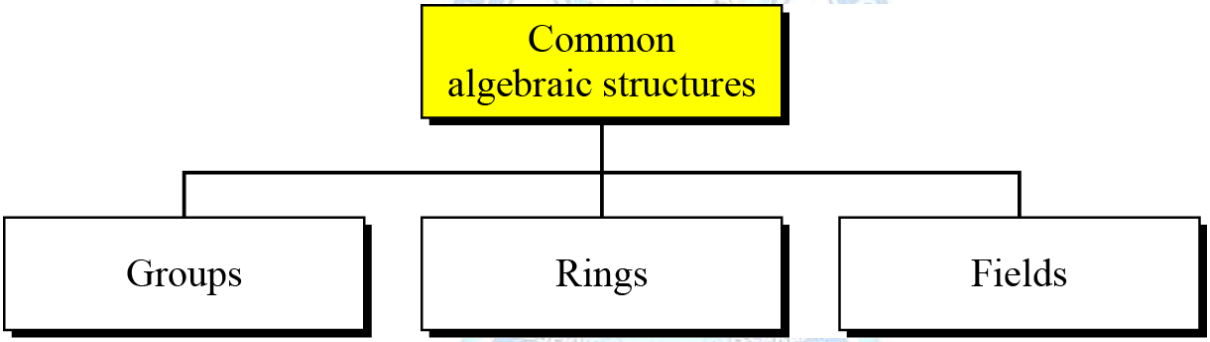
MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY:

Algebraic structures

Cryptography requires sets of integers and specific operations that are defined for those sets. The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure. Three common algebraic structures: groups, rings, and fields.



MODULAR ARITHMETIC

If *a* is an integer and *n* is a positive integer, we define *a* mod *n* to be the remainder when *a* is divided by *n*. The integer *n* is called the **modulus**.

$$a = qn + r \qquad 0 \le r < n;$$

$$q = \lfloor a/n \rfloor$$

Congruent modulo

Two integers a and b are said to be congruent modulo n if

a (mod n)≡ b (mod n)

a ≡ b (mod n)

73 ≡ 4 mod 23

Properties of modulo operator

Congruences have the following properties:

1. a≡ b (mod n) if n|(a-b)

2. a≡ b (mod n) implies b≡ a(mod n)

3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.

Modular Arithmetic Operations

Modular arithmetic exhibits the following properties:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$

2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$

3. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

11 mod 8 = 3; 15 mod 8 = 7

[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2

(11 + 15) mod 8 = 26 mod 8 = 2

[(11 mod 8) - (15 mod 8)] mod 8 = -4 mod 8 = 4

(11 - 15) mod 8 = -4 mod 8 = 4

$$[(11 \bmod 8) * (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$$

$(11 * 15) \bmod 8 = 165 \bmod 8 = 5$

GROUPS, RINGS, AND FIELDS

Groups, rings, and fields are the fundamental elements of a branch of mathematics known as abstract algebra, or modern algebra.

GROUPS

A **group** G, sometimes denoted by $\{G, \bullet\}$, is a set of elements with a binary operation denoted by $\bullet$ that associates to each ordered pair (a, b) of elements in G an element $(a \bullet b)$ in G, such that the following axioms are obeyed:

(A1) Closure: If a and b belong to G, then $a \bullet b$ is also in G.

(A2) Associative: $a\bullet(b\bullet c) = (a\bullet b)\bullet c$ for all a, b, c in G.

(A3) Identity element: There is an element e in G such that $a \bullet e = e \bullet a = a$ for all a in G.

(A4) Inverse element: For each a in G, there is an element a^{-1} in G such that $a \bullet a^{-1} = a^{-1} \bullet a = e$.

If a group has a finite number of elements, it is referred to as a **finite group**, and the **order** of the group is equal to the number of elements in the group. Otherwise, the group is an **infinite group**. A group is said to be **abelian** if it satisfies the following additional condition:

(A5) Commutative: $a \bullet b = b \bullet a$ for all a, b in G.

A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element $a \, \varepsilon \, G$. The element a is said to **generate** the group G or to be a **generator** of G. A cyclic group is always abelian and may be finite or infinite.

RINGS

A **ring** R, sometimes denoted by $\{R, +, *\}$, is a set of elements with two binary operations, called *addition* and *multiplication*,6 such that for all a, b, c in R the following axioms are obeyed.

(A1–A5) R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5.

(M1) Closure under multiplication: If a and b belong to R, then ab is also in R.

(M2) Associativity of multiplication: $a(bc) = (ab)c$ for all a, b, c in R.

(M3) Distributive laws: $a(b + c) = ab + ac$ for all a, b, c in R.

$$(a + b)c = ac + bc \text{ for all } a, b, c \text{ in } R.$$

A ring is said to be **commutative** if it satisfies the following additional condition:

(M4) Commutativity of multiplication: $ab = ba$ for all a, b in R.

An **integral domain**, which is a commutative ring that obeys the following axioms.

(M5) Multiplicative identity: There is an element 1 in R such that $a1 = 1a = a$ for all a in R.

(M6) No zero divisors: If a, b in R and $ab = 0$, then either $a = 0$ or $b = 0$.

FIELDS

A **field** F, sometimes denoted by $\{F, +, *\}$, is a set of elements with two binary operations, called *addition* and *multiplication*, such that for all a, b, c in F the following axioms are obeyed.

(A1–M6) F is an integral domain; that is, F satisfies axioms A1 through A5 and M1 through M6.

(M7) Multiplicative inverse: For each a in F, except 0, there is an element a-1 in F such that

$aa^{-1} = (a^{-1})a = 1$

Relatively prime

Two integers are **relatively prime,** if their only common positive integer factor is 1.

8 and 15 are relatively prime because

Positive divisors of 8 are 1,2,4,8

Positive divisors of 15 are 1, 3, 5, 15

Therefore, common positive factor=1.