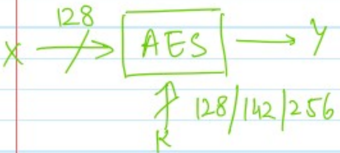
AES

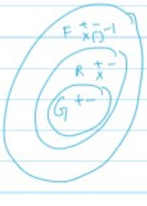
Thursday, 28 November 2019 1:58 PM

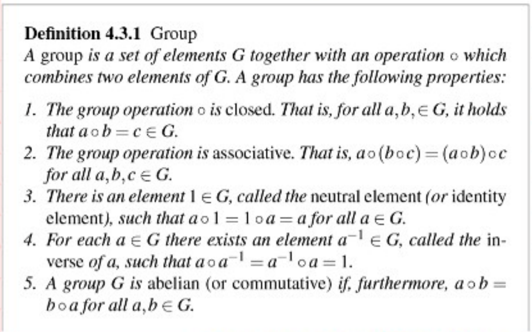


Drawback: All internal operations of AES are based on FINITE FIELDS

INTRODUCTION TO FINITE FIELDS / GALOIS FIELD

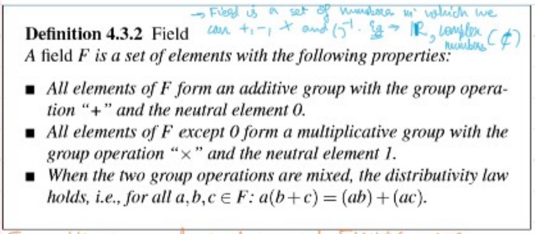
3 basic algebraic groups:





Definition 4.3.1 Group
A group is a set of elements G together with an operation ∘ which combines two elements of G. A group has the following properties:

1. *The group operation ∘ is* closed. *That is, for all $a,b,\in G$, it holds that $a \circ b = c \in G$.*
2. *The group operation is* associative. *That is, $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a,b,c \in G$.*
3. *There is an element $1 \in G$, called the* neutral element *(or* identity element*), such that $a \circ 1 = 1 \circ a = a$ for all $a \in G$.*
4. *For each $a \in G$ there exists an element $a^{-1} \in G$, called the* inverse *of a, such that $a \circ a^{-1} = a^{-1} \circ a = 1$.*
5. *A group G is* abelian (or commutative) *if, furthermore, $a \circ b = b \circ a$ for all $a,b \in G$.*



→ Field is a set of numbers in which we can +, −, × and ()$^{-1}$. Eg → $\mathbb{R}$, complex numbers ($\mathbb{C}$)

Definition 4.3.2 Field
A field F is a set of elements with the following properties:

- *All elements of F form an additive group with the group operation "+" and the neutral element 0.*
- *All elements of F except 0 form a multiplicative group with the group operation "×" and the neutral element 1.*
- *When the two group operations are mixed, the distributivity law holds, i.e., for all $a,b,c \in F$: $a(b+c) = (ab) + (ac)$.*

In cryptography, we almost always need FINITE SETS

Finite Field only exist if they have p^m elements (p → prime, m → integer)

Ex:

(a) There is a F.F. with 11 elements : GF(11)
(b) " " " " " 81 elements : GF(81) / GF(3^4)
(c) " " " " " 256 elements : GF(256) / GF(2^8) → AES FIELD / GALOIS FIELD
(d) There is NO FF with 12 elements : ✗

Types of FF:

GF(p^m)
m=1 → GF(p) (prime fields)
m>1 → GF(p^m) (extension fields) } cryptographers especially interested in fields of form GF(2^m)

PRIME FIELDS: ARITHMETIC

The elements of a prime field GF(p) are the integers in the set {0, 1, ……, p−1}

(a) Add, substract, multiply:

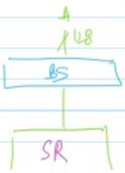
Let $a, b \in GF(p) = \{0, 1, \ldots, p-1\}$

$a+b \equiv c \mod p$
$a-b \equiv d \mod p$
$a \cdot b \equiv e \mod p$

} note all conditions of Fields are SATISFIED.

(b) Inversion

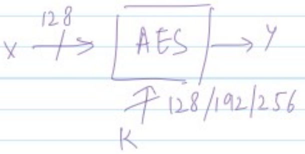
$a \in GF(p)$, then the inversion a^{-1} must satisfy $a \cdot a^{-1} \equiv 1 \mod p$



THE AES

1997 → DES was failing. Call for AES by NIST
↓
by 1998 → 15 algorithmic submission
↓
by 1999 → 5 Finalist algorithms are selected.
Oct 2, 2000 → RIJNDAEL was selected as the AES

designers → JOAN DAEMON and VINCENT RIJMEN



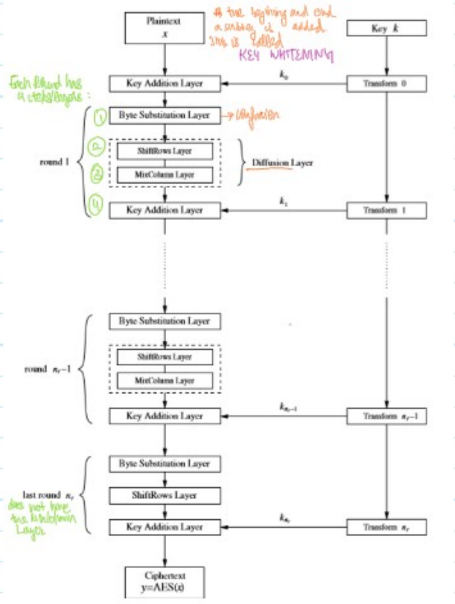
number of Rounds depends on the key length.

K	# rounds
128	10
192	12
256	14

Remarks: (1) AES is the most important SYMMETRIC ALGORITHM in the world
(2) NSA allows AES for classified upto TOP SECRET with 192 and 256 bit key.

STRUCTURE of AES:

→ AES is not a FIESTAL CIPHER.
→ AES encrypts all 128 bits of the data path in 1 round.



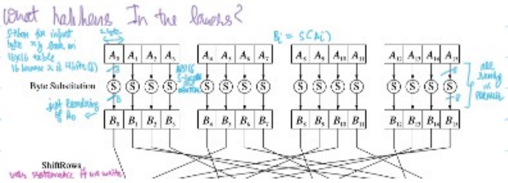
At the beginning and end a subkey is added. This is called KEY WHITENING

Each Round has 4 steps/layers:

→ Confusion

last round n_r does not have the MixColumn Layer

→ What happens In the layers?


A_0 A_1 A_2 A_3 A_4 A_5 A_6 A_7 A_8 A_9 A_{10} A_{11} A_{12} A_{13} A_{14} A_{15}
Byte Substitution
S
B_0 B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8 B_9 B_{10} B_{11} B_{12} B_{13} B_{14} B_{15}
ShiftRows
1 byte
8
8

S-box for input byte xy look in 16x16 table 16 because x is 4 bits

$B_i = S(A_i)$

just Rendering of A_0

AES 16 S-boxes

are [illegible] in parallel

very systematic if we write

(b) Inversion

$a \in GF(p)$, then the inversion a^{-1} must satisfy $a \cdot a^{-1} \equiv 1 \bmod p$

is computed using Extended Euclid Algorithm.

EXTENSION FIELD ARITHMETIC:

(a) Element representation:

The elements of $GF(2^m)$ [in this course ∴ $p=2$] are polynomials

$$a_{m+n}x^{m-1} + \cdots + a_n x + a_0 = A(x) \in GF(2^m)$$

$$a_i \in GF(2) = \{0,1\}$$

example:

$$GF(2^3) = GF(8)$$

$$A(x) = a_2x^2 + a_1x + a_0 = (a_2, a_1, a_0)$$

$$GF(2^3) = \underbrace{\{\overset{000}{0}, \overset{001}{1}, \overset{010}{x}, \overset{011}{x+1}, \overset{100}{x^2}, \overset{101}{x^2+1}, \overset{110}{x^2+x}, \overset{111}{x^2+x+1}\}}_{8\text{ elements}}$$

Q→ how to compute with these elements?

(b) Addition and subtraction in $GF(2^m)$:

use regular polynomial addition and subtraction, where coefficients are computed in $GF(2)$

eg: $GF(2^3)$

$$A(x) = x^2 + x + 1$$
$$B(x) = x^2 + 1$$
$$A+B = (1+1)x^2 + x + (1+1)$$
$$= 0x^2 + x + 0$$
$$= x$$

note Add and Sub in $GF(2^m)$ are the same operations

(c) Multiplication in $GF(2^m)$

Intuition → just do regular polynomial multiplication

eg $GF(2^3)$

$$A \cdot B = (x^2+x+1)(x^2+1)$$
$$= x^4 + x^2 + x^3 + x + x^2 + 1$$
$$= x^4 + x^3 + (1+1)x^2 + x + 1$$
$$= x^4 + x^3 + x + 1 \quad (= c'(x))$$

but it's NOT in $GF(2^3)$

solution: Reduce $c'(x)$ modulo a polynomial that "behaves like a prime"

These are called IRREDUCIBLE POLYNOMIALS

for $GF(2^3)$ is $P(x) = x^3 + x + 1$

eg:

$$c'(x) \text{ was } \overbrace{(x^4+x^3+x+1)}^{A \times B} \times \underbrace{(x^3+x+1)}_{P(x)} = x + 1$$

$$\begin{array}{r} x^4+x^3+x+1 \\ +\;x^4 \qquad\; x^2+x \\ \hline x^3+x^2+1 \\ +\;x^3 \qquad\; +x+1 \\ \hline \end{array}$$

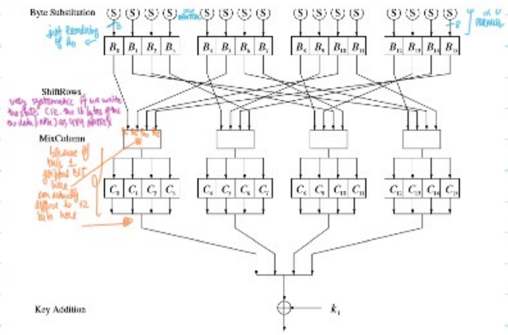
$$\boxed{x^2+x} \rightarrow A \cdot B \bmod P(x)$$

for every field $GF(2^m)$ there are several irreducible polynomials

eg: $P(x) = x + x + 1$

The "AES IRREDUCIBLE POLYNOMIAL"

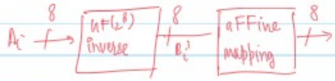
is $P(x) = x^8 + x^4 + x^3 + x + 1$


Byte Substitution
just rendering of A0
8
in parallel
ShiftRows
very systematic if we write the state (i.e. the 16 bytes of the data path) as 4x4 MATRIX
MixColumn
because of this 1 flipped bit here can actually diffuse to 32 bits here
Key Addition
k_i

All operations in AES are BYTE ORIENTED as opposed to DES which was BIT ORIENTED

The 128 bit Data Path is split into 16 BYTES

how IS THE S-BOX TABLE CONSTRUCTED?



consider $A_i \in GF(2^8)$ and compute its inverse

example → $A_i = 1100\ 0010$

$$A_i(x) = x^7 + x^6 + x$$
$$B_i'(x) = A_i^{-1}(x)$$
$$= x^5 + x^3 + x^2 + x + 1$$
$$= 0010\ 1111$$

check: $(x^7+x^6+x)\cdot(x^5+x^3+x^2+x+1) = 1 \bmod \underbrace{(x^8+x^4+x^3+x+1)}_{\text{AES IRREDUCIBLE POLYNOMIAL}}$

AFFINE MAPPING

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} \equiv \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \bmod 2.$$

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

B_0	B_4	B_8	B_{12}	no shift
B_5	B_9	B_{13}	B_1	⟵ one position left shift
B_{10}	B_{14}	B_2	B_6	⟵ two positions left shift
B_{15}	B_3	B_7	B_{11}	⟵ three positions left shift

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02&03&01&01 \\ 01&02&03&01 \\ 01&01&02&03 \\ 03&01&01&02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}.$$

all B_i, C_i constants are Bytes.

$$C_0 = \underbrace{\underbrace{02 \cdot B_0}_{GF(2^8) \times GF(2^8)} + 03 \cdot B_5}_{GF(2^8) + GF(2^8)} + 01 \cdot B_{10} + 01 \cdot B_{15}$$

01 = 0000 0001 → 1

02 = 0000 0010 → x

03 = 0000 0011 → $x+1$

1 bit change in B0 gets dispersed to the whole 1st column ⇒ changes diffused to C_0, C_1, C_2, C_3 ⇒ 4×8 ⇒ changes dispersed in 32 bits.

~~eg~~: $P(x) = \quad x \quad + x + 1$

The "AES IRREDUCIBLE POLYNOMIAL"
is $P(x) = x^8 + x^4 + x^3 + x + 1$

(d) Inversion in $GF(2^m)$

Aaain, the inverse $A^{-1}(x)$ of an element $A(x) \in hF(2^m)$ must satisfy

$$A(x) \times A^{-1}(x) \equiv 1 \bmod P(x)$$

↳ to find this we need extended Euclidean Algorithm