Free essay on cryptography

Sociology, Community

According to Stanoyevitch (2010), cryptography refers to one of the oldest branches of pure mathematics that primarily deal with the study of integers. It deals with the prime numbers and also the properties of the objects which are made out of the integers like the algebraic integers. Cryptography is a very important tool for protecting information from unauthorized access in the computer systems. Currently, finite fields are becoming very vital in cryptography. Most cryptographic algorithms depend heavily on the properties of the finite fields especially the elliptic curve cryptography and the Advanced Encryption Standard (AES). The most important concepts of the number theory which are mostly used include the Euclidian algorithm, divisibility and modular arithmetic.

In the division algorithm, for a positive integer n, and any other integer which is not negative a, when a is divided by n, there is an integer quotient q, and an integer remainder r which follow the relationship of a= qn+r, and where 0 <= r < n; q= floor (a/n). This is called the division algorithm. The remainder r is mostly called the residue. When one is given a and the positive number n, it is very possible to calculate the q and r which satisfy the relationship which precede it. This is done by representing the integers in a number line where a falls somewhere on the line. Starting from 0 and proceeding to n, the 2n up to qn such that qn <= a and (q+1) n> a. the distance that exists between qn and a is the r. This is used to find the unique values of q and r.

One of the fundamental techniques of the number theory is the Euclidean algorithm. This is a simple procedure for calculating the greatest common divisor of any two positive integers. It uses the notation of gcd (a, b) to mean the greatest common divisor of two numbers a and b. A positive number c can be said to be the greatest common divisor of both a and b if it is a divisor of both and any divisor of a and b is a divisor of c. Mathematically also, gcd(0, 0)= 0. Two integers are said to be relatively prime if they have only one common positive integer factor which is 1. This is written as GCD (a, b)= 1 .

In the modular arithmetic, only the remainder or the residue is used in the calculations following division by some modulus. The results that have the same remainder can be said to be equivalent. When given a positive integer n and a number which is not negative a, when a is divided by n, the result is an integer quotient q and an integer remainder r. Modulo operator, which is written as a mod n, can be defined as the remainder when a is divided by n. b can be referred to as a residue of a mod n because with integers, it is possible to write a= qn + b. In most cases, the smallest positive remainder is chosen as the residue. This can be written as 0 <= b <= n-1. This process is called modulo reduction. Two integers are congruent modulo n when (a mod n) = (b mod n) . The (mod n) operator maps the entire integers into the set of integers {0, 1,.(n-1)}, which is denoted as Zn. This is called the residue classes (mod n) or the set of residues. Arithmetic operations can be performed within the confines of that set and this technique is referred to as the modular arithmetic. The process of finding the smallest integer which is not negative to which k is congruent modulo is referred to as reducing k modulo n. . Fields, rings and groups are the basic elements of abstract or modern algebra. Abstract algebra deals with the sets whose elements can be used algebraically, i. e. two elements of a set can be combined in several ways to obtain a third element if the set. A group can be described as the set of elements with a binary operation. Exponentiation can be defined as a repeated application of operator. A group is said to be cyclic when every element is a power of another constant element. A ring is a set where addition, subtraction and multiplication can occur without leaving the set. It should also obey both associative and distributive laws. A field is a set where addition, subtraction and multiplication and division without leaving the set and division is defined by the rule a/b = a (b–1) . According to Stallings, W. (2011), finite fields play a very important role in various cryptographic algorithms. It can be demonstrated that the number of elements in the field or the order of finite field must be a positive power and these are called Galois fields. Cryptography is an influential tool in modern technology because it helps in protecting computer systems; it is essential in information security aspects such as authentication, maintaining data integrity, and protecting user's privacy. Over the years, cryptography has become increasingly complex as the number of applications applying the technique has become widespread. However, cryptography has been faced with legal issues, which make it difficult to enforce the law when a cryptography-related crime has been committee with defendants arguing that their constitutional rights are violated. Altogether, cryptography will continue to be an indispensable tool in the coming decades.

References

Delfs, H., & Knebl, H. (2007). Introduction to Cryptography: Principles and Applications. London: Springer.

Stallings, W. (2011). Cryptography and Network Security: Principles and

Practice. Washington D. C.: Prentice Hall.

Stanoyevitch, A. (2010). Introduction to Cryptography with Mathematical Foundations and Computer Implementations. Boca Raton, FL: CRC Press.