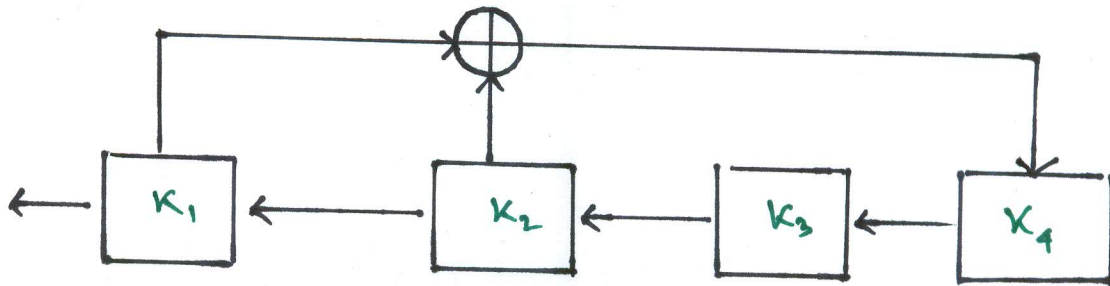


Week-3 : Lecture Notes

Topics :

LFSR based Stream cipher.
Mathematical background.
Abstract algebra.
Number theory.
Modular inverse.

Linear Feedback Shift Register (LFSR)



- An LFSR of length m consists of m stages numbered $1, 2, 3, \dots, m$, each storing one bit and having one input and one output; together with a clock which controls the movement of data.

- The vector (k_1, k_2, \dots, k_m) would be used to initialize the shift register.
- During each unit of time the following operation would be performed concurrently
 - i) k_1 would be tapped as the next key stream bit.
 - ii) k_2, \dots, k_m would be shifted one stage to the left
 - iii) the 'new' value of k_m would be computed to be

$$\sum_{j=1}^{m-1} c_j k_{j+1}$$

$$j=1.$$

The linear feedback is carried out by taping certain stages of the register (as specified by the constants c_j having the value 1) and computing a sum modulo 2 (which is an exclusive-or) .

Mathematical background

- In order to understand some of cryptographic algorithms dealt with throughout this course, it is necessary to have some background in two areas of mathematics
 1. Number Theory.
 2. Abstract Algebra.
- New Advanced Encryption Standard (AES) relies on the subject of finite fields which forms a part of abstract algebra.
- Going to deal with Number Theory for the moment.

Number Theory

- Number theory deals with the theory of numbers and is probably one of the oldest branches of mathematics.

- It is divided into several areas including elementary, analytic and algebraic number theory.
- These are distinguished more by the methods used in each than the type of problems posed.
- Relevant ideas discussed here and include:
 - prime numbers
 - the greatest common divisor
 - the modulus operator
 - the modular inverse

Prime numbers

- A prime number p is an integer greater than 1 with only two positive divisors, 1 and itself.
- Therefore its entire set of divisors (i.e. its factors) consist only of four integers ± 1 and $\pm p$

- It can be seen that 1 is not a prime number.
- Prime numbers are of the utmost importance to certain cryptographic algorithms and most of the techniques used will not work without them.
- Any positive integer $I \geq 2$ is either a prime or can be expressed as the product of primes.
- This is known as the fundamental theorem of arithmetic:

$$I = P_N^{\epsilon_N} \times P_{N-1}^{\epsilon_{N-1}} \times \dots \times P_1^{\epsilon_1}, \quad P_N > P_{N-1} > \dots > P_1$$

- - - (i)

- Another way of looking at this would be:

$$I = \prod_s P_n^{\epsilon_n} \quad \epsilon_n \geq 0 \quad - \dots (ii)$$

Here 's' is the set of all prime numbers.

- In general most of the exponents ϵ_n will be '0'.

- As a result of equation (i) and (ii) any integer > 1 , that is not a prime number is known as a composite number.
- It can be seen that from this and the definition of a prime number above, that 1 is neither prime nor composite.
- The first prime numbers are:
2, 3, 5, 7, 11, 13, 17, 19, 23 and 29.

Division

- Any integer can be expressed as $n = q \times m + r$, where n, q , and r are integers, m is a positive integer and $0 \leq r < m$
- The remainder (also known as residue) r , must be non-negative (i.e. either positive or 0)

- This is seen by two restrictions:
 1. $0 \leq r < m$
 2. $q = \left\lfloor \frac{n}{m} \right\rfloor$
- The notation $\lfloor x \rfloor$ is known as the floor of the integer x and is the greatest integer $\leq x$.
- The notation $\lceil x \rceil$ is the ceiling of the integer x and is the least integer $\geq x$.
- For example, $24 \div 10$ is 2 with a remainder 4 however, $-24 \div 10$ is -3 with a remainder 6 and not -2 with a remainder -4 as might be expected.
- If $r=0$ then n is said to be a multiple of m . This is also the same as saying that m divides n , is a divisor of n or is a factor of n and the notation used to express this is $m|n$.

- The greatest common divisor, m_{\max} , of two integers a and b is the largest positive integer that will divide both a and b without a remainder.
- Therefore $m_{\max} | a$, $m_{\max} | b$ and $m_n | m_{\max}$ for any divisor m_n of a and b .
- The notation generally used to represent this is $\text{gcd}(a, b) = m_{\max}$.
- If $\text{gcd}(a, b) = 1$, this means that a and b have no common factors other than 1.
- Such pair is known as relatively prime or co-prime
- Along with prime numbers, numbers that are relatively prime have considerable importance in cryptography as will be seen later.

- The greatest common divisor of two positive integers a and b ($\text{gcd}(a, b)$) can be determined by a procedure known as Euclid's Algorithm. It is based on the theorem that
$$\text{gcd}(a, b) = \text{gcd}(b, a \bmod b)$$

- The expression 'mod' is used in modular arithmetic which is a special kind of arithmetic involving remainders as will be seen next.

Modular Arithmetic

- The symbol used (\equiv) is known as the congruence symbol.
- Modular relationships are of the form $n \equiv R \pmod{m}$ (spoken as "n is congruent to R mod m") where n and R are integers and m is a positive integer known as the modulus.

- If this congruence relationship holds, then it is said that n is congruent to R modulo m .
- The modulus operator (mod) produces the remainder when the integer on its left is divided by the modulus.
- Thus the term $(R \text{ mod } m)$ is equal to the remainder r , when R is divided by m .
- If two remainders are equal then it can be written that $(n \text{ mod } m) \equiv (R \text{ mod } m)$ - a standard equality.
- However, if the modulus is equal on both sides of the equation, then the $(\text{mod } m)$ term can be removed from the left side and the equality symbol replaced with a congruence symbol (along with a slight rearrangement of the brackets).

- Assuming $n \neq r$, it would be incorrect to say $n = (R \bmod m)$.
- However, it is correct to say that $n \equiv R \pmod{m}$ and this basically states that the same remainder (in this case r) results when both n and R are divided by m .
- As mentioned, the remainder r is also known as a residue.
- If $R = r$ (i.e. $0 \leq R < m$) then R is known as a least residue.
- The congruent relation ' \equiv ' is an equivalence relation.
- The set of numbers congruent to some value ' $a \pmod{m}$ ' is known as a residue class (or a congruent class).
- As $0 \leq r < m$, this means there are m possible values of r and hence there are m possible residue classes.

- The congruence relationship $n \equiv R \pmod{m}$ is only true if $m \mid n - R$
- If $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$, then $a + b \equiv a_1 + b_1 \pmod{m}$ and $ab \equiv a_1 b_1 \pmod{m}$
- The integers modulo m , denoted Z_m is the set of integers $\{0, 1, 2, \dots, m-1\}$
- To understand why, it must be remembered that the integers n and R can be expressed as $q_{\{n, R\}} \times m + r_{\{n, R\}}$ where the subscript $\{n, R\}$ represents the fact that q and r will generally take on different values for n and R .
- Only if $r_n = r_R$ will $m \mid (n - R)$ because in this case the two remainders cancel each other in the $(n - R)$ term:

$$(q_n \times m + r_n - q_R \times m - r_R) = (q_n \times m - q_R \times m)$$
- Because $m \mid (q_n \times m)$ and $m \mid (q_R \times m) \Rightarrow m \mid (q_n \times m - q_R \times m)$. If $(n - R)$ is not

divisible by m then the notation used to represent this is χ and therefore $m \chi (n - R)$. In this case $n \not\equiv R \pmod{m}$.

Modular Inverse

- The idea of an inverse is important both in ordinary arithmetic and modular arithmetic.
- In any set of numbers, the inverse of a number contained in that set is another number which when combined with the first under a particular operation will give the Identity element for that operation.
- The identity element for a particular operation is a number that will leave the original number unchanged under that operation.
- Two examples of inverses are the:
(1) Additive inverse, (2) Multiplicative inverse.

- The Identity element under different operations will be different.
- Under addition, it is '0', as any number added to '0' will remain unchanged.
- However, under normal multiplication the identity element is 1 as any number multiplied by 1 will remain unchanged.
- In ordinary arithmetic if the number is x then the additive inverse is $-x$ and multiplicative inverse is $\frac{1}{x}$.
- The idea is same in modular arithmetic however if x is an integer then its multiplicative inverse would not be $\frac{1}{x}$ as there is no such things as a ~~fraction~~ in modular arithmetic.
- In this case, it would be a number which, when multiplied by the

original number, would give a result that is congruent $1 \pmod{m}$ (again, m is the modulus).

- A number x can only have a multiplicative inverse if it is relatively prime to the modulus (i.e. $\gcd(x, m) = 1$)
- When one number is operated on modulo some other number, it is said that the first number has been reduced modulo the second and the operation is called a modular reduction.
- Let $a \in \mathbb{Z}_m$, the multiplicative inverse of a modulo m is an integer x belongs to \mathbb{Z}_m such that $ax \equiv 1 \pmod{m}$. If such an ' x ' exists, then it is unique and a is said to be invertible. The inverse of a is denoted by a^{-1} .

Abstract Algebra

- Will only be looking at a very small subset of what this subject has to offer.
- Three main ideas here that need to be grasped:
 1. Group (G, \cdot)
 2. Ring $(R, +, \cdot)$
 3. Field $(F, +, \cdot)$
- Basically, three different types of sets along with some operations.
- The classification of each set is determined by the axioms which it satisfies.

Group

- A Group (G, \cdot) is a set under some operation (\cdot) if it satisfies the following 4 axioms:
 1. **closure** (A_1) : For any two elements $a, b \in G$, $c = a \cdot b \in G$.

2. Associativity (A_2): For any three elements $a, b, c \in G$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

3. Identity (A_3): There exists an Identity element $e \in G$ such that $\forall a \in G$, $a \cdot e = e \cdot a = a$.

4. Inverse (A_4): Each element a in G has an inverse i.e. $\forall a \in G$ $\exists a^{-1} \in G$, $a \cdot a^{-1} = a^{-1} \cdot a = e$

• However it is said to be an Abelian group if in addition to the above the set follows the axiom:

5. Commutativity (A_5): For any $a, b \in G$

$$a \cdot b = b \cdot a$$

Cyclic group

• Exponentiation is the repeated application of the group operator.

- We might have a^3 and this would equal $a \cdot a \cdot a$.
- So, if the operation was addition then a^3 would in fact be $a + a + a$.
- Also we have $a^0 = e$ which for an additive group is 0.
- $a^{-n} = (a^{-1})^n$
- A group is said to be cyclic if every element of the group G is a power a^k (where k is an integer) of a fixed element $a \in G$.
- The element a is said to generate G or be a generator of G .
- A cyclic group is always abelian and may be finite or infinite.
- If a group has a finite number of elements it is referred to as a finite group.
- The order of the group is equal to the number of elements in the

group. Otherwise the group is an infinite group.

Ring

- A binary operation is a mapping of two elements into one element under some operation. For a set S we have $f: S \times S \rightarrow S$
- A ring $\{R, +, \cdot\}$ is a set with two binary operations addition and multiplication that satisfies the following axioms:
 1. Abelian group under addition ($A_1 \rightarrow A_5$):
It satisfies all the of the axioms for an abelian group (all of the above) with the operation of addition.
The identity element is '0' and inverse is denoted by $-a$.
 2. closure under multiplication (M_1):
For any $a, b \in R$,
 $c = a \cdot b \in R$

3. Associativity of multiplication (M_2):

For any elements $a, b, c \in R_q$, $(a \cdot b) \cdot c = a(b \cdot c)$

4. Distributive (M_3): For any

elements $a, b, c \in R_q$,

$$a(b+c) = ab+ac$$

- It is then said to be a commutative ring if in addition the ring follows the axiom:

5. Commutativity (M_4): For any

$$a, b \in R_q \quad ab = ba$$

- It is an integral domain if in addition the commutative ring follows the axioms:

6. Multiplicative Identity (M_5): There is an element 1 in R_q such that $a1=1a=a \quad \forall a \in R_q$.

7. No Zero Divisors (M_6): If $a, b \in R_q$ and $ab=0$ then either $a=0$ or $b=0$.

Field

- A field $\{F, +, \times\}$ is a set with two binary operations addition and multiplication that satisfies the following axioms:

1. Integral Domain ($A_1 \rightarrow M_6$): It satisfies all of the axioms for an integral domain (all of the above)

2. Multiplicative Inverse (M_7): Each element in F (except 0) has an inverse i.e

$$\forall a (\neq 0) \in F, \exists a^{-1} \in F, aa^{-1} = a^{-1}a = 1.$$

- In ordinary arithmetic it is possible to multiply both sides of an equation by the same value and still have the equality intact.
- Not necessarily true in finite arithmetic.
- In this particular type of arithmetic we are dealing with a set containing a finite number of values.

- The set of real numbers is an infinite set and is not really useful for working with computer systems due to the limited amount of memory and processing power.
- Much easier if every operation the computer performed resulted in a finite value that was easily handled. This is where finite fields come into play.
- Closure is the property that causes the result of a binary operation on an ordered pair of a set to be a part of that set also.
- The term ordered pair is important as it is not generally the case that $a \cdot b = b \cdot a$
- To restate, Groups, Rings and Fields are all sets defined with either one or more binary operations.

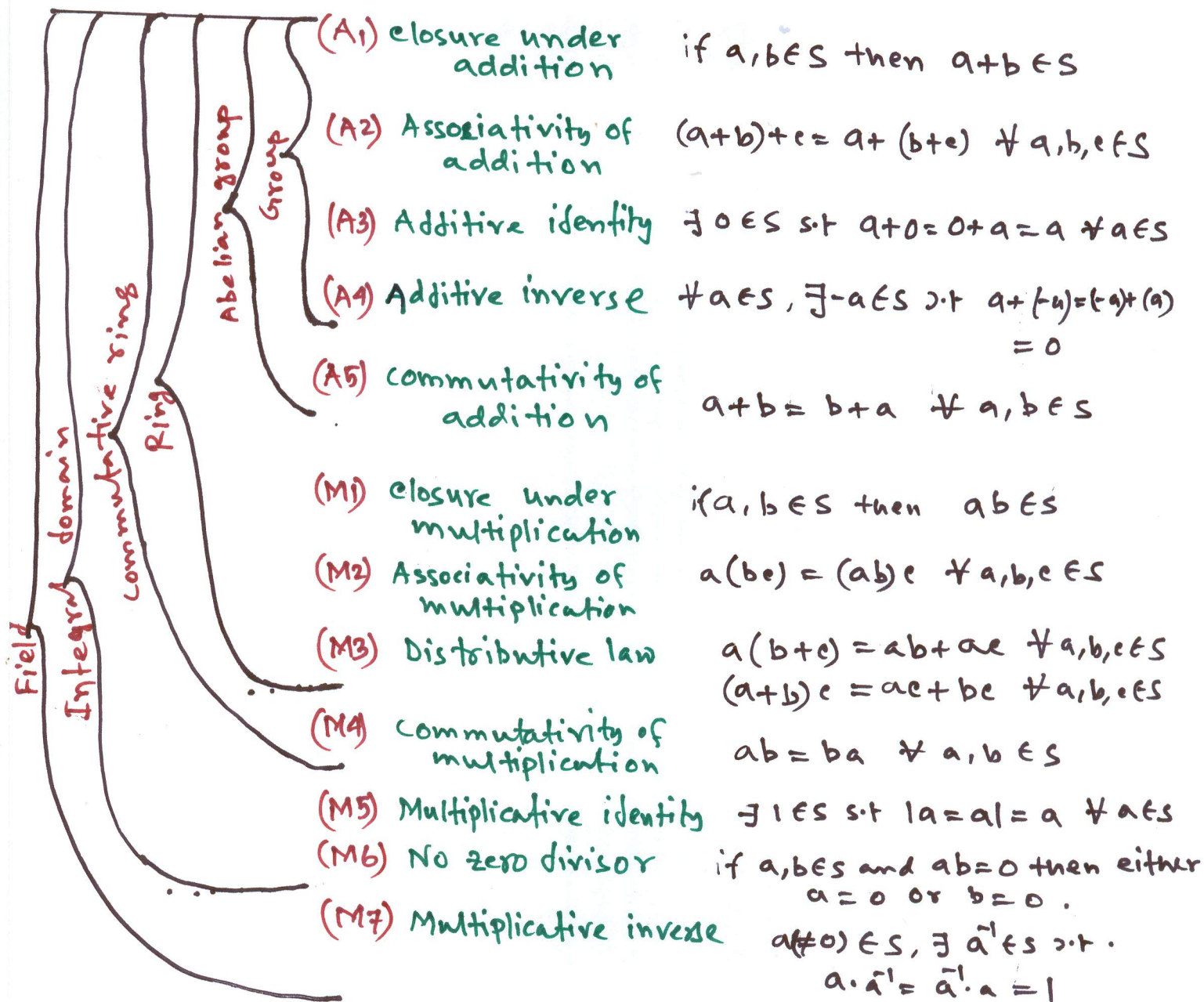


Fig2 Group, Ring, Field.

- Fig2 summarises the hierarchical structure of the group, ring and field. It can be seen that the group is defined under addition.