APPLICATION OF MODULUS THEORY TO CRYTOGRAPHIC SYSTEM

BELELA SAMUEL KOTOLA, Department of Mathematics, Debre Berhan Univesity Ethiopia

ABSTRACT

In this paper, introduce the reader to some of the fundamental notions of cryptography in a number theory context. Cryptography has long been an important issue in the realm of computers, mainly due to security needed for passwords. Security is a human issue in today's world. Cryptography is only as good as the practices of the people who use it. With the growing quantity of digital data stored, communicated by electronic data, processing system, organization like public and commercial sectors have felt the need to protect information from unwanted intrusion. These wide spread uses of electronic funds transfer has made privacy a pressing concern in most financial transaction. There for the secret communication system are needed. The complexity of cryptography effectively puts it outside the understanding of most people and so motivation for the practices of cryptographic security is not available.

KEYWORDS: *security, cryptography, modulus, communication system*

INTRODUCTION AND DEFINATION OF MODULUS THEORY

Let $m > 0$be an integer. We say that the integers a and b are congruent $modulo\ m$ if their difference $a - b$ is divisible by m we write $a \equiv b(mod\ m)$, to indicate that the integers a and b are congruent$modulo\ m$.

The number m is called the modulus and $a \equiv b(mod\ m)$ means a and b they are differ only by a factor of m. If m not divides $a - b$ we write as $a \not\equiv b\ (mod\ m)$.

Example 1: let $m = 10$ then $5 + 7 = 12 \equiv 2(mod\ 10)$ i.e 10 divides $12 - 2 = 10$

Example 2: $19 \equiv 1(mod\ 3)$ because 3divides $19 - 1 = 18$

1) RESULTS ON MODULUS THEORY

2) ELEMENTARY PROPERTIES OF CONGRUENCES

Let $n > 1$ be fixed and a, b, c and d be arbitrary integers. Then the following properties are holds.

a. $a \equiv a(mod\ n)$.
b. If $a \equiv b(mod\ n)$then$b \equiv a(mod\ n)$.
c. If $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$ then $a \equiv c(mod\ n)$.
d. If $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$ then
$a + c \equiv b + d(mod\ n)$and $ac \equiv bd(mod\ n)$.
e. If $a \equiv b(mod\ n)$, then $a + c \equiv b + c(mod\ n)$ and $ac \equiv bc(mod\ n)$.
f. If $a \equiv b(mod\ n)$, then $a^k \equiv b^k(mon\ n)$ for any positive integer k.

Proof

a. For any integer a we know that$a - a = 0 = n.0$, so that$a \equiv a(mod\ n)$.
b. If $a \equiv b(mod\ n)$ then $a - b = kn$ for some integer Hence $b - a = -(kn) = (-kn)$ and because $-k$ is an integer so $b \equiv a(mod\ n)$
c. This properties is slightly less obvious: suppose that $a \equiv b(mod\ n)$ and also $b \equiv c(mod\ n)$.Then there exist integers h and k satisfying $a - b = hn$and$b - c = kn$.

It follows that $a - c = (a - b) + (b - c) = hn + kn = (h + k)n$ which is $a \equiv c(mod\ n)$

In congruence notation:

d. In the same way, if $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$ then we are assured that $a - b = k_1 n$ and $c - d = k_2 n$ for some choice of k_1 and k_2. After adding these equations we obtain $(a + c) - (b + d) = (a - b) + (c - d)$

$\Rightarrow (a + c) - (b + d) = k_1 n + k_2 n = (k_1 + k_2)n$

Or as a congruence statement$a + c \equiv b + d(mod\ n)$

Note that $ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n$

Because $bk_2 + dk_1 + k_1 k_2 n$ is an integer, this says that $ac - bd$ is divisible by n hence

$ac \equiv bd(mod\ n)$.

The proof of e is converted by d and the fact that $c \equiv c(mod\ n)$.

Finally, we obtain property (f) by making an induction argument. The statement certainly holds for $k = 1$and we will assume it is true for some fixed k.

From (d), we know that $a \equiv b(mod\ n)$ and $a^k \equiv b^k(mon\ n)$ together imply that

$aa^k \equiv ab^k(mon\ n)$or equivalently $a^{k+1} \equiv b^{k+1}(mon\ n)$.

This is the form the statement should take for $k + 1$ and so the induction step is complete.

3) Euler Phi Function

For each positive integer m then the Euler phi function $\phi(m)$ is one if $m = 1$ and the number of positive integer less than or equal to n that are $coprime$ to m.

Theorem (Euler)

If$n \geq 1$ and $gcd(a, n) = 1$ then $a^{\phi(m)} \equiv 1(mod\ n)$

Proof

Without loose of generality let $n > 1$ and assume $a_1, a_2, \ldots, a_{\phi(n)}$ be positive integer less than n which are relatively prime to n. Since $gcd(a, n) = 1$ then the numbers $aa_1, aa_2, \ldots, a_{\phi(n)}$ are congruent to $a_1, a_2, \ldots, a_{\phi(n)} (mod n)$ but not necessary in order of appearance

Then

$aa_1 \equiv b_1 (mod\ n)$

$aa_2 \equiv b_2 (mod\ n)$

$aa_3 \equiv b_3 (mod\ n)$

$aa_4 \equiv b_4 (mod\ n)$)

$aa_{\phi(n)} \equiv b_{\phi(n)} (mod\ n)$ Where b_i are integers $a_1, a_2, \ldots, a_{\phi(n)}$ in some order taking the product of these $\phi(m)$ congruence we get

$(a.a_1)(a.a_2)(a.a_3)\ldots\ldots\ldots (a.a_{\phi(n)}) \equiv b_1.b_2 \ldots . b_{\phi(n)} (mod\ n)$

Example

Find the remainder when 2^{100} is divisible by 15

Solution:

We know that gcd (2, 15)=1 and 2>1, then by the above theorem,

$2^{\phi(15)} \equiv 1 (mod 15)$

But $4.2 = 8$

So $2^8 \equiv 1 (mod 15)$

$\Rightarrow 2^{8.12} \equiv 1^{12} (mod 15) = 2^{96} \equiv 1 (mod 15)$

But $2^4 \equiv 1\ (mod\ 15)$

$2^4.2^{16} \equiv 1.1\ (mod\ 15)$

$\Rightarrow 2^{100} \equiv 1\ (mod\ 15)$

Therefore when the number 2^{100} is divided by 15 the reminder is 1.

Theorem: (FERMAT LITTLE THEOREM)

Let p be prime number and suppose that p not divides a, where a is any integer, the

Proof

We be gain by constricting the first $p - 1$ positive multiple of a.

$i.e.\ a, 2a, 3a, 4a, 5a, \ldots\ldots\ldots\ldots\ldots\ldots (p-1)a$: No one of these numbers congruent $modulo\ p$ to any other nor is congruent to zero. There for these set of integers must be congruent $modulo\ p$ to $1, 2, 3\ldots\ldots\ldots\ldots\ldots\ldots (p-1)$ taken in some order multiply all there congruent together we find that

$a.2a.3a.4a.\ldots\ldots\ldots\ldots\ldots(p-1)a$ $1.2.3.4.\ldots\ldots\ldots\ldots(p-1)(mod\ p)$ which implies $a^{p-1}(p-1)! \equiv (p-1)!(mod\ p)$ once $(p-1)!$ is cancelled from both side. There for $a^{p-1} \equiv 1(mod\ p)$

Example

Find the reminder when 24^{1997} is divisible by 17.

Solution:

Here 17 is prime and 17 cannot divides 24.

Hence we can use the above theorem (Fermat little theorem).

$24^{16} \equiv 1(mod\ 17)$

$\Rightarrow 24^{16.124} \equiv 1(mod\ 17) = 24^{1984} \equiv 1(mod\ 17)\ldots\ldots(1)$

But $24^2 \equiv 15(mod\ 17)$

$\Rightarrow 24^4 \equiv 15.15(mod\ 17) = 24^4 \equiv 4(mod\ 17)$

$\Rightarrow 28^8 \equiv 16(mod\ 17)$

$\Rightarrow 24^{12} \equiv 13(mod\ 17)$

$\Rightarrow 24^{13} \equiv 6(mod\ 17)$..... (2)

from (1) and (2)

$24^{1997} \equiv 6(mod\ 17)$.

Therefore 6 is the remainder when 24^{1997} is divisible by 17.

Corollary

1. If p is a prime number such that can't divided by p then $a^p \equiv a(mod\ p)$ for any integer.
2. If p is any prime number and a is any integer, then $a^p \equiv a(mod\ p)$

Proof

1. **case1**: if p not divides a by Fermat Little theorem $a^p \equiv a(mod\ p)$

case2: if p/a then $\frac{p}{a(a^{p-1}-1)}$ which leads to the truth $\frac{p}{a^p-a}$

$\Rightarrow a^p \equiv a(mod\ p)$

2. If p and q are distinct prime number with $a^p \equiv a(mod\ q)$ and $a^q \equiv a(mod\ p)$ then $a^{pq} \equiv a(mod\ pq)$

$\Rightarrow \frac{p}{a^{pq}-a}$ Similarly $\frac{q}{a^{pq}-a} \Rightarrow \frac{pq}{a^{pq}-a}$

HISTORICAL BACK GROUND OF CRYPTOGRAPHY

4) Definition of Cryptography

The word cryptography is come from two Greek words. Which are ''kryptos'' and ‘‘graphei’’.Krypto means hidden and graphei means written. Cryptography is the design and implementation of secrecy system. The study of secrecy is called cryptology. The information or the message we wants to send by using the technique of Cryptography secretly is known as plain text. After the transformation to be secret form, message is called cipher text. Device used to transform the plain text to cipher text is called cipher. We can also define cipher by the language of cryptography as code.

The process of converting plain text into cipher text is called encrypting or enciphering. The rivers process of changing cipher text into plain text is known as decycrpting or deciphering. The study of system or method of breaking cipher is called cryptanalyst.

Classically the making and breaking of secret codes has usually been confined to diplomatic and military practices in the past time. With the growing quantity of digital data stored, communicated by electronic data, processing system, organization like public and commercial sectors have felt the need to protect information from unwanted intrusion. These wide spread uses of electronic funds transfer has made privacy a pressing concern in most financial transaction. There for the secret communication system are needed'

As we have saw in the privies chapter Cryptography is the Greek word which tell us it is the creation of Greek. However one of the earliest cryptography systems was used bay Roman emperor Julius caeser 50 B.C. The other famous poly alphabetic cipher was published by the French cryptologist Blaise de vegenere (1528-1996). In 1977 R.RivestA. Shamir and L.Adleman proposed a key crypto system. In 1929 Lester Hill devised away ensures the greatest security in alphabet substitution. Another influential none alphabetic cipher was devised 1917 by Gilbert S.verman. In the next chapter we will see the detail of each inventer’s methods one by one

CRYTOGRAPHIC SYSTEM

5) Julius Caesar System

Caesar was the great Roman's emperor who used cryptography earlier around 50 B.C. Caesar wrote to Marcus Cicero using rudimentary substitution cipher in which each latter of the alphabet is replaced by the letter that occurs three places down the alphabet. With the last three letters cycled back to the first three letters. If we write the cipher text equivalent underneath the plain text letters, the substitution alphabet for the Caesar cipher is given by:

plain text; A B C D E F G H I J K L M N O P Q R S T U V W X Y Z and the corresponding

cipher text; D E F G H I J K L M N O P Q R S T U V W X Y Z A B C (i.e. A substitute by D ,B Substituted by E, Z substitute by C and so on.)

Example

If someone want to send the message NUMBER THEORY IS INTERSTING COURSE by using Caesar Cryptographer system the message will encrypted as QXPEHU WKHRUB LV LQWHUHV WLQJ FRXUVH.

The Caesar cipher can be described easily using congruence theory. Any plain text is first expressed numerically by translating the characters of the text into digits by means of some correspondence such as following.

A	B	C	D	E	F	G	H	I	J	K	L	M
	N											
00	01	02	03	04	05	06	07	08	09	10	11	12
	13											
O	P	Q	R	S	T	U	V	W	X	Y	Z	
14	15	16	17	18	19	20	21	22	23	24	25	

If P is the digits equivalent of a plain text letters and C is the digital equivalent of the corresponding cipher text, then

$$C \equiv P + 3(mod26)$$

Example

The example we have saw above NUMBER THEORY IS INTERESING COURSE has the numerical equivalent

13 20 12 01 04 17 19 0714 17 2408 1818 13 19 04 17 19 08 13 0602 14201718 04

Using the congruence $C \equiv P + 3(mod26)$the above text will be converted as

$C = 13 + 3 \equiv 16(mod26)$

$C = 20 + 3 \equiv 23(mod26)$

$C = 12 + 3 \equiv 15(mod26)$

$C = 01 + 3 \equiv 04(mod26)$ and so on

Finally the message will be have the following numerical form. 16 2315040720 211017200111 21111622072020221221116 09051723202107 which is equivalent to *QXPEHU WKHRUB LV LQWHUHV WLQJ FRXVH*

To recover the plain text the procedure is simply reversed by means of the congruency $P \equiv C - 3(mod26)$.

An encryption technique in which each letter of the original message is replaced by the same cipher substitute is known as a mono alphabetic cipher.

Such cryptographic systems are extremely vulnerable to statically methods of attach because they preserve the frequency or relative commonness of individual letters.

BLAISED DE VEGENERE (POLYALPHABETIC CIPHER)

In poly alphabetic cipher, plain text letter has more than one cipher text equivalent. The French cryptographer Blasé de-vigenere introduces the most famous example of poly alphabetic cipher in (1528-1996) in his Tracie de chiffres of 1986.

To implement this system, the communicating parties agree on an easily remembered word or phrase with the standard alphabet number from

$A = 00$ to $Z = 25$.

The digital equivalent of the key word is repeated as many times as necessary beneath that of the plain text message.

The message is enciphered by adding modulo 26, each plain text. The process may be illustrated with the key word MATHS whose numerical version is 12 00 19 07 18 if someone wants to send the message GOOD LUCK, whose numerical values 06 14 14 03 11 20 02 10 they do the following.

06 14 14 03 11 20 02 10

12 00 19 07 18 12 00 19 then add column *modulo* 26.

Then the plain text will be 18 14 07 10 03 22 02 03 or converted to the text *SOGK EWCD*.

In general any sequence of n letters with numerical equivalents $b_1, b_2, b_3, b_4, \ldots \ldots b_n$, provide that $00 < b_i < 25$ will serve as key word. The plain text message is expressed as recursive blocks $P_1, P_2, P_3, P_4, \ldots\ldots\ldots\ldots P_n$ of n two digits integers P_i and then converted to cipher text blocks $C_1, C_2, C_3, C_4, \ldots\ldots\ldots\ldots C_n$ by means of congruence

$C_i \equiv P_i + b_i(mod\ 26)$ for $1 < i < n$.

Decryption carried out by using the relations $P_i \equiv C_i - b_i (mod\ 26)$ for $1< i < n$.

For insistence $18 - 12 \equiv 06 (mod\ 26)$ =G. $14 - 00 \equiv 14 (mod\ 26)$and so on .

Note

In this cryptographic system the letter that is double at plain text may not be exist as double at cipher text.

For example the letter ''O'' in the above plain text is double but in the cipher text it is not longer doubled.

Limitation of vigenere's approach

Once the length of the key word has been determined a coded message can be regarded as a number of separate mono alphabetic ciphers, each subject to strength forward frequency analysis.

A variant to the continued repetition of the key word is called running key, random assignment of cipher text letters to plain text letters.

Strong side of vigenere's approach

A clever modification that vigenere contrived for his poly alphabetic cipher is currently called auto key or automatic key.

This approach makes use of the plain message itself in constructing the encryption key.

The procedure is by start off the key word with a short seed or primer (generally a single letter) followed by the plain text, whose ending is instructed by the length of the seed. This auto key enjoyed considerable popularity in the 16thand 17th centuries.

Example

Assume the message is COME ON it is going to be encrypted by using the letter D as a seed. So the word will be DCOMEO .Then when both the plain text and the key word changed to its equivalent numerical values respectively, we have the following.

Plain text: $02\ 14\ 12\ \ 04\ 14\ 13$

Key word: $03\ 02\ 14\ 12\ \ 04\ 14$ then add the two rows diagonally modulo 26 we obtain $05\ 16\ 00\ 16\ \ 18\ 01$ whose have the text equivalent $FQAQ\ SB$.

Deciphererment is achieved by returning the numerical form of both the plain text and its cipher text. Let the plain text has digital equivalent $P_1, P_2, P_3, P_4, \ldots\ldots\ldots P_n$and the cipher text $C_1, C_2, C_3, C_4, \ldots\ldots\ldots C_n$if S indicates the seed then the first plain text number is

$P_1 \equiv C_1 - S(mod\ 26)$and the K^{th}plain text becomes $P_k \equiv C_k - P_{k-1}(mod\ 26)$ provided that k is between 2 and n.

For instance in our above example $FQAQ\ SB$ is become

$P_1 \equiv C_1 - S(mod\ 26) = 05 - 02(mod\ 26) = 02(mod\ 26) = C.$

The second letter can be changed as

$P_2 \equiv C_3 - S(mod\ 26) = 00 - 14(mod\ 26) = 12(mod\ 26)$ the next letter are also can be solved in the same manner.

6) LESTER HILL

Hill was an assistance professor of mathematics at Hunter University. He devised away to ensure a greater security in alphabetic substitution in 1929.

Hill's approach is to divided the plain text message in to blocks of n letters (possibly filling out the last block by adding "dummy “letters such as "x”)then encrypt block by block using system of n linear congruence’s in n variables in its simplest form. When n=2 the procedure takes two successive letters and transform their numerical equivalents P_1P_2 in to a block of C_1C_2 of cipher text number via the pair of congruence’s.

$C_1 \equiv aP_1 + bP_2(mod\ 26)$

$C_2 \equiv cP_1 + dP_2(mod\ 26)$

To permit decipherment the four coefficients must be selected so that $gcd(ad - dc, 26) = 1$.

Example

To use Hill's cipher, let us use the congruence

$C_1 \equiv 2P_1 + 3P_2(mod\ 26)$

$C_2 \equiv 5P_1 + 8P_2(mod\ 26)$

We took these four coefficients due to $2x8 - 3x5 = 16 - 15 = 1$ which is relatively prime with 26.

To encrypt the message $HOME$ the first two letter have numerical values of $07\ 14$ is replaced by $C_1 \equiv 2x07 + 3x14 = 56 \equiv 04(mod26) = E$

$C_2 \equiv 5 * 07 + 8x14 = 147 \equiv 04(mod\ 26) = R$

The second two letters are numerically $12\ 04$ should be replaced by

$C_1 \equiv 2x12 + 3x04 = 36 \equiv 10(mod\ 26) = K$

$C_2 \equiv 5x12 + 8x04 \equiv 92(mod\ 26) \equiv 14(mod26) = O$

So the message HOME is transfer in to the message ERKO by the system of Hill's.

Decipherment can be done by solving the original system of congruence for P_1andP_2 in terms of C_1andC_2. Hence the plain text block P_1P_2 can be recovered from the cipher text block C1C2 by means of the congruence.

$P_1 \equiv dC_1 - bC_2(mod26)$ and $P_2 \equiv aC_1 + C_2(mod26)$

So the message $ERKO$ can be deciphered by taking the first two letters ER can be

$P_1 \equiv 8x04 - 3x17(mod\ ) \equiv 07(mod\ 26) = H$

$P_2 \equiv -5x04 + 2x17(mod\ 26) \equiv 14(mod\ 26) = O$

And the second two letters are KO can be

$P_1 \equiv 8x08 - 3x14(mod\ 26) \equiv 12(mod\ 26) = M$

$P_2 \equiv 2x08 - 5x14(mod\ 26) \equiv 04(mod\ 26) = E$

Note

When we use this method we should remember that the words which have the length of prime number can be encrypted by adding one or more letters at the end. During deciphering the added letters shall be ignored.

THE KNAPSACK CRYPTO SYSTEM

A public key Cryptosystem also can be based on the classic problem in combinatory known as the knapsack problem or the subset sum problem. This problem is stated as follows: Given knapsacks of volume V and n items of various volumes. $ß_1, ß_2 \ldots\ldots\ldots\ldots ß_n$, can be a subset of these items be found that will completely fill the knapsack? There is an alternative formulation.

Example integers $ß_1, ß_2 \ldots\ldots\ldots\ldots ß_n$ and the sum V solve the equation

$V = ß_1x_1 + ß_2x_2 + \ldots\ldots\ldots\ldots ß_nx_n$ where $x_i = 0$for $i = 1, 2, 3, \ldots\ldots n.$

To the problem depending on the choice of the sequence $ß_1, ß_2 \ldots\ldots\ldots\ldots ß_n$ and the integer V, there might be no solution or more than one solution.

For instance the knapsack problem$22 = 3x_1 + 7x_2 + 9x_3 + 11x_4 + 20x_5$ has no solution and the knapsack problem $27 = 3x_1 + 7x_2 + 9x_3 + 11x_4 + 20x_5$ has two distinct solution namely $x_1 = x_5 = 0\ , x_2 = x_3 = x_4 = 1$ and $x_2 = x_5 = 1\ , x_1 = x_3 = x_4 = 0.$

Finding a solution to a randomly chosen Knapsack problem is notoriously difficult. It is so difficult to solve by searching all the second possibilities for$x_1,\ x_2,x_3.\ .\ .x_n$ spatially for n greater than 100 and so.

However if the sequence $ß_1,ß_2.....ß_n$ happens to have some spatial properties, the knapsack problem becomes much easier to solve. The sequence $ß_1,ß_2.....ß_n$ is called super increasing when each $ß_i$ are greater than the sum of all the preceding ones.

$i.e.ß_i > ß_1 + ß_2 + ß_3 + ... + ß_{i-1} i = 1,2,3,.....n$

Knapsack problem based on super increasing sequence are uniquely solvable whenever they are solvable at all.

For example let us consider sequence which is the super increasing

a. $1,\ 2,\ 4,\ 16 ....., 2n$

b. $1,\ 4,\ 6,\ 13,\ 25$

Example

Let us solve the super increasing Knapsack problem.

$28 = 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5$

Start with the largest coefficient in the equation which is 41.Here 41>28 $\Longrightarrow x_5 = 0$, that means it cannot be part of our subset sum. The next largest coefficient is 20 with 20<28 and now the sum of the preceding coefficient is

$3 + 5 + 11 = 18 < 28$

So that these cannot fill the knapsack, therefore 20 must be included in the sum, and so on $x_4 = 1$ knowing the value of $x_4$and x_5 the original problem can rewritten as

$28 = 3x_1 + 5x_2 + 11x_3 + 20$

$28 - 20 = 3x_1 + 5x_2 + 11x_3$

Now repeating our earlier procedure the largest coefficient is

$11 > 8$ so $x_3 = 0$

Then the problem will reduced into $8 = 3x_1 + 5x_2$

Which implies $x_1 = x_2 = 1$.This identifies a subset of $3, 5, 11, 20, 41$ having the desired sum $3 + 5 + 20 = 28$.

Generally when we wish to solve $V = ß_1x_1 + ß_2x_2 + ... ß_nx_n$ where $ß_1,ß_2.....ß_n$is a super increasing sequence of integers. Assume that V can be

obtained by using some subset of the sequence of integers, so that V is not larger than the sum

$ß_1 + ß_2 + \ldots\ldots\ldots\ldots + ß_n$.Working from right to left in our sequence we, begin by letting x_n=1 if v is greater than or equal to $ß_n$ and $x_n = 0$ if $v < ß_n$. then obtain $x_{n-1}, x_{n-2} \ldots, x_1$ in turn by choosing $x_i = 1$ if $V - (a_{i+1} + a_{i+2} + 1 + \ldots\ldots\ldots\ldots\ldots\ldots a_n x_n) > a_i$ and $x_i = 0$ if $V - (a_{i+1} + a_{i+2} + 1 + \ldots\ldots\ldots\ldots\ldots\ldots a_n x_n) < a_i$

With this algorithm, knapsack problems using super increasing sequence can be solved quite readily

7) R. MERKLE AND M.HELLMAN CONCEPTS

In 1978 they introduce a public-key cryptosystem based on the knapsack problem.

It works as follow. Atypical user of the system starts by choosing a super increasing sequence $ß_1, ß_2 \ldots\ldots\ldots\ldots ß_n$. Now select a modulus $m > 2ß_n$ and multiplier ß with $0 < ß < m$ and $gcd(ß, m) = 1$

This ensures that the congruence $ßx \equiv 1 (mod\ m)$ has unique solution, say

$x \equiv c (mod m) i = 1,2,3,4\ldots\ldots, n$ where $0 < b_i < m$. Carrying out this last transformation generally destroys the super increasing properties enjoyed by the $ß_i$.

The user keeps secret the original sequence $ß_1, ß_2 \ldots\ldots\ldots\ldots ß_n$ and the number m messages to the employs the publicly available sequence as the encryption key. The sender begins by converting the plain text message in to string m of 0's and 1's using the binary equivalent of letters as bellow.

$A = 00000$	$O = 01110$
$B = 00001$	$P = 01111$
$C = 00010$	$Q = 10000$
$D = 00011$	$R = 10001$
$E = 00100$	$S = 10010$
$F = 00101$	$T = 1OO11$
$G = 00110$	$U = 10100$
$H = OO111$	$V = 10101$
$I = 01OOO$	$W = 10110$
$J = 01001$	$X = 10111$
$K = 01010$	$Y = 11000$

$L = 01011 \qquad Z = 11001$

$M = 01100 N = 01101$

The procedure we should follow to use this system

First the message would be converted into the numerical representation. The string is then split in to the blocks of n binary digits with the last block being filled out with 1's at the end if necessary.

The public encrypting sequence $b_1, b_2, b_3, b_4, \ldots\ldots b_n$ it is next used to transform a given plain text (say) $x_1, x_2, x_3, x_4, \ldots\ldots x_n$, in to the sum $S = b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 + \cdots + b_nx_n$

The number S is the hidden information that the sender transmit over communication channel, which is presumed to be insecure.

Notice that because each x_i is either 0 or 1, the problem of recreating the plain text block from S is equivalent to solving an apparently difficult knapsack problem. It is difficult due to the reason that the sequence $b_1, b_2, b_3, b_4, \ldots\ldots b_n$ is not necessarily super increasing. On the first impression, the intended recipient and any eavesdropper are faced with the same task. However with the aid of the private decryption key, the recipient can change the difficult knapsack problem in to an easy one.

No one without the private key can make this change.

Knowing c and m, the recipient computes.

S≡CS (mod m) provide that S is the number that is greater than or equals to zero and less than m.

Let us consider the example with n=5. suppose that typical user of this cryptosystem selects key the super increasing sequence 3,5,7,10,21 the modulus m=85 and the multiplier ß=22 each member of the super j increasing sequence is multiplied by 22 and reduced modulo 40 to yield 26,30,34,20,22.

This is the encryption key that the user submits to the public directory.

Someone who wants to send HELP US

First change the text HELP US in to the strings of 0's and 1's.

The word has the numerical equivalent

M=00111 00100 01011 01111 10100 10010

The string then broken in to blocks of digits, in the current case blocks of length 5.Using the listed public key to encrypt, the sender transform the successive blocks into

47*0+50*0+59*1+30*1+19*1=108

47*0+50*0+59*1+30*0+19*0=59

47*0+50*1+59*0+30*1+19*1=99

47*0+50*1+59*1+30*1+19*1=158

47*1+50*0+59*1+30*0+19*0=106

47*1+50*0+59*0+30*1+19*0=77

The transmitted cipher text consists of the sequence of positive integers will be

108 59 99 158 106 77

To read the message, the legitimate receiver first solves the congruence

44x≡1 (mod 85) yielding x≡29 (mod 85)

Then each cipher text number is multiply by 29 and reduced to modulus 85, to produce a super increasing knapsack problem.

For instance 108 is converted to 72 because 108.29≡72 (mod 85) and the corresponding knapsack problem is $72 = 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5$. The procedure for handling super increasing knapsack problem quickly produces the solution $x_1 = x_2 = x_3 = x_4 = x_5 = 1$in this way the first block will be 00111 of binary equivalent of lain text is recovered.

CONCLUSION

In recent times, due to the Internet, it has taken on more importance with sensitive information of all kinds, such as credit card numbers, passing over media which are fairly easy to monitor by unintended third parties. Security in the Internet is improving. The increasing use of the Internet for commerce is improving the deployed technology to protect the financial transactions. Extension of the basic technologies to protect multicast communications is possible and can be expected to be deployed as multicast becomes more widespread.

Control over routing remains the basic tool for controlling access to streams. Implementing particular policies will be possible as multicast routing protocols improve. Cryptography is a tool which may alleviate many of the perceived problems of using the Internet for

communications. However, cryptography requires the safe implementation of complex mathematical equations and protocols, and there are always worries about bad implementations. A further worry is that users are integral to securing communications, since they must provide appropriate keys.

REFERENCE

[1] D. Stinson, Cryptography, Theory and Practice, CRC Press, Second edition, 2000. [10] W. Stallings, Cryptography and Network Security: Principles and Practice, Second edition, Prentice Hall, 1999. [11] . J. Menezes and P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[2] ESTREAM - The ECRYPT Stream Cipher Project, http://www.ecrypt.eu.org/stream/ [6] Y. Nawaz and G. Gong, WG: A family of stream ciphers with designed randomness properties, Information Sciences, Vol. 178, No. 7, April 1, 2008, pp. 1903-1916.

[3] G. Gong, K. C. Gupta, M. Hell, andY. Nawaz, Towards a General RC4-like Key stream Generator, SKLOIS Conference on Information Security and Cryptology (CICS05), December15-17, Beijing, China. Springer-verlag, 2006.

[4] JamesJ.Tattersall, Elementary number theory in nine chapters.

[5] Jeffrey Hoffstein Jill pipher JophesH. Silverman: Introduction to mathematical cryptography.

[6] National Bureau of Standards, Data Encryption Standard, FIPS Publication 46, U.S. Department of Commerce, 1977.