Cryptography and network security essay example

Sociology, Communication

Abstract

The document below is an outline essay on the following topics:

Basic concepts in number theory and finite fields, Divisibility and the division algorithm, the euclidena algorithm, modular artithmetic, groups, rings and fields, finite fields of the form, polynomial arithmetic, Finite fields of the form, Advance encryption standard, The origins AES, AES Structure, AES round functions and AES Key expansion.

Essay

Divisibility

Mathematics involves many rules as well as formulae which are followed to derive the exact outcomes. One such mathematic term is ‘ divisibility’. When a number is able to divide with another number without any reminder, it is known as the divisibility of the number. For example 9 is divisible by 3 (9/3 = 0) as the reminder is 0. However there are many divisibility rules applicable while dividing numbers.

Division Algorithm

An algorithm in which two given integers, ‘ n’ and ‘ m’ compute their quotient and reminder with result of division is known as Division algorithm.

q= n/d where q= quotient; n= numerator (dividend); d= denominator (divisor)

Some algorithms maybe done by hand, while others may require calculators. Division algorithms are further divided into two types known as slow division and fast division.

The Euclidean Algorithm

The Euclidean algorithm is one of the most efficient methods for computing the greatest common factor (GCF) of two positive integers, ‘ a’ and ‘ b’. Under this algorithm,

If, b/a then the GCF (a, b)= b

This holds true since no number (especially b) can have a divisor that is greater than the number itself (in case of non-negative integers only).

The algorithm starts with 2 positive integers that form into a new pair that has the smaller number and the difference between the larger and smaller number. The procedure is repeated until equal numbers are achieved. This number is then the greatest common factor of the original pair. This algorithm although mathematical, has many practical as well as theoretical uses.

Modular Arithmatic

Modular arithmetic is also known as clock arithmetic is a system for integers wherein a ‘ wrap around’ for numbers occur upon reaching its specific value known as modulus. This can be well illustrated in the use of 12 hour clock. The day is divided into periods of 12 hours. If the time was 7’o clock at the moment, after 8 hours it will be 3’o clock. Usually it would be 7+8= 15, however in a clock, the time ‘ wraps around’ after every 12 hours, i. e. after 12 it begins with 1 again. As the hour number begins after reaching 12, it is known as modulo 12. Here the number 12 is not just congruent with 12 itself, but also with 0, thus 12: 00 is also known as 0: 00 where 0= 12.

Groups, Rings and Fields

Groups, rings and fields are all a part for abstract algebra largely used in cryptology. A group is a set of elements along with operation which merges any two elements present in the set while also fulfilling the four conditions known as axioms. These axioms are, closure, identity, associativity and invertibility. One of the common examples of a group would be where a set of integers are added (operation) and its sum forms another integer.

A ring is an algebraic structure which generalizes and abstracts the arithmetic operations of addition and multiplication. It is an abelian group having a secondary binary operation. The operation is associative and distributive on the abelian group operation. The operation of abelian group is addition while the secondary binary operation is multiplication. An example of rings would be a set of integers which are a communicative ring where a times b is equal to b times a.

A field is a communicative ring where for every nonzero element; there is a multiplicative inverse, equivalently a ring wherein under multiplication, the nonzero elements form an abelian group. The common fields include the field of rational numbers, real numbers and complex numbers.

Finite Field of Form

A finite field is a field that constitutes many finite elements. Thus F4 is a field with 4 elements. The smallest finite field is F2 that consist of 0 and 1 elements. By definition, a finite field has at least two elements. It is applicable in cryptography, computer science and coding theory.

Polynomial Arithmetic

Polynomial arithmetic involves performing basic mathematic operations on the polynomials. These operations include addition, subtraction, division and multiplication. When a polynomial is added, subtracted or multiplied, it results in another polynomial, however, when it is divided, it does not result in a polynomial but instead in a complex expression called a rational expression.

Advanced Encryption Standard

In order to secure classified and sensitive data of the US Government agencies, an encryption data was established. It was developed by the US national Institute of Standards and Technology in 2001 and was based on the Rijndael cipher. The AES was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. Although initially adopted by the US government, it is now used by everyone worldwide.

The AES structure is based on the substitution-permutation network design. Unlike DES, AES does not make use of the Feistel network. AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits; called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds.

The following functions are performed by the main loop of AES • SubBytes()

• ShiftRows()

• MixColumns()

• AddRoundKey()

AES Structure:

1. State ← x

2. State← AddRoundKey (x, K1)

3. for i ←1 to Nr-1 do

4. State← SubBytes (State)

5. State← ShiftRows (State)

6 State← MixColumns (State)

7. State← AddRoundKey (State, Ki)

8. State← SubBytes (State)

9. State← ShiftRows (State)

10. State← AddRoundKey (State, KNr+1)

Key Schedule: S : {0, 1}t → {0, 1}(Nr+1)t

K ⊢→ (K1, ., KNr+1)

References:

John H. Conway, The Sensual (Quadratic) Form, Carus Mathematical Monographs, vol. 26, Mathematical Association of America, Washington, DC, 1997, With the assistance of Francis Y. C. Fung. MR 98k: 11035

R. Crandall and C. Pomerance, Prime Numbers, Springer-Verlag, New York, 2001, A computational perspective. MR 2002a: 11007

Algorithms for modular elliptic curves, second ed., Cambridge University Press, Cambridge, 1997.

W. Di and M. E. Hellman, New directions in cryptography, IEEE Trans. Information Theory IT-22 (1976), no. 6, 644{654. MR 55 #10141