1. INTRODUCTION:

The origin of the word cryptology lies in ancient Greek. The word cryptology is made up of two components: "kryptos", which means hidden and "logos" which means word. Cryptology is as old as writing itself, and has been used for thousands of years to safeguard military and diplomatic communications. For example, the famous Roman emperor Julius Caesar used a cipher to protect the messages to his troops. Within the field of cryptology one can see two separate divisions: cryptography and cryptanalysis. The cryptographer seeks methods to ensure the safety and security of conversations while the cryptanalyst tries to undo the former's work by breaking his systems.

The main goals of modern cryptography can be seen as: user authentication, data authentication (data integrity and data origin authentication), non-repudiation of origin, and data confidentiality.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.

Cryptology embraces both cryptography and cryptanalysis.

Cryptography can be strong or weak. Cryptographic strength is measured in the time and resources it would require to recover the plaintext. The result of strong cryptography is cipher text that is very difficult to decipher without possession of the appropriate decoding tool. How difficult? Given all of today's computing power and available time — even a billion computers doing a billion checks a second — it is not possible to decipher the result of strong cryptography before the end of the universe.

2. MATHEMATICS BEHIND CRYPTOGRAPHY:

1. Z denotes the set of *integers*.
2. Q denotes the set of *rational numbers*.
3. R denotes the set of *real numbers*.

Let a, b be integers. Then a *divides* b (equivalently: a is a *divisor* of b, or a is a factor of b) if there exists an integer c such that b = ac. If a divides b, then this is denoted by a|b.

For all a, b, c belonging to Z, the following are true:
(i) a|a.
(ii) If a|b and b|c, then a|c.
(iii) If a|b and a|c, then a|(bx + cy) for all x, y belonging to Z.
(iv) If a|b and b|a, then a = b.

2.1. Division algorithm for integers - If a and b are integers with $b \geq 1$, then division of a by b yields integers q (the *quotient*) and r (the *remainder*) such that

$$a = qb + r, \text{ where } 0 \leq r < b.$$

Moreover, q and r are unique. The remainder of the division is denoted a mod b, and the Quotient is denoted a div b.

An integer c is a **common divisor** of a and b if c|a and c|b.

2.1.1 Greatest common divisor - A non-negative integer d is the *greatest common divisor* of integers a and b, denoted d = gcd(a, b), if
(i) d is a common divisor of a and b, and
(ii) whenever c|a and c|b, then c|d.
Equivalently, gcd(a, b) is the largest positive integer that divides both a and b, with the exception that gcd(0, 0) = 0.

2.1.2 Prime and Composite Numbers

Two integers a and b are said to be relatively prime or co-prime if gcd(a, b) = 1.

An integer $p \geq 2$ is said to be **prime** if its only positive divisors are 1 and p.

Otherwise, p is called **composite**.

If p is prime and p|ab, then either p|a or p|b (or both).

There are an infinite number of prime numbers.

2.2 Fundamental theorem of arithmetic – Every integer $n \geq 2$ has a factorization as a Product of prime powers:

n = p1^e1* p2^e2*……*pk^ek

Where the pi are distinct primes, and the ei are positive integers. Furthermore, the factorization is unique up to rearrangement of factors.

2.3 The integers modulo n – Let n be a positive integer. If a and b are integers, then a is said to be congruent to b **modulo** n, written $a \equiv b \pmod{n}$, if n divides (a − b). The integer n is called the modulus of the congruence.

2.3.1 Properties of congruence - For all a, a1, b, b1, c Є Z, the following are true.

(i) $a \equiv b \pmod{n}$ if and only if a and b leave the same remainder when divided by n.

(ii) (*Reflexivity*) $a \equiv a \pmod{n}$.

(iii) (*Symmetry*) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.

(iv) (*Transitivity*) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

(v) If $a \equiv a1 \pmod{n}$ and $b \equiv b1 \pmod{n}$, then $a + b \equiv a1 + b1 \pmod{n}$ and $ab \equiv a1b1 \pmod{n}$.

2.3.2 Equivalence class - The equivalence class of an integer a is the set of all integers congruent to a modulo

n. From properties (ii), (iii), and (iv) above, it can be seen that for a fixed n the relation of Congruence modulo n partitions Z into equivalence classes. Now, if a = qn + r, where

$0 \leq r < n$, then $a \equiv r \pmod{n}$. Hence each integer a is congruent modulo n to a unique integer between 0 and n−1, called the *least residue* of a modulo n. Thus a and r are in the same equivalence class, and so r may simply be used to represent this equivalence class.

2.3.2 Multiplicative inverse - Let a Є Zn. The **multiplicative inverse** of a modulo n is an integer x Є Zn such that $ax \equiv 1 \pmod{n}$. If such an x exists, then it is unique, and a is said to be *invertible*, or a *unit*, the inverse of a is denoted by a^−1.

Let a, b Є Zn. *Division* of a by b modulo n is the product of a and b−1 modulo n, and is only defined if b is invertible modulo n.

Let a Є Zn. Then a is invertible if and only if gcd(a, n) = 1

2.4 Rings:

2.4.1 Definition - A *ring* (R, +, x) consists of a set R with two binary operations arbitrarily denoted + (addition) and x (multiplication) on R, satisfying the following axioms.

(i) (R, +) is an abelian group with identity denoted 0.

(ii) The operation x is associative. That is, a x (b x c) = (a x b) x c for all a, b, c Є R.

(iii) There is a multiplicative identity denoted 1, with $1 \neq 0$, such that 1 x a = a x 1 = a for all a Є R.

(iv) The operation x is *distributive* over +. That is, a x (b + c) = (a x b) + (a x c) and (b + c) x a = (b x a) + (c x a) for all a, b, c Є R.

The ring is a *commutative ring* if a x b = b x a for all a, b Є R.

The set of integers Z with the usual operations of addition and multiplication is a commutative ring.

The set Zn with addition and multiplication performed modulo n is a commutative ring.

An element a of a ring R is called a *unit* or an *invertible element* if there is an element b Є R such that a x b = 1.

The set of units in a ring R forms a group under multiplication, called the *group of units* of R.

2.5 Fields:

2.5.1 Definition - A *field* is a commutative ring in which all non-zero elements have multiplicative inverses.

The set of integers under the usual operations of addition and multiplication is not a field, since the only non-zero integers with multiplicative inverses are 1 and−1. However, the rational numbers Q, the real numbers R, and the complex numbers C form fields of characteristic 0 under the usual operations.

Zn is a field (under the usual operations of addition and multiplication modulo n) if and only if n is a prime number. If n is prime, then Zn has characteristic n. If the characteristic m of a field is not 0, then m is a prime number.

2.5.2 Subfield - A subset F of a field E is a *subfield* of E if F is itself a field with respect to the operations of E. If this is the case, E is said to be an *extension field* of F.

2.6 Polynomial Rings:

2.6.1 Definition - If R is a commutative ring, then a *polynomial* in the indeterminate x over the ring R is an expression of the form $f(x) = a_n x^n + \ldots\ldots\ldots\ldots + a_2 x^2 + a_1 x + a_0$ where each $a_i \in R$ and $n \geq 0$. The element a_i is called the *coefficient* of x^i in f(x).

The largest integer m for which $a_m \neq 0$ is called the *degree* of f(x), denoted deg f(x), a_m is called the *leading coefficient* of f(x). If $f(x) = a_0$ (a *constant polynomial*) and $a_0 \neq 0$, then f(x) has degree 0. If all the coefficients of f(x) are 0, then f(x) is called the *zero polynomial* and its degree, for mathematical convenience, is defined to be −1. The polynomial f(x) is said to be *monic* if its leading coefficient is equal to 1.

If R is a commutative ring, the *polynomial ring* R[x] is the ring formed by the set of all polynomials in the indeterminate x having coefficients from R. The two operations are the standard polynomial addition and multiplication, with coefficient arithmetic performed in the ring R.

Let f(x) Є F[x] be a polynomial of degree at least 1. Then f(x) is said to be *irreducible over* F if it cannot be written as the product of two polynomials in F[x], each of positive degree.

If g(x), h(x) Є F[x] then h(x) *divides* g(x), written h(x)|g(x), if g(x) mod h(x) = 0.

If g(x), h(x) Є F[x], then g(x) is said to be *congruent to* h(x) *modulo* f(x) if f(x) divides g(x) − h(x). This is denoted by g(x) ≡ h(x) (mod f(x)).

2.6.2 Properties of congruence - For all g(x), h(x), g1(x), h1(x), s(x) Є F[x], the following
are true.

(i) g(x) ≡ h(x) (mod f(x)) if and only if g(x) and h(x) leave the same remainder upon division by f(x).
(ii) (Reflexivity) g(x) ≡ g(x) (mod f(x)).
(iii) (Symmetry) If g(x) ≡ h(x) (mod f(x)), then h(x) ≡ g(x) (mod f(x)).
(iv) (Transitivity) If g(x) ≡ h(x) (mod f(x)) and h(x) ≡ s(x) (mod f(x)), then g(x) ≡ s(x) (mod f(x)).
(v) If g(x) ≡ g1(x) (mod f(x)) and h(x) ≡ h1(x) (mod f(x)), then g(x) + h(x) ≡ g1(x) + h1(x) (mod f(x)) and g(x)h(x) ≡ g1(x)h1(x) (mod f(x)).

Let f(x) is a fixed polynomial in F[x]. The *equivalence class* of a polynomial g(x) Є F[x] is the set of all polynomials in F[x] congruent to g(x) modulo f(x). From properties (ii), (iii), and (iv) above, it can be seen that the relation of congruence modulo f(x) partitions F[x] into equivalence classes. If g(x) Є F[x], then long division by f(x) yields

unique polynomials q(x), r(x) Є F[x] such that g(x) = q(x)f(x)+r(x), where deg r(x) < deg f(x).

Hence every polynomial g(x) is congruent modulo f(x) to a unique polynomial of degree less than deg f(x). The polynomial r(x) will be used as representative of the equivalence class of polynomials containing g(x).