Basic Cryptography

None(n0n3x1573n7)

November 28, 2018

1 Preliminaries

1.1 Mathematical Structures

1.1.1 Sets

Definition 1 (Set). A set is a collection of distinct objects.

1.1.2 Group

Definition 2 (Group). A group is a set G with a binary operation $\cdot$, denoted $(G, \cdot)$, which satisfies the following conditions:

- **Closure**: $\forall a, b \in G, a \cdot b \in G$
- **Associativity**: $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- **Identity**: $\exists e \in G, \forall a \in G, a \cdot e = e \cdot a = a$
- **Inverse**: $\forall a \in G, \exists a^{-1} \in G, a \cdot a^{-1} = a^{-1} \cdot a = e$

Definition 3 (Semigroup). A semigroup is $(G, \cdot)$, which satisfies Closure and Associativity.

Definition 4 (Monoid). A monoid is a semigroup $(G, \cdot)$ which also has identity.

Definition 5 (Abelian Group). An Abelian Group or Commutative Group is a group $(G, \cdot)$ with the following property:

- **Commutativity**: $\forall a, b \in G, a \cdot b = b \cdot a$

1.1.3 Ring

Definition 6 (Ring). A Ring is a set R with two binary operations $+$ and $\cdot$, often called the addition and multiplication of the ring, denoted $(R, +, \cdot)$, which satisfies the following conditions:

- $(R, +)$ is an abelian group
- $(R, \cdot)$ is a semigroup
- **Distribution** $\cdot$ is distributive with respect to $+$, that is, $\forall a, b, c \in R$:
  - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
  - $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

The identity element of $+$ is often noted 0.

Definition 7 (Ring with identity(1)). A Ring with identity is a ring $(R, +, \cdot)$ of which $(R, \cdot)$ is a monoid. The identity element of $\cdot$ is often noted 1.

Definition 8 (Commutative Ring)**.** A commutative ring is a ring $(R, +, \cdot)$ of which $\cdot$ is commutative.

Definition 9 (Zero Divisor)**.** For a ring $(R, +, \cdot)$, let 0 be the identity of $+$.
$a, b \in R$, $a \neq 0$ and $b \neq 0$, if $a \cdot b = 0$, a, b are called the zero divisors of the ring.

Definition 10 (Integral Domain)**.** An integral domain is a commutative ring $(R, +, \cdot)$ with 1 which does not have zero divisors.

1.1.4 Field

Definition 11. A Field is a set F with two binary operations $+$ and $\cdot$, often called the addition and multiplication of the field, denoted $(R, +, \cdot)$, which satisfies the following conditions:

- $(F, +, \cdot)$ is a ring
- $(F \backslash \{0\}, \cdot)$ is a group