(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

Consider: $G = \{ P(x) \text{ of degree} \leq 7 \}$

$G = \{ (a_0 + a_1 x + a_2 x^2 + \dots + a_7 x^7) \}$

where coefficients $\in GF(2)$

$a_0, a_1, \dots a_7 \in \{0, 1\}$

Representation:

1 byte

$* \Rightarrow \quad a(x) * b(x)$

$= \quad a(x) + b(x) \mod 2$ (for each coeff)

$P_1(x) = x + 1$

$P_2(x) = x^2 + x$ $\Rightarrow$ $P_1(x) + P_2(x) = x^2 + 1$

Notice that this creates a group.

$\rightarrow$ Abelian group

What if we wanted multiplication of polynomials?

$P_1(x) \cdot P_2(x) \mod$ (degree 8 poly. $p(x)$) (terms mod 2)

$(x^8 + \dots -)$

irreducible polynomial

Consider Z_p^*

$Z_n = \{0, 1, 2, \dots (n-1)\}$

$\{0\}$

$* =$ multip. mod n

Is it a group? —— if n is prime then already proved

what if n is composite.

$\mathbb{Z}_6 - \{0\} = \{1, 2, 3, 4, 5\} \mod 6$

$2 * 3 = 0 \rightarrow$ Not closed

$$\mathbb{Z}_n^* = \{ x : 1 \leq x < n \text{ s.t } \gcd(x, n) = 1 \}$$

$\mathbb{Z}_6^* = \{1, 5\}, * \mod 6$

$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$

$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

$7^{-1} = 3$

$3^{-1} = 7$

AES polynomial:

11 B

0001 0001 1011

1 1 B

$= (x^8 + x^4 + x^3 + x + 1)$

Coeff' are mod (2) $\equiv$ Coeff are in GF(2)

Galois field.

Field: $(G, +, \cdot)$

(i) $(G, +)$ is an Abelian group with identity as $\overline{0}$

(ii) $(G - \{0\}, \cdot)$ is an Abelian group

(iii) Distributive operation

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$\forall\ a, b, c \in G$$

GF(2)

$\{0, 1\}$ + mod 2
× mod 2

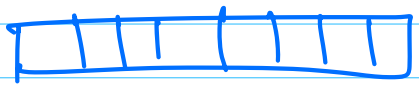
⊕ AND

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Rijndael finite field / AES f.f.

Contains = 2^8 elements



← 8 bits → 0 or 1

+ ≡ usual addition of polynomials with coeff ∈ GF(2)

① Every finite field of same size is isomorphic to each other

② The no. of elements in a finite field are p^n for some prime p & some int n.

Most common finite fields in Crypto are

$GF(2^n)$

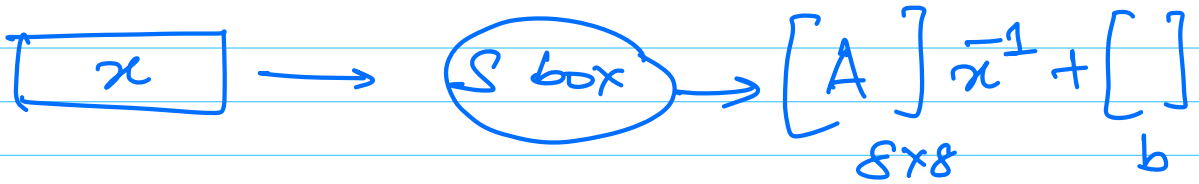
AES finite field = $GF(2^8)$

Polynomial of degree ≤ 7 with coeff ∈ GF(2)

mod 11B

S-box in AES.

8 bit → 8 bit



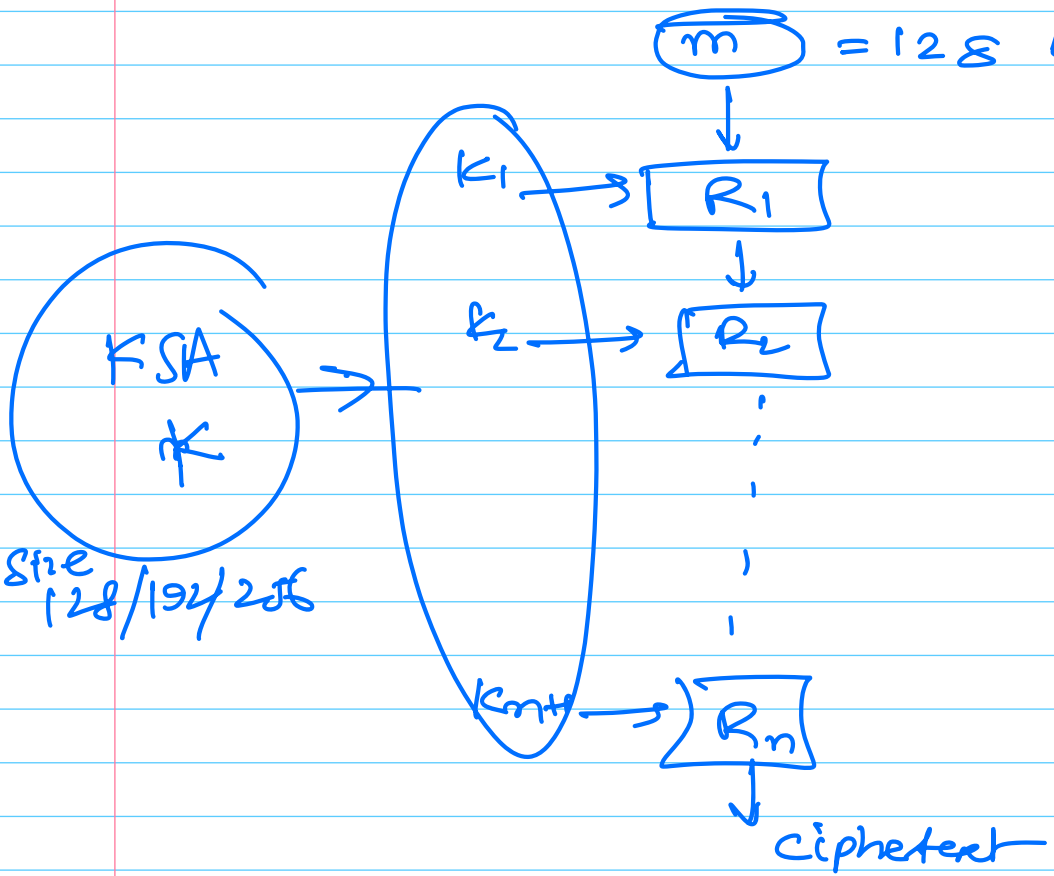
Where we take $\vec{0}$ as

AES : Iterated block cipher

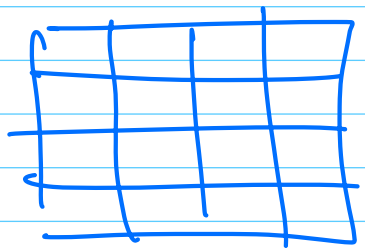
AES-128 : 10 rounds

AES-192 : 12 rounds

AES-256 : 14 rounds



Each round has 4 operations, which are implemented on a state array of 128 bits

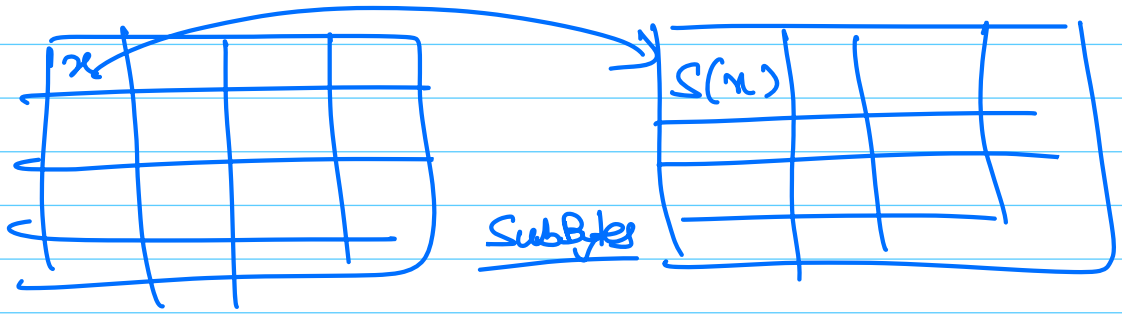
State 

4x4 matrix of bytes

16x8 = 128 bits

Round function: Round i

1. SubBytes(S)
2. ShiftRows(S)
3. MixColumns(S)
4. ~~Add~~ Round Keys(S, Ki)



$$S(x) = Ax^{-1} + b$$

some const.

Precomputed S Box size:

2^8 inputs x 1 byte each = 256 bytes