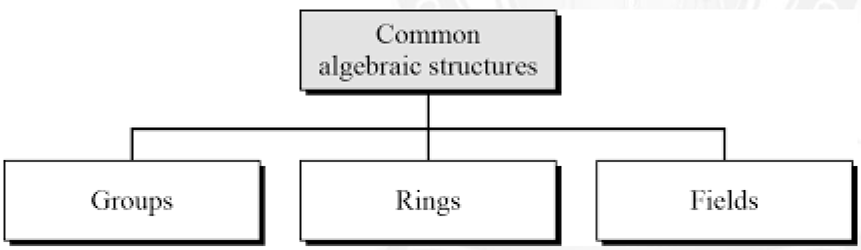
MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY

- Cryptography is based on some specific areas of mathematics including number theory, linear algebra, and algebraic structures.
- Symmetric ciphers use symmetric algorithms to encrypt and decrypt data. These ciphers are used in symmetric key cryptography.
- A symmetric algorithm uses the same key to encrypt data as it does to decrypt data.

ALGEBRAIC STRUCTURES

- Algebra is about operations on sets.
- You have met many operations; for example:
    - addition and multiplication of numbers;
    - modular arithmetic;
    - addition and multiplication of polynomials;
    - addition and multiplication of matrices;
    - union and intersection of sets;
    - composition of permutations.



Reference :William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006

Sets

- A set is a well-defined collection of distinct objects, considered as an object in its own right.
- Two sets are equal if and only if they have the same members
    - That is, A = B if and only if$((x \in A) \Leftrightarrow (x \in B))$.
    - This means that, to prove that two sets are equal, you have to do two things:
        - (i) show that any element of A lies in B;
        - (ii) show that any element of B lies in A.

- (i) means that $A \subseteq B$ (that is, A is a subset of B), while
- (ii) means that $B \subseteq A$.
- So we can re-write our rule:
  - $A \subseteq B$ if and only if $((x \in A) \Rightarrow (x \in B))$,
  - $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.
- From two sets A and B we can build new ones:
  - union: $A \cup B = \{x : x \in A \text{ or } x \in B\}$;
  - intersection: $A \cap B = \{x : x \in A \text{ and } x \in B$;
  - difference: $A \backslash B = \{x : x \in A \text{ and } x \in/ B\}$;
  - symmetric difference: $A \Theta B = (A \backslash B) \cup (B \backslash A)$.

Functions

- A function f from A to B is, informally, a "black box" such that, if we input an element $a \in A$, then an element $f(a) \in B$ is output.
- More formally, a function is a set of ordered pairs (that is, a subset of the cartesian product $A \times B$) such that, for any $a \in A$, there is a unique $b \in B$ such that $(a,b) \in f$; we write $b = f(a)$ instead of $(a,b) \in f$.
- The sets A and B are called the domain and codomain of f ; its image consists of the set
- $\{b \in B : b = f(a) \text{ for some } a \in A\}$, a subset of the codomain.
- A function f is surjective (or onto) if, for every $b \in B$, there is some $a \in A$ such that $b = f(a)$ (that is, the image is the whole codomain);
- injective (or one-to-one) if $a1 \neq a2$ implies $f(a1) \neq f(a2)$ (two different elements of A cannot have the same image);
- bijective if it is both injective and surjective.

Operations

- An operation is a special kind of function.
- An n-ary operation on a set A is a function f from $A^n = A \times \cdots \times A$ to A.
- That is, given any $a1,...,an \in A$, there is a unique element $b = f(a1,...,an) \in A$ obtained by applying the operation to these elements.
- The most important cases are $n = 1$ and $n = 2$; we usually say unary for "1- ary", and binary for "2-ary". We have already seen that many binary operations (addition, multiplication, composition) occur in algebra

Example

- Addition, multiplication, and subtraction are binary operations on R, defined by
  - f(a,b) = a+b (addition),
  - f(a,b) = ab (multiplication),
  - f(a,b) = a−b (subtraction).
- Taking the negative is a unary operation: f(a) = −a

Notation

- we often write binary operations, not in functional notation, but in either of two different ways:
  - infix notation, where we put a symbol for the binary operation between the two elements that are its input, for example a + b, a − b, a · b, a ∗ b, a ◦ b, a • b; or
  - juxtaposition, where we simply put the two inputs next to each other, as ab (this is most usually done for multiplication).
- There are various properties that a binary relation may or may not have. Here are two. We say that the binary operation ◦ on A is
  - commutative if a ◦ b = b ◦ a for all a,b ∈ A;
  - associative if (a ◦ b) ◦ c = a ◦ (b ◦ c) for all a,b,c ∈ A.
  - For example, addition on R is commutative and associative; multiplication of 2×2 matrices is associative but not commutative; and subtraction is neither.

Relations

- A binary relation R on A is a subset of A × A. If (a,b) ∈ R, we say that a and b are related, otherwise they are not related, by R.
- As with operations, we often use infix notation, for example a < b, a ≤ b, a = b, a ∼= b, a ∼ b.
- But note the difference:
- + is an operation, so a+b is a member of A;
- < is a relation, so a < b is an assertion which is either true or false.
- Example Let A = {1,2,3}.
- Then the relation < on A consists of the pairs

  {(1,2),(1,3),(2,3)},
- while the relation ≤ consists of the pairs

{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)}.

- Also like operations, there are various laws or properties that a relation may have.
- We say that the binary operation R on A is
  - reflexive if (a,a) ∈ R for all a ∈ A;
  - irreflexive if (a,a) ∈/ R for all a ∈ A;
  - symmetric if (a,b) ∈ R implies (b,a) ∈ R;
  - antisymmetric if(a,b) and (b,a) are never both in R except possibly if a = b;
  - transitive if (a,b) ∈ R and (b,c ∈ R imply (a,c) ∈ R.
- For example, < is irreflexive, antisymmetric and transitive, while ≤ is reflexive, antisymmetric and transitive.

Equivalence relations and partitions

- A binary relation R on A is an equivalence relation if it is reflexive, symmetric and transitive.
- A partition P of A is a collection of subsets of A having the properties
- (a) every set in P is non-empty;
- (b) for every element a ∈ A, there is a unique set X ∈ P such that a ∈ X.
- The second condition says that the sets in P cover A without overlapping.

Algebraic Structure

- A non empty set S is called an algebraic structure w.r.t binary operation (*) if it follows following axioms:
- Closure:(a*b) belongs to S for all a,b ∈ S.
- Ex : S = {1,-1} is algebraic structure under *
- As 1*1 = 1, 1*-1 = -1, -1*-1 = 1 all results belongs to S.
- But above is not algebraic structure under + as 1+(-1) = 0 not belongs to S.

Semi Group

- A non-empty set S, (S,*) is called a semigroup if it follows the following axiom:
- Closure:(a*b) belongs to S for all a,b ∈ S.
- Associativity: a*(b*c) = (a*b)*c ∀ a,b,c belongs to S.
- Note: A semi group is always an algebraic structure.

- Ex : (Set of integers, +), and (Matrix ,*) are examples of semigroup.

Monoid

- A non-empty set S, (S,*) is called a monoid if it follows the following axiom:
- Closure:(a*b) belongs to S for all a,b ∈ S.
- Associativity: a*(b*c) = (a*b)*c ∀ a,b,c belongs to S.
- Identity Element: There exists e ∈ S such that a*e = e*a = a ∀ a ∈ S
- Note: A monoid is always a semi-group and algebraic structure.
- Ex : (Set of integers,*) is Monoid as 1 is an integer which is also identity element . (Set of natural numbers, +) is not Monoid as there doesn't exist any identity element. But this is Semigroup.
- But (Set of whole numbers, +) is Monoid with 0 as identity element.

Group

- A non-empty set G, (G,*) is called a group if it follows the following axiom:
- Closure:(a*b) belongs to G for all a,b ∈ G.
- Associativity: a*(b*c) = (a*b)*c ∀ a,b,c belongs to G.
- Identity Element:There exists e ∈ G such that a*e = e*a = a ∀ a ∈ G
- Inverses:∀ a ∈ G there exists a^{-1} ∈ G such that $a*a^{-1} = a^{-1}*a = e$

Note:

- A group is always a monoid, semigroup, and algebraic structure.
- (Z,+) and Matrix multiplication is example of group.

Abelian Group or Commutative group

- A non-empty set S, (S,*) is called a Abelian group if it follows the following axiom:
- Closure:(a*b) belongs to S for all a,b ∈ S.
- Associativity: a*(b*c) = (a*b)*c ∀ a,b,c belongs to S.
- Identity Element:There exists e ∈ S such that a*e = e*a = a ∀ a ∈ S
- Inverses:∀ a ∈ S there exists a^{-1} ∈ S such that $a*a^{-1} = a^{-1}*a = e$
- Commutative: a*b = b*a for all a,b ∈ S
- Note : (Z,+) is a example of Abelian Group but Matrix multiplication is not abelian group as it is not commutative.