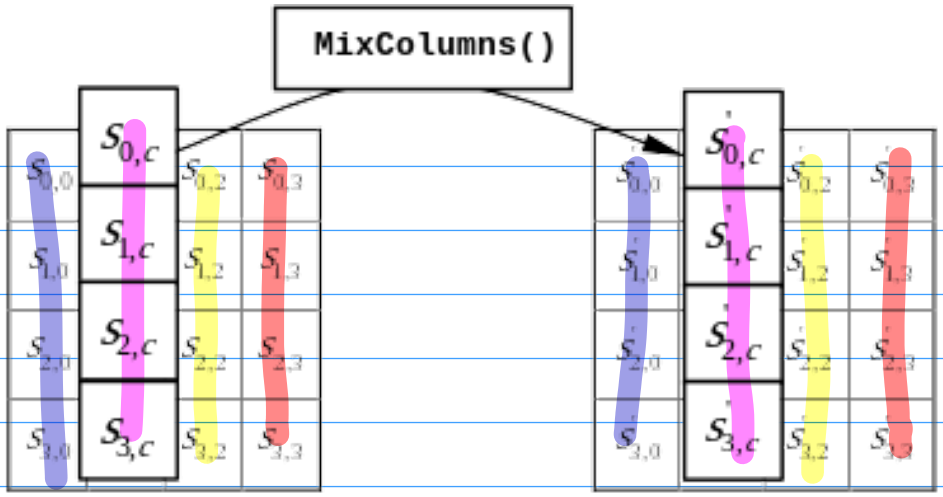


Figure 9. MixColumns() operates on the State column-by-column.

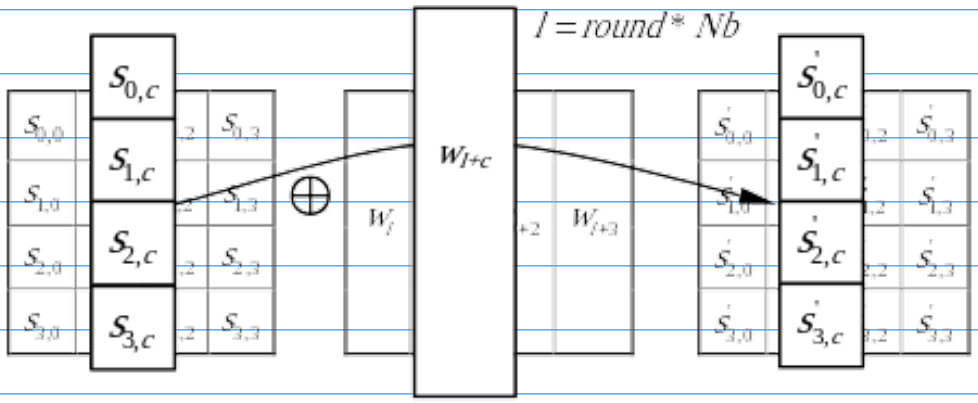


Figure 10. AddRoundKey() XORs each column of the State with a word from the key schedule.

Le operazioni di AES sono definite in termini algebrici
→ inclusa la subbytes.

→ IDEA DI BASE considerare i bytes come elementi di un campo finito con 256 elementi, $\mathbb{F}_{256}$
↓
TRASFORMARLI IN MODO NON LINEARE CON LA SUBBYTES.

→ le colonne (ma anche le righe) dell'array di stato sono considerate come polinomi in $\mathbb{F}_{256}$

COME COSTRUIRE UN CAMPO CON 256 ELEMENTI?

$(\mathbb{Z}_p, +, \cdot)$ con p primo è un campo

Teorema: Sia p primo $k \geq 1 \Rightarrow \exists$ un campo finito con p^k elementi che chiameremo $\mathbb{F}_{p^k}$

N.B. $\boxed{\mathbb{F}_{p^k} \neq \mathbb{Z}_{p^k}}$ se $k > 1$

COSTRUZIONE DI $\mathbb{Z}_p$ a partire da $\mathbb{Z}$

1) partiti da $\mathbb{Z}$ e considerato $p\mathbb{Z}$ l'insieme dei multipli di p in $\mathbb{Z}$ con p primo.

2) osservato che $p\mathbb{Z} \leq \mathbb{Z}$ è un ideale di $\mathbb{Z}$

cioè $(p\mathbb{Z}, +, \cdot)$ è un anello commutativo (senza identità)

? $\boxed{a \cdot p\mathbb{Z} \subseteq p\mathbb{Z}}$

3) $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ è un anello con unità $1 + \mathbb{Z}_p$

4) in $\mathbb{Z}/p\mathbb{Z}$ abbiamo fatto vedere che $\forall$ elemento diverso da $0 + p\mathbb{Z}$ ammette inverso usando l'algoritmo euclideo esteso.

perché dato $x \neq 0$, $x + p\mathbb{Z}$ troviamo con alg. euclideo esteso y tale che $\boxed{xy + pk = 1}$ (che è risolubile perché $0 < x < p$, p primo $\Rightarrow MCD(p, x) = 1$) e

$$(x+p\mathbb{Z})(y+p\mathbb{Z}) = xy + p\mathbb{Z} = \underline{1} + p\mathbb{Z}$$

e dunque $(y+p\mathbb{Z})$ è l'inverso moltiplicativo di $x+p\mathbb{Z}$.

$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ è un campo $\Leftrightarrow$ p è primo.

La stessa costruzione si può fare ogniqualvolta abbiamo un <u>dominio euclideo</u>

↓

AMBIENTE IN CUI VALE L'ALGORITMO EUCLIDEO → AMBIENTE IN CUI SI PUÒ APPLICARE L'ALG. DELLA DIVISIONE CON RESTO

prop. fondamentale: il resto è "più piccolo" del divisore

Def: Un anello commutativo con unità $(A,+,\cdot)$ è detto dominio euclideo se

1) $\forall a,b \in A : ab=0 \Leftrightarrow a=0$ oppure $b=0$
(A è un dominio di integrità).

2) $\exists$ una funzione $\partial : A\setminus\{0\} \to \mathbb{N}$ tale che $\forall a \in A, \forall b \in A\setminus\{0\}$ abbiamo che

a è divisibile per b

$a = bq$ per $q \in A$ oppure

$a = bq + r$ con $q, r \in A$, $\partial(r) < \partial(b)$

il "resto" della divisione di a per b ha $\partial(r) < \partial(b)$

[valutazione euclidea]

Esempi: $(\mathbb{Z},+,\cdot)$, $\partial(x) = |x|$

$(\mathbb{K}, +, \cdot)$, $\mathbb{K}$ campo $\quad \partial(x) = 0$

$(\mathbb{K}[x], +, \cdot)$ con $\mathbb{K}$ campo e

$\partial(p(x)) = \deg p(x) \quad p(x) \neq \underline{0}$

↑

anello dei polinomi a coeff. in $\mathbb{K}$ nella incognita x

N.B $\deg \underline{0}$ non è definito, se volte possiamo dire $\deg \underline{0} = -1$ ma serve a poco.

Oss: Sia $\mathbb{K}$ un campo e $p(x) = p_0 + p_1 x + \dots + p_n x^n \in \mathbb{K}[x]$ un polinomio di grado n e $q(x) = \sum_{i=1}^{k} q_i x^i$ un polinomio di grado k.

Se $k > n \Rightarrow p(x) = q(x) \cdot 0 + p(x)$ ed il "resto" $p(x)$ ha grado $< k = \deg q(x)$.

Se $k = n \Rightarrow p(x) = \boxed{\frac{p_n}{q_n}} q(x) + \left[p(x) - \frac{p_n}{q_n} q(x) \right]$

$\deg < k$

Se $k < n$ si procede in modo iterativo

$$p_1(x) = p(x) - \frac{p_n}{q_k} q(x) \cdot x^{n-k}$$

$$p_2(x) = p_1(x) - \frac{p_{2(n-1)}}{q_k} q(x) \cdot x^{n-k-1}$$

$\vdots$

fino a che non otteniamo quoziente e resto con $\deg < k$

$(\mathbb{Z}[x], +, \cdot)$ non è un dominio euclideo!!

$x^2 - 1$ diviso $2x + 1$

in $(\mathbb{Q}[x], +, \cdot)$

$$\left(x^2 - 1\right) = \left(\frac{1}{2}x - \frac{1}{4}\right)(2x+1) + \frac{3}{4}$$

oss: possiamo definire MCD fra polinomi (o comunque fra elementi di un dominio euclideo).

> d è $MCD(a,b)$ se $d|a$, $d|b$ e $\forall c$ tale che $c|a$ e $c|b$ si ha $c|d$.

Esempio MCD in $\mathbb{R}[x]$ fra

$$(x^2-1) \text{ ed } (x-1)(x+3)$$

$(x-1)$ è un MCD. ma $\forall a \neq 0$ $a(x-1)$ è anche esso un MCD.

Se moltiplicate un MCD per un elemento invertibile $\Rightarrow$ ottenete ancora un MCD.

Dim $d|a$, $d|b$ & $\forall c$: $c|a$ & $c|b$, $c|d$

$d'|a$ $d'|b$ & $\forall c'$: $c'|a$ & $c'|b$, $c|d'$

$\Rightarrow d \mid d' \Rightarrow d' = d\alpha$ & $d' \mid d \Rightarrow d = d'\beta$

$\Rightarrow d = d\beta = d(\alpha\beta)$ e quindi deve essere $\alpha\beta = 1$

In $\mathbb{Z}$: $\alpha\beta = 1 \Rightarrow \alpha = \beta = \pm 1$

In $\mathbb{K}[x]$: $\alpha\beta = 1 \iff \alpha, \beta \neq 0$ & $\alpha, \beta \in \mathbb{K}$

con $\beta = \alpha^{-1}$

In particolare di MCD ce ne sono tanti quanti gli elementi di $\mathbb{K} \setminus \{0\}$.

D'altro canto di MCD in $\mathbb{K}[x]$ monici cioè in cui il coeff. del termine di grado massimo è $+1$ ne esiste esattamente 1 !!

$MCD(x^2-1, (x-1)(x+3)) = (x-1)$

N.B possiamo applicare l'algoritmo euclideo.

```
function my_xgcd(x,y)
    local U=[oneunit(x),zero(x),x]
    local V=[zero(y),oneunit(y),y]
    while V[3]!=zero(x)
        q=U[3]÷V[3]
    ||  U,V=V,U-V*q
    end
    U
end
```

implicito

diff prodotto divisione

ALGORITMO EUCLIDEO esteso

```
function my_gcd(x,y)
    x>y || return my_gcd(y,x)
    y==0 && return x
    my_gcd(y,mod(x,y))
end
```

ALGORITMO EUCLIDEO

$\partial(x) > \partial(y)$

$\partial(x) < \partial(b)$

Campi finiti: Campi con un numero finito di elementi

$\rightarrow \mathbb{Z}_p$ p primo.

Supponiamo che $\mathbb{K}$ sia un campo con $|\mathbb{K}| < \infty$ $\Rightarrow |\mathbb{K}| = p^n$ per qualche primo p.

$|\mathbb{K}| = a \cdot b$ con $MCD(a,b) = 1$, $a, b \neq 1$

allora $\underbrace{(1+1+\dots+1)}_{a \text{ volte}}$ $\underbrace{(1+\dots+1)}_{b \text{ volte}}$

e $a \cdot b = \underbrace{1+1 \dots +1}_{a \cdot b \text{ volte}} = 0$

e quindi né a né b sono invertibili perché $a \neq 0$, $b \neq 0$ $ab = 0$

$\mathbb{Z}_6$ $(1+1+1) = 3 \neq 0$ $(1+1) = 2 \neq 0$

$1+1+\dots+1 = 0$

$256 = 2^8$. Sia $\mathbb{K}[x]$ l'anello dei polinomi in x su $\mathbb{K}$ e sia $p(x) \in \mathbb{K}[x]$ un polinomio irriducibile di grado n su $\mathbb{K}$.

[polinomio irriducibile vuol dire che $q(x) \in \mathbb{K}(x)$ se $q(x) \mid p(x)$ $\Rightarrow$ $q(x) = a \in \mathbb{K}^*$ oppure $q(x) = a\,p(x)$ con $a \in \mathbb{K}^*$]

In particolare se $\deg(q(x)) < \deg(p(x)) \Rightarrow$ $q(x) \neq 0$

$$MCD(q(x), p(x)) = 1$$

Costruiamo $\dfrac{\mathbb{K}[x]}{p(x)\,\mathbb{K}[x]}$ quoziente $\left[\mathbb{Z}/p\mathbb{Z}\right]$

$p(x)\,\mathbb{K}[x] = \{ p(x)q(x) \mid q(x) \in \mathbb{K}[x] \}$ è un ideale

$$\frac{\mathbb{K}[x]}{p(x)\,\mathbb{K}[x]} = \frac{\mathbb{K}[x]}{(p(x))}$$ è un anello commutativo con unità.

$a(x) + (p(x)) \in \dfrac{\mathbb{K}[x]}{(p(x))}$ e osserviamo che

1) $a(x) + (p(x)) = (a(x) \bmod p(x)) + (p(x))$.

perché se $a(x) = q(x)p(x) + r(x)$

$b(x) = q'(x)p(x) + r'(x)$

$\Rightarrow a(x) - b(x) = (q(x) - q'(x))\,p(x) \in (p(x))$

$\Rightarrow a(x) \in b(x) + (p(x))$

In particolare ogni classe contiene un polinomio di grado minimo e le classi corrispondono ai resti della divisione per $p(x)$.

$\rightarrow \dfrac{\mathbb{K}[x]}{(p(x))} \cong$ come spazio vettoriale $\{ r(x) \mid \deg r(x) < \deg p(x) \} \cong$

$\cong \mathbb{K}^n$ come spazio vettoriale.

$$\left[\ |\mathbb{K}^n| = |\mathbb{K}|^n\ \right]$$

Mostriamo che ogni $a(x) + (p(x))$ è invertibile. $\quad a(x) \neq 0$

infatti dalla sua classe consideriamo l'equazione $a(x)\,b(x) + p(x)k(x) = 1$

essa è risolubile perché $MCD(a(x), p(x)) = 1$

e si può applicare l'alg. euclideo esteso.

$$[a(x) + (p(x))][b(x) + (p(x))] =$$

$$= [a(x)b(x) + (p(x))] =$$

$$= [1 - k(x)p(x) + (p(x))] = 1 + (p(x))$$ □

Quindi ogni elemento non nullo di $\dfrac{\mathbb{K}[x]}{(p(x))}$ è invertibile.

$\Rightarrow \dfrac{\mathbb{K}[x]}{(p(x))}$ è un campo!

Esempio $\mathbb{K} = \mathbb{R} \qquad p(x) = (x^2 + 1)$

$$\frac{\mathbb{R}[x]}{(x^2+1)} = \{a+bx \mid a,b \in \mathbb{R}\}$$

$$(a+bx)\cdot(c+dx) = ac + (bc+ad)x + bdx^2 \mod x^2+1$$

$$= (ac-bd) + (bc+ad)x$$

$x = i$

In generale non è detto che dato $\mathbb{K}$ campo e $n \geq 2$

$\exists\, p(x) \in \mathbb{K}[x]$ con $\deg p(x) = n$ e $p(x)$ irriducibile

[Se $\mathbb{K} = \mathbb{Z}_p \Rightarrow$ esistono $\forall n \geq 1$ polinomi irriducibili di grado n a coeff. in $\mathbb{K}$

[In particolare poniamo

$$\mathbb{F}_{p^n} := \frac{\mathbb{Z}_p[x]}{(u(x))} \quad \text{con } u(x) \in \mathbb{Z}_p[x]$$

irriducibile in $\mathbb{Z}_p[x]$ e di grado n.]

→ 1) $\mathbb{F}_{p^n}$ è un campo finito di ordine p^n

→ 2) $\mathbb{F}_{p^n}$ ha su $\mathbb{F}_p = \mathbb{Z}_p$ la struttura di uno spazio vettoriale $\mathbb{F}_p^n$ di dimensione n

In particolare su $\mathbb{Z}_2^8$ possiamo definire una struttura di campo finito con 256 elementi identificandolo

con $\mathbb{F}_{256} = \frac{\mathbb{Z}_2[x]}{(u(x))}$ con $u(x)$ irriducibile in $\mathbb{Z}_2$

di grado 8.

La somma di $\mathbb{F}_{256}$ coincide con la somma di $\mathbb{Z}_2^8$ ed è lo XOR.