Cryptography And Cryptanalysis

Ph. D. Course/ 2019-2020

Introduced By

Dr. Faez Hassan Ali

Lecture One-2

Mathematical Basic Concepts

Group Theory

__Definition__: A **binary operation** * on a set A is a rule that assign to each ordered pair (a,b) of elements of A a unique element of A.

__Example__: Ordinary addition + and multiplication • are binary operations on N, Z, R, or C.

__Definition__: A **group**, denoted by $\langle G,*\rangle$ (or (G,*)), or simply G, is a $G \neq \phi$ of elements together with a binary operation *, s.t. the following axioms are satisfied:

- **Closure**: $a*b \in G$, $\forall a,b \in G$.
- **Associativity**: $(a*b)*c=a*(b*c)$, $\forall a,b,c \in G$.
- **Existence of identity**: $\exists!$ element $e \in G$, called the identity, s.t. $e*a=a*e=a$, $\forall a \in G$.
- **Existence of inverse**: $\forall a \in G$, $\exists!$ Element $b \in G$, s.t. $a*b=b*a=e$. This b is denoted by a^{-1} and called the **inverse** of a.
- The group $\langle G,*\rangle$ is called **commutative** (**abelian**) group if it satisfies further axiom: **Commutativity**: $a*b=b*a$, $\forall a,b \in G$.

Group Theory

Example: the set Z^+ with operation + is not group ($\exists$ no identity element), and it's not group with operation $\bullet$ ($\exists$ no inverse element in Z^+).

Definition: If the binary operation of a group is +, then the identity of group is 0 and the inverse of $a \in G$ is $-a$; this said to be an **additive group**.

If the binary operation of a group is $\bullet$, then the identity of a group is 1 or e, this group is said to be **multiplicative group**.

Definition: A group is called a **finite group** if it has finite number of elements; otherwise it is called an **infinite group**.

Definition: The **order** of the group G, denoted by $|G|$ (or by $\#(G)$) is the number of elements of G. for example: the order of Z is $|Z|=\infty$.

Definition: Let $a \in G$, where G is multiplicative group. The elements a^r, where r is an integer, form a subgroup of G, called the **subgroup** generated by a. A group G is **cyclic** if $\exists$ $a \in G$ s.t. the subgroup generated by a is the whole of G.

Remark: If G is a finite cyclic group with identity element e, the set of elements G may be written $\{e,a,a^2,\ldots,a^{n-1}\}$, where $a^n=e$ and n is the smallest such positive integer.

Definition : A **field** by $\langle F,\oplus,\otimes \rangle$ (or $(F,\oplus,\otimes)$) or simply F, is abelian group w.r.t. addition, and F-{0} is abelian w.r.t. to multiplication.

Group Theory

Definition: A **finite field** is a field that has a finite number of elements in it; we call the number the order of the field.

Theorem: $\exists$ a field of order q iff q is **prime power** (i.e. $q=p^r$) with p prime and $r \in N$.

Remark: A field of order q with q prime power is called **Galois field** and is denoted by GF(q) or just F_q.

Example : The finite field F_5 has elements {0,1,2,3,4} and is described by the table(4.1) addition and multiplication table.

$\oplus$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Boolean Ring and Boolean Algebra

Definition: Let $A \neq \phi$ be a set, f be a binary operation on a set A ($f: A \times A \to A$), we call the pair (A,f) as **mathematical system**.

Definition: Let X be the universal set, and let A and B be two subsets of X, then:

The operation + defined as $A+B=A \cup B$.

The operation $\oplus$ defined on the power P(X) set of X by:

$A \oplus B=(A-B) \cup (B-A)$ s.t. $A-B=A \cap B'$, B' is the **complement** set of B.

The operation $\oplus$ called **Exclusive-OR** (**XOR**) (or the **symmetric difference**).

The operation • defined as $A \bullet B=A \cap B$.

Definition: Let (R,+,•) be a ring with identity element, if the **law** be satisfied $a^2=a$, $\forall a \in R$, then the ring called **Boolean ring**.

Example: Let P(X) represents the set of all the subsets of the universal set X, then the ring $(P(X),\oplus,\bullet)$ is Boolean ring.

Boolean Ring and Boolean Algebra

<u>Definition:</u> In Boolean ring $(B,\oplus,\bullet)$, we defined:

Complement: $a=a\oplus 1$, $\forall a\in B$. and **Sum (OR)**: $a+b=a\oplus b\oplus a.b$ $\forall a,b\in B$.

<u>Definition:</u> The **Boolean algebra** is the mathematical system $(B,\vee,\wedge)$ where $B\neq\phi$, and the binary operations $\vee$ and $\wedge$ defined on B as follows:

The operations $\vee$ and $\wedge$ are commutative.

The operations $\vee$ and $\wedge$ are satisfy the distribution law for each to other.

$\exists$ two identity distinct elements 0 and 1 of the operations $\vee$ and $\wedge$ respectively s.t. $a\vee 0=a$ and $a\wedge 1=a$, $\forall a\in B$.

<u>Example</u>: The system $(P(X),\bigcup,\bigcap)$ is boolean algebra, $X\neq\phi$, we use $\phi=0$ and $X=1$. If B be a set of subsets of X including ϕ and X which is closed on $\bigcup$ and complement then $(B,\bigcup,\bigcap)$ is boolean algebra too.

<u>Theorem</u>: Every boolean algebra $(B,\vee,\wedge)$ is boolean ring $(B,\oplus,\bullet)$ when we defined the operations $\oplus$ and as follows:

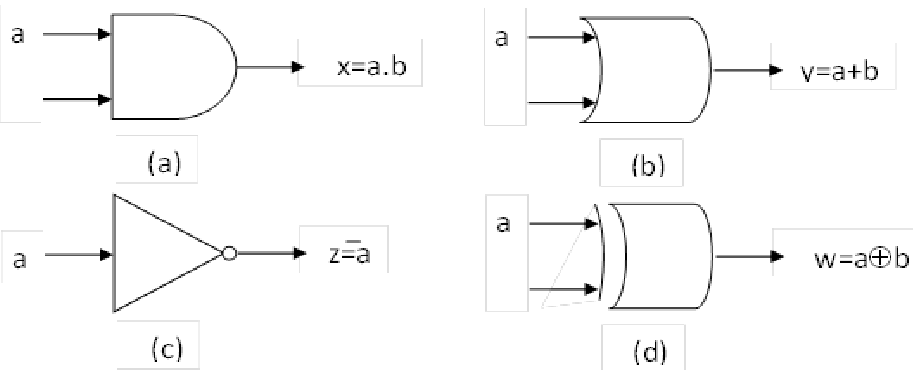
$a\oplus b=(a\wedge b')\vee(a'\wedge b)$. and $a\bullet b=a\wedge b$, $\forall a,b\in B$.

<u>Theorem</u>: Every ring $(B,\oplus,\bullet)$ is Boolean algebra $(B,\vee,\wedge)$ when we defined $\vee$ and $\wedge$ as follows: $\forall a,b\in B$. $a\vee b=a\oplus b\oplus a\bullet b$ and $a\wedge b=a\bullet b$.

<u>Theorem</u>: The ring $(Z_p,\oplus,\otimes)$ is field iff p is prime number s.t. $a\oplus b=a+b \pmod{p}$. And $a\otimes b=a\bullet b \pmod{p}$.

This field is **Galois field** and is denoted by GF(p), $\forall a,b\in Z_p$.

Algebra Description of Logic Circuits



•	0	1
0	0	0
1	0	1

+	0	1
0	0	1
1	1	1

a	$\bar{a}$
0	1
1	0

⊕	0	1
0	0	1
1	1	0

(a).The gate AND: is multiplying the input variables.

(b).The gate OR: summing the input variables.

(c).The gate NOT: complement of the input variable.

(d).The gate XOR: summing XOR the input variables.

Definition (6.1): The logical function f is called the **output function** defined f:$B^n \rightarrow B$, where B^n is a set of n input binary data, f subject to the Boolean algebra laws and we can apply the gates concepts on it, s.t. $x=f \bullet g$, $y=f+g$, $z=\bar{f}$, and $w=f \oplus g$, where f and g are Boolean functions.

Algebra Description of Logic Circuits

Q4. Draw and simplify the logical circuit:

$$F(a,b,c) = (\overline{ab} \oplus 1) + \overline{ac} \oplus \bar{c} + 1 + ab(\overline{ac} \oplus b) + 1$$

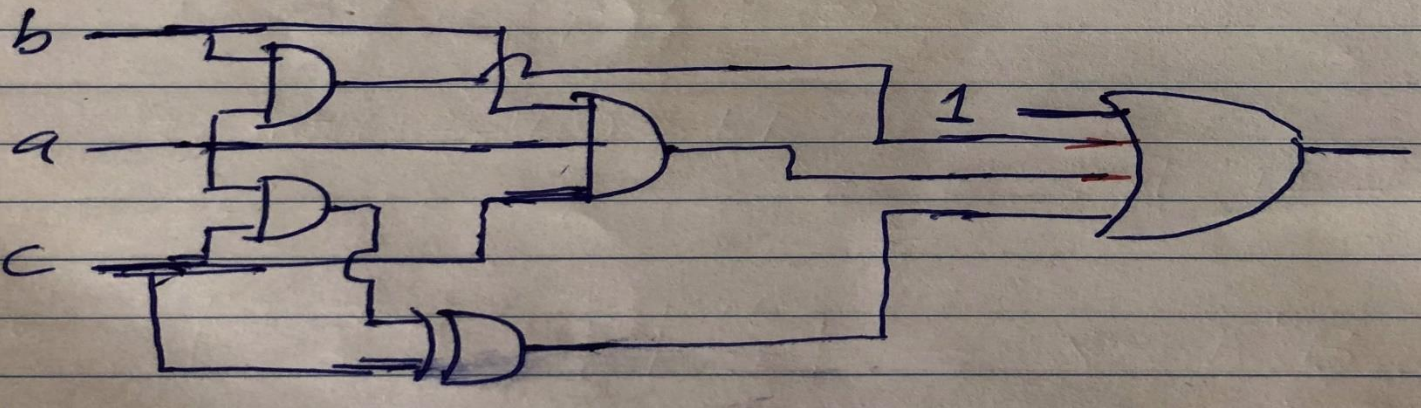
Then draw the simplified circuit. Check the equivalency of the two circuits.

$$F(a,b,c) = (ab \oplus \cancel{1} \oplus \cancel{1}) + (ac \oplus \cancel{1} \oplus c \oplus \cancel{1}) + \cancel{1} + ab(ac \oplus 1 \oplus b) + \cancel{1}$$

$$= ab + (ac \oplus c) + ab(ac \oplus b \oplus 1) + 1$$

$$= ab + (ac \oplus c) + abc \oplus \cancel{ab} \oplus \cancel{ab} + 1$$

$$= ab + (ac \oplus c) + abc + 1$$



Algebra Description of Logic Circuits

$F_2(a,b,c) = ab + (ac \oplus c) + abc + 1$

a	b	c	ab	ac	$ac \oplus c$	abc	1	F_2
0	0	0	0	0	0	0	1	1
0	0	1	0	0	1	0	1	1
0	1	0	0	0	0	0	1	1
0	1	1	0	0	1	0	1	1
1	0	0	0	0	0	0	1	1
1	0	1	0	1	0	0	1	1
1	1	0	1	0	1	0	1	1
1	1	1	1	1	1	1	1	1

ab	$\overline{ab}$	ac	$\overline{ac}$	$\overline{c}$	$\overline{ab} \oplus 1$	$\overline{ac} \oplus \overline{c}$	$\overline{ac} \oplus b$	$ab(\overline{ac} \oplus b)$		$+1$
0	1	0	1	1	0	0	1	0	0	1
0	1	0	1	0	0	1	1	0	1	1
0	1	0	1	1	0	0	0	0	0	1
0	1	0	1	0	0	1	0	0	1	1
0	1	0	1	1	0	0	1	0	0	1
0	1	1	0	0	0	0	0	0	0	1
1	0	0	1	1	1	0	0	0	1	1
1	0	1	0	0	1	0	1	1	1	1

Sequences and Series

Sequences

Definition : The **sequence** in the field F is a function *f*, whose domain is the set of non negative (or could be positive) integer, s.t. f:Z→F, and its denoted by $S = \{S_n\}_{n=0}$

Definition : The Sequence S is **periodic** when $\exists p \in Z^+$ s.t. $s_0=s_p, s_1=s_{p+1},\ldots$, the minimum p is the **period** of S.

If $Z_m=\{0,1,\ldots,m-1\}$, where $m \in Z^+$, then S is digital sequence. In special case, if m=2 then S is binary sequence.

Series

Definition: An infinite series is an expression of the form:

- $u_1+u_2+\ldots u_k+\ldots= \sum_{k=1}^{\infty} u_k$
- Let S_n denotes the sum of the first *n* terms of the series s.t.
- $S_n= \sum_{k=1}^{n} u_k$, and $\{S_n\}_{n=0}$ is called the **sequence of partial sums**.
- $S= \sum_{k=1}^{\infty} u_k$ is called the **sum** of the series.

Polynomials over Fields

Let $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \ldots + a_1 \cdot x + a_0$ be a polynomial of degree n in one variable x over a field F (namely $a_n, a_{n-1}, \ldots, a_1, a_0 \in F$).

Theorem: The equation $f(x)=0$ has at most n solutions in F.

Irreducible Polynomials

Definition : A polynomial is irreducible in GF(p) if it does not factor over GF(p). Otherwise it is reducible.

Examples:

The polynomial $x^5+x^4+x^3+x+1$ is **reducible** in Z_5 but **irreducible** in Z_2.

Polynomials over Fields

Implementing $GF(p^k)$ Arithmetic

Theorem: Let f(x) be an irreducible polynomial of degree k over Z_p. The finite field $GF(p^k)$ can be realized as the set of degree k-1 polynomials over Z_p, with addition and multiplication done modulo f(x).

Example: **(Implementing $GF(2^k)$)**

By the theorem the finite field $GF(2^5)$ can be realized as the set of degree 4 polynomials over Z_2, with addition and multiplication done modulo the irreducible polynomial: $f(x)=x^5+x^4+x^3+x+1$.

The coefficients of polynomials over Z_2 are 0 or 1. So a degree k polynomial can be written down by k+1 bits.

For example, with k=5: x^3+x+1 (0,1,0,1,1), x^4+x^3+x+1 (1,1,0,1,1).

Implementing $GF(2^k)$

Addition: bit-wise XOR (since 1+1=0)

x^3+x+1 (0,1,0,1,1)

+

x^4+x^3+x+1 (1,1,0,1,1)

----

x^4 , (1,0,0,0,0)

Multiplication: $(x^2+x+1)\cdot(x^3+x+1)$ in $GF(2^5)$.

(1,1,1)·(1,0,1,1)

```
1 0 1 1
  1 0 1 1
    1 0 1 1
----------------
1 1 0 0 0 1
```

1 1 0 0 0 1 = x^5+x^4+1

Polynomials over Fields

The Number of Irreducible and Primitive Polynomials

The function $\mu : Z^+ \rightarrow Z^+$ defined by:

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1; \\ (-1)^r \text{ if } n = p_1 p_2 \ldots p_r, \text{ where the } p_i \text{ are distinct primes;} \\ 0 \text{ if } n \text{ has a squared factor} \end{cases}$$

is called the **Möbius Function**.

The number of monic irreducible polynomials of degree k over F_q is given by: $\psi_q(k) = \frac{1}{k}\sum_{d|k}\mu(\frac{k}{d})q^d$

Clearly, not every monic irreducible polynomial in $F_q[x]$ is necessarily a primitive polynomial over F_q. In fact, the number of primitive polynomials of degree k over F_q is: $\lambda_q(k) = \frac{\phi(q^k - 1)}{k}$

__Example__ : Consider (monic) irreducible polynomials of degree 8 over $F_2=Z_2$. The positive divisors of 8 are d = 1, 2, 4, 8 so that 8/d = 8, 4, 2, 1 and μ(8/d)= 0, 0,−1, 1. Therefore, the number of monic irreducible polynomials of degree 8 in $F_2[x]$ is:

$\psi_2(8) = \frac{1}{8}\sum_{d|8}\mu(\frac{8}{d})2^d$ = (0 + 0 − 16 + 256)/8= 30.

Furthermore, the number of primitive polynomials of degree 8 in $F_2[x]$ is:

$\lambda_2(8) = \frac{\phi(2^8 - 1)}{8} = \frac{\phi(255)}{8} = \frac{\phi(3.5.17)}{8} = \frac{2.4.16}{8}$ = 16.

Hence, just over half the irreducible polynomials of degree 8 in $Z_2[x]$ are primitive.

However, if $2^k - 1$ is prime then $(2^k - 2)/k$ so that every irreducible polynomial of degree k is in fact a primitive polynomial in $Z_2[x]$. It is therefore beneficial, in the practical sense, to choose a reasonably large value of k such that $2^k - 1$ is prime.