[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2023-2024
Scribed by: Priyansh Vaishnav (202151120) — Lecture 6 & 7 (Week 4)

LECTURE 6 — Date: - 6th Feb 2024

Subgroup:

H is called a proper subgroup of $(G, *)$ if:
$(i) H \subseteq$ G
$(ii) H$ is itself a group with $*$ operation

1. If $(G, *)$ is a group, then $a^i = \underbrace{a * a * a * \ldots * a}_{i \text{ times}} \in G$

Cyclic Group:

A group G is cyclic if it has an element $\alpha \in$ G such that all the elements in G can be represent as power of α. Then α is called as generator of G.
Or we can say that there is an element $b \in G$ with integer i such that $b = \alpha^i$.

Order of an element:

$O(a)$ is the order of element a, such that $a^m = \varepsilon$ where ε is the identity element of G and m is the least positive integer.

Example:

$(\mathbb{Z}_5, *_5)$ is the group, and the basic operation $*_5$ is defined as $x *_5 y = (x \cdot y) \mod 5$. Then, $O(4) = 2$.

1. Cyclic subgroup is denoted as $< a >$.

2. $| < a > |$ is denoted as size of the subgroup.

Lagrange's Theorem:

- If G is a finite group and H is a subgroup of G, then the order (number of elements) of H divides the order of G. Mathematically, if $|G|$ is the order of G and $|H|$ is the order of H, then $|G|/|H|$ is an integer.

$$a \in G \text{ and order is } O(a)$$
$$S = \{\varepsilon, a, a^2, a^3, \ldots, a^{O(a)-1}\}$$
$$(S, *) \text{ is a subgroup of } (G, *)$$
$$|S| \mid |G|$$
$$O(a) \mid |G|$$

- If the order of $a \in G$ is t then order of a^k will be $\frac{t}{\gcd(t,k)}$

Ring:

- We have one set and two binary operations denoted as $(R, +_R, \times_R)$ where $+_R$ is addition (non-standard) and $\times_R$ is multiplication (non-standard).
- Properties of R:
  1. $(R, +_R)$ is an abelian group with the identity element O_R.
  2. The operation $\times_R$ is associative.
  3. There is a multiplication identity denoted by 1_R with $1_R \neq 0_R$.
  4. $\times_R$ is distributive over $+_R$.
- Distributive property:

$$(B +_R C) \times_R A = (B \times_R A) +_R (C \times_R A).$$

- **Example:** $(\mathbb{Z}, +, \cdot)$ forms a ring.
- $(R, +_R, \times_R)$ is abelian ring if the second operation $(\times_R)$ is abelian.
- An element a of a ring R is called **Unit** or an invertible element if these is an element $b \in R$ such that $a \times_R b = 1_R$.
- Set of unit is a ring R forms a group under multiplication this is known as group of unit of R.

Field:

A non-empty set F together with two binary operations $+_F$ and $\times_F$ with the following properties.
Properties:

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

Example:

$\mathbb{F} = \{0, 1, 2, \ldots, P-1\}$, where P is a prime number. Then,
$(\mathbb{F}_P, +_P, \times_P)$ is a field.
$+_P : (x + y) \mod P$
$\times_P : (x \cdot y) \mod P$

Field Extension:

- Suppose K_2 is a field with operations $+$ and $*$.
- Suppose $K_1 \subseteq K_2$ is closed under both operations such that K_1 itself is a field with operations $+$ and $*$.
- K_1 is a subfield of K_2.
- K_2 is a field extension of K_1.

1. $F(x) = \{a_0 + a_1x + a_2x^2 + \ldots + a_nx^{n-1}\}$ where $a_i \in F$

1. $\{F(x), +, *\} = a_0 + a_1x + a_2x^2 + \ldots + a_nx^{n-1} + b_0 + b_1x + b_2x^2 + \ldots + b_nx^{n-1}$
   $= (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^{n-1}$ where $a_i + b_i$ represent the additive operation in the field F.
2. $(a_0 + a_1x + a_2x^2 + \ldots + a_nx^{n-1}) * (b_0 + b_1x + b_2x^2 + \ldots + b_nx^{n-1})$
   $= (a_0b_0) + (a_0b_1 + a_1b_0) + \ldots + (a_{n-1}b_{n-1})x^{2n-2}$

Irreducible Polynomial

A polynomial $p(x) \in F[x]$ of degree $n \geq 1$ is called *irreducible* if it cannot be expressed in the form $p_1(x) \cdot p_2(x)$, where $p_1(x)$ and $p_2(x)$ are polynomials in $F[x]$, and the degrees of $p_1(x)$ and $p_2(x)$ are both greater than or equal to 1.

1. $I = \langle P(x) \rangle = \{q(x) \cdot p(x) \mid q(x) \in F(x)\}$ where $(F(x), +, \cdot)$ is a Polynomial Ring. This I is called as Ideal Ring.
2. The set of $F(x)$ modulo $P(x)$, denoted as $F(x)/\langle P(x) \rangle$ (where $P(x)$ is an irreducible polynomial), is called a field under the operations $+$ and $\cdot$ defined modulo $P(x)$. Here, $q(x)$ can be any polynomial in $F(x)$, and it can be expressed as $q(x) = d(x) \cdot P(x) + r(x)$, where $d(x)$ is the quotient and $r(x)$ is the remainder.

Advanced Encryption Standard (AES):

AES is an iterated block cipher that uses a substitution-permutation network (SPN) structure. It operates on fixed-size blocks of data and supports key sizes of 128, 192, or 256 bits.

AES-128:

- Block Size: 128 bits
- Number of Rounds: 10
- Secret Key Size: 128 bits

AES-192:

- Block Size: 128 bits
- Number of Rounds: 12
- Secret Key Size: 192 bits

AES-256:

- Block Size: 128 bits
- Number of Rounds: 14
- Secret Key Size: 256 bits

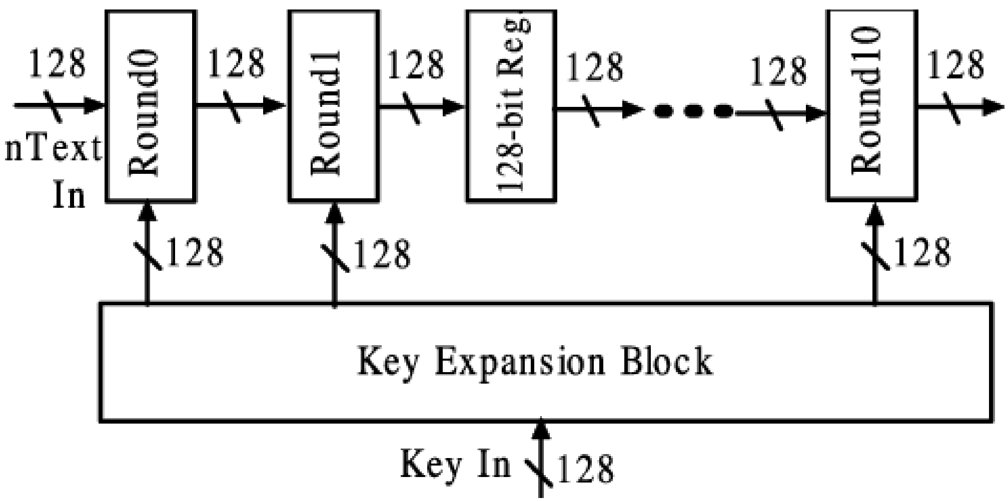

Figure 1: AES-128
Image Source: Research Gate