[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2022-2023
Scribed by : Pallikonda Sai Teja — Lecture (Week 05)
Student ID : 202011052

1 Group

• Group → (G,$*$) — $\boxed{\text{G is closed under } *}$
$\alpha \in$ G
$\alpha^0, \alpha^1, \alpha^2, ... \in$ G
$\alpha^0 \rightarrow$ identity
for a b $\in$ G
$\exists$ i $\geq$ such that b = $\alpha^i \Rightarrow$ G $\subseteq < \alpha >$
then α is called the generator of (G, $*$)
• (G, $*$) = $< \alpha >$
• A Group G is cyclic if there is an element $\alpha \in$ G, such that for every b $\in$ G there is an integer i with b = α^i
This α is called the generator of G.

$$G =< \alpha >$$

• (G, $*$) — $|G|$: finite
a $\in$ G o(a) = m, a^m = e
e = $a^0, a^1, a^2, .., a^{m-1} in$ G
H = $\{a^0, a^1, a^2, .., a^{m-1}\}$

1. H $\subseteq$ G
2. H is a group under $*$
   if x, y $\in$ H
   $\Rightarrow$ x $*$ y $\in$ H

for every $a^i \in$ H $\exists$ the inverse of a^i
H is a group with $*$.
H is a sub group of G.

$$H =< a >$$

H is a cyclic sub group of G.
$|H| = | < a > | \rightarrow$ order of cyclic subgroup = O(a)

2 Lagrange Theorem

If G is a finite group.
H is a sub group of G then $|H|$ divides $|G|$. — $\boxed{|S| \text{ is cardinality of set S}}$

• G is a finite group
a $\in$ G

O(a) divides $|G|$.
$rightarrow$ a $\in$ G
H = {e=$a^0, a^1, a^2, .., a^{O(a)-1}$}
H is a sub group of G.

• If the order of a $\in$ G is t then

$$O(a) = \frac{t}{gcd(t, k)}$$

If gcd(t, k) = 1
then O(a^k) = t = O(a)
$\Rightarrow$ | $< a^k >$ | = | <a> |
x $\in$ $< a^k >$
$\Rightarrow$ x = $(a^k)^i$ = a^{ki} $\in$ <a>
$< a^k >$ $\subseteq$ <a>
$< a^k >$ = <a> (Since | $< a^k >$ | = | <a> |)
a^k is also a generator of $< a >$

• $Z^*{}_{19}$ = { x | gcd(x, 19) = 1, 1 $\leq$ x $\leq$ 18 }
$*_{19}$: multiplication modulo 19.

Find the generator of ($Z^*{}_{19}$, $*_{19}$)
$< 2 >$ ={1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10} = $Z^*{}_{19}$
$< 2^5 > = < 13 >$ is also a generator of $Z^*{}_{19}$

3 Ring

A ring (R, $+_{\mathrm{R}}$, $*_{\mathrm{R}}$) consists of one set R with two binary operations arbitrarily denoted by $+_{\mathrm{R}}$ (addition) and $*_{\mathrm{R}}$ (multiplication) on R satisfing the following properties.

1. (R, $+_{\mathrm{R}}$) is a abelian group with the identity element 0_{R}.
2. The operation $*_{\mathrm{R}}$) is associate i.e.,

$$a *_{\mathrm{R}} (b *_{\mathrm{R}} c) = (a *_{\mathrm{R}} b) *_{\mathrm{R}} c \ \ \forall \ a, b, c \in R$$

3. There is a multiplication identity denooted by 1_{R} with $1_{\mathrm{R}} \neq)_{\mathrm{R}}$ such that

$$1_{\mathrm{R}} *_{\mathrm{R}} a = a *_{\mathrm{R}} 1_{\mathrm{R}} = a \ \ \forall \ a \in R$$

4. The operation $*_{\mathrm{R}}$ is distributive over $+_{\mathrm{R}}$ i.e.,

$$(b +_{\mathrm{R}} c) *_{\mathrm{R}} a = (b *_{\mathrm{R}} a) +_{\mathrm{R}} (c *_{\mathrm{R}} a)$$

$$a *_{\mathrm{R}} (b +_{\mathrm{R}} c) = (a *_{\mathrm{R}} b) +_{\mathrm{R}} (a *_{\mathrm{R}} c)$$

Example : (Z, +, .) $\rightarrow$ Ring
$\Rightarrow$ a.b = b.a $\forall$ a, b $\in$ Z commutative ring
An element 'a' of a ring R is called unit or an invertable elements if there is an element b $\in$ R such that a $*_{\mathrm{R}}$b = 1_{R}
• The set of units in a Ring R forms a group under multiplication operation.
$\Rightarrow$ This is known as group of units of R.

4 Field

A field is a non-empty set F together with two binary operations +(addition) and $*$(multiplication) for which the following properties are satisfied.

1. (F, +) is an abelian group.
2. If 0_F denotes the additive identity element of (F,+) then (F $\setminus$ $\{0_F\}$, $*$) is a commutative abelian group.
3. $\forall$ a, b, c $\in$ F we have
$$a * (b + c) = (a * b) + (a * c)$$

Example: $(Z_P, +_P, *_P) \rightarrow$ Field ? P$\rightarrow$ Prime

1. Z_P = {0,1,2,...,P-1}
2. It is a group under first operation.
3. 0 is the identity, if x $\in Z_P$ then $\exists$ P-x such that x $+_P$ (P-x) = 0.
4. The operation is commutative.
5. $(\{Z_{P\text{ - }0}\}, *)$ is a commutative group.
6. $\exists$ multiplicative identity is "1".
7. x $\in$ {Z_P-0} $\exists$ y $\in$ {Z_P-0} such that x $*_P$ y = 1, because (x, p) = 1.
8. It is a abelian group.
$$x * ymodp = y * xmodp.$$
9. It is distributive
$$a *_P (b +_p c = (a *_p b) +_p (a *_p c)$$
$$(Z_P, +_P, *_P) \rightarrow Field$$

5 Field Extension

Suppose k_2 is a field with addition (+) and multiplication (*). Suppose $k_1 \subseteq k_2$ is closed under both these operations such that k_1 itself is a field with the restriction of + and * the set k_1.

• F $\rightarrow$ field (F, +, $*$)
F(x) = {a_0 + a_1x + ...| $a_i \in$ F} (F(x), +, $*$) $\rightarrow$ Polynomial Ring
+ $\rightarrow$ Polynomial addition
$*$ $\rightarrow$ Polynomial multiplication
$P_1(x) \in F(x)$, $P_1(x) = a_0 + a_1x + a_2x^2$
$P_2(x) \in F(x)$, $P_2(x) = b_0 + b_1x + b_2x^2$
$P_1(x) + P_2(x) = (a_0 + a_1x + a_2x^2) + (b_0 + b_1x + b_2x^2)$
$P_1(x) + P_2(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2$
$(a_i + b_i) \rightarrow$ Field addition.
additive operation on F as $(a_i, b_i) \in F$.
$\rightarrow (a_0 + a_1x + a_2x^2 + .. + a_{n-1}x^{n-1}) * (b_0 + b_1x + b_2x^2 + .. + b_{n-1}x^{n-1})$

$= a_0b_0 + (a_0b_1 + a_1b_0)x + ... + (a_{n-1}b_{n-1})x^{2n-2}$
$a_i * b_i \rightarrow$ Field multiplication in F as a_i, $b_i \in F$.
addition between the elements has to be done in the field.

- (F[x], +, $*$) is a polynomial ring.

1. (F[x], +) must be a abelian group.

$$\begin{array}{l} \quad a_0 + a_1x + a_2x^2 \\ + \; b_0 + b_1x + b_2x^2 \\ \hline (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 = 0 \end{array} \qquad \begin{array}{r} a_i \in F \\ a_i + b_i = 0 \end{array}$$

2. $*$ is associative.
3. 1 is the multiplicative identity.
4. $*$ is distributive over +.

- $F_2 = \{0,1\}$ $\quad (F_2, +_2, *_2) \rightarrow$ Field

$F_2[x] = \{a_0 + a_1x + a_2x^2 + ... \mid a_i \in F_2\}$
$p(x) = x + 1 \in F_2[x]$
$q(x) = x^2+x+1 \in F_2[x]$
$p(x) + q(x) = (x + 1) + (x^2 + x + 1) = x^2 + (1+1)x + (1+1) = x^2$ $p(x) * q(x) = (x+1)*(x^2+x+1)$
$= (x^3 + x^2 + x) + (x^2+x+1) = x^3 + (1+1)x^2 + (1+1)x + 1 = x^3 + 1$.

- A polynomial P(x) $\in$ F(x) of degree n (n >= 1) is called irreducible if it cannot be written in the form of $P_1(x) * P_2(x)$ with $P_1(x)$, $P_2(x) \in F[x]$ and degree of $P_1(x)$, $P_2(x)$ must be >= 1.

$$P(x) \neq P_1(x) * P_2(x)$$

.

- $x^2 + 1 \in F(x)$

$(x+1)*(x+1) = x^2+(1+1)x+1 = x^2 + 1$.
$(x^2 + 1) = (x+1)*(x+1)$ in $F_2[x]$
$x^2 + 1$ is reducable in $F_2[x]$

- $I = < P(x) > = \{Q(x).P(x) \mid Q(x) \in F(x)\}$

I $\rightarrow$ ideal generated by P(x).

- $f[x] \,/ < P(x) > = \{g(x) \% P(x) \mid g(x) \in F(x)\}$

$Q(x) \in F[1]$
$Q(x) = d(x) * P(x) * r(x)$
$r(x) \in F[x]/< P(x) >$
if P(x) is irreducable polynomial then
  $(F[x]/< P(x) >, +, *)$ becomes field.
Example : $x^2 + x + 1 \in F_2[x]$, $F_2 = \{0, 1\}$
$P(x) = x^2 + x + 1$ is irreducible

- $F_2[x]/< x^2 + x + 1 >$

$q(x) = d(x).p(x) + r(x)$
$\deg(r(x)) < 2$
$r(x) = \{0, 1, x, x+1\}$

- $x^2+x+1 \ ) \ x^2+1 \ (\ 1$

$$\begin{array}{l} x^2+x+1 \\ \hline x \end{array}$$

- x^3+1
$= x.x^2+1$
$= x(x+1)+1$
$= x^2+x+1$
$= x+1+x+1$
$= 0$

- F_2[x] / $< x^2+x+1 >$
$x^2+x+1 = 0$
α is the root of $x^2+x+1 = 0$
$\alpha^2+\alpha+1 = 0$
$\Rightarrow \alpha^2 = \alpha+1$
$< \alpha > = \{0,\ 1{=}\alpha^0,\ \alpha^1,\ \alpha^2 = \alpha+1\} \Rightarrow \mathrm{O}(\alpha) = 2$
$\Rightarrow \{0,\ 1,\ \alpha,\ \alpha+1\}$
x^2+x+1 is a primitive polynomial.

Example : F_2[x] / $< x^3+x+1 >$
$=\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$
$\alpha^3+\alpha+1 = 0$
$\alpha^3 = \alpha+1$
$\{0, \alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1, 1\}$
x^3+x+1 is a primitive polynomial.
$x^2 * (x^2+x+1) = x^4+x^3+x^2$
$= x(x+1)+(x+1)+x^2$
$= x^2+x+x+1+x^2$
$= 1$

6 Advanced Encryption Standard (AES)

It is standardized by NISP.
$\Rightarrow$ Rijndael
winner of Advanced Encryption Standard competition.
$\Rightarrow$ Winner of competition was named as AES.
AES $\rightarrow$ i) It is iterated block cipher
ii) It is based on SPN

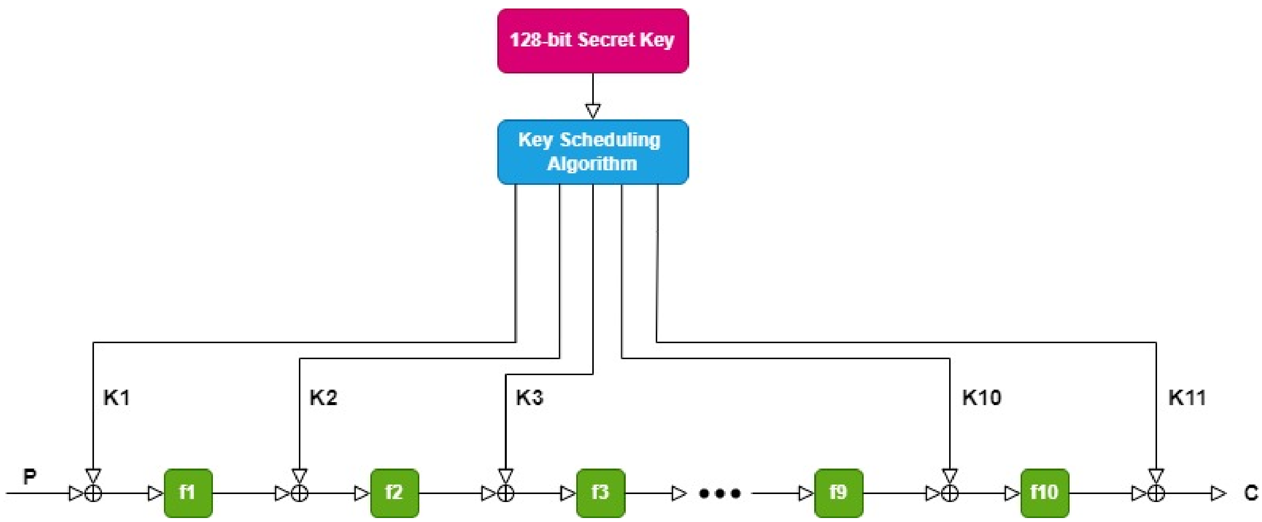
AES-128
i) Block size = 128 bit.
ii) Number fo rounds = 10.
iii) Secret key size = 128 bit.

AES-192
i) Block size = 128 bit.
ii) Number of rounds = 12.

iii) Secret key size = 192 bit.

AES-256
i) Block size = 128 bit.
ii) Number of rounds = 14.
iii) Secret key size = 256 bit.

- **AES-128**



THE END