SOLVING KNAPSACK PROBLEM BY USING SUPER-INCREASING SEQUENCE METHOD

[1]K.Subbanna,[2]P.Moulali,[3]Ch.Venkateswarlu
[1]*Assistant Professor, Department of Mathematics*
[2]*Assistant Professor, Department of Computer Science*
[3]*Assistant Professor, Department of Statistics*
[1,2,3]*Shri Gnanambica Degree College, Madanapalle, Andhra Pradesh-517325, India*

Abstract :In this Paper, we will study the Knapsack Problem whose solutions are obtained by using super-Increasing Sequence with some basic number theory properties like fundamental theorem of arithmetic, modular arithmetic, modular multiplication, congruence's, Pair of relatively primes, Inverse modulo etc., with counter example, for a given sequence the knapsack problem solution will be presented some types they are inspection method, the ciphers describe based on transformed super-increasing sequences, the enciphering and deciphering procedures of the knapsack cipher based on modular arithmetic and a multiplicative knapsack problem will be solved by analytically.

Keywords – Super increasing sequence, fundamental theorem of arithmetic, modular arithmetic; modular multiplication, pair of relatively primes, Inverse modulo, encipher and decipher

I. INTRODUCTION

The **knapsack problem** is a problem in combinatorial optimization: Given a set of items, each with a weight and a value, determine the number of each item to include in a collection so that the total weight is less than or equal to a given limit and the total value is as large as possible. It derives its name from the problem faced by someone who is constrained by a fixed-size knapsack and must fill it with the most valuable items. The problem often arises in resource allocation where the decision makers have to choose from a set of non-divisible projects or tasks under a fixed budget or time constraint, respectively.

The knapsack problem has been studied for more than a century, with early works dating as far back as 1897[1].The name "knapsack problem" dates back to the early works of the mathematician Tobias Dantzig (1884–1956) [2], and refers to the common place problem of packing the most valuable or useful items without overloading the luggage.Publickey cryptography was invented by Whitfield diffie, Martin Hellman and Ralph Merkle in 1970 [3, 4]. The cipher system was invented by Merkle and Hellman [4], Shamir [4,6] has shown that knapsack ciphers are not satisfactory for public-key cryptography, A method for obtaining digital signatures and public-key cryptosystems invented by R. L. Rivest, A. Shamir, and L. M. Adleman [5],Shamir investigated how to share secret[6],

II. GENERAL METHOD/INSPECTION METHOD

Given a set of positive integers $a_1, a_2, a_3, ...a_n$ and a Sum **S** of a subset of these integers, the knapsack problem asks which of these integers add together to give S. Another way to phrase the knapsack problem is to ask for the values of $x_1, x_2, x_3, ...x_n$ each either 0 or 1, such that

$$S = a_1x_1 + a_2x_2 + a_3x_3 + ... + a_nx_n \quad \textbf{(1)}$$

Example: Let all subsets of the integers $(a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (2, 3, 4, 7, 11, 13, 16)$ that have 18 as their sum. we see that there are four subsets of these six integers that add together to give 18 namely 2+16 = 18, 7+11 = 18, 3+4+11 = 18 and 2+3+13 = 18.
Equivalently, there are exactly four solutions to the equation
$2x_1 + 3x_2 + 4x_3 + 7x_4 + 11x_5 + 13x_6 + 16x_7 = 18$ With $x_i = 0$ or 1 for i=1,2,3,4,5,6,7.

namely

$x_1 = x_7 = 1, x_2 = x_3 = x_4 = x_5 = x_6 = 0$

$x_4 = x_5 = 1, x_1 = x_2 = x_3 = x_6 = x_7 = 0$

$x_2 = x_3 = x_5 = 1, x_1 = x_4 = x_6 = x_7 = 0$

$x_1 = x_2 = x_6 = 1, x_1 = 1 = 0$

To verify equation (1) hold, whether each x_i is either 0 or 1, requires that we perform at most n additions. On the other hand, to search by trial and error solutions of equation (1), may require that we check all 2^n possibilities for $(x_1, x_2, x_3, ...x_n)$.

The best method known for finding a solution of the knapsack problem requires $O(2^{\frac{n}{2}})$ bit operations by using recurrence relation solving, which makes a computer solution of general knapsack problem extremely infeasible even n=100.Certain values of the integers $a_1, a_2, a_3, ...a_n$ make the solution of the knapsack problem much easier than the solution in the general case or inspection method.

For the instance if $a_j = 2^{j-1}$ to find the solution of $S = a_1x_1 + a_2x_2 + a_3x_3 + ... + a_nx_n$ where $x_i = 0$ or 1 for i = 1, 2, 3, 4…..,n, simply requires that we find the binary expression of S. We can also produce easy knapsack problems by choosing the integers $a_1, a_2, a_3, ...a_n$ so that the sum of the first (j-1) of these integers is always less than the j^{th} integer i.e., so that

$$\sum_{i=1}^{j-1} a_i < a_j \qquad j = 1, 2, 3, ...n$$

If a sequence of integers $a_1, a_2, a_3, ...a_n$ satisfies this inequality we call the sequence *Super Increasing*

III.SUPER INCREASING SEQUENCE METHOD

1. Definition of Super increasing sequence:

The sequence $a_1, a_2, a_3, ...a_n$ is super increasing if it satisfies the following inequality

$a_2 > a_1, a_3 > a_2 + a_1, a_4 > a_3 + a_2 + a_1 .....a_n > a_{n-1} + a_{n-2} + ... + a_3 + a_2 + a_1$. then corresponding x value is 0 otherwise 1.

By Super increasing sequence method:

Example: Let us find the integers $(a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (2, 3, 4, 7, 11, 13, 16)$ that have 18 as their sum.

First, we note that since 2+3+4+7+11>18, a sum of integers from this set can only be less than 18 if the sum contains the integers 18.

$2x_1 + 3x_2 + 4x_3 + 7x_4 + 11x_5 + 13x_6 + 16x_7 = 18$ with each $x_i = 0$ or 1, we must have $x_7 = 1$ and

$2x_1 + 3x_2 + 4x_3 + 7x_4 + 11x_5 + 13x_6 = 2$ since 13>2, $x_6 = 0$.

Since $2x_1 + 3x_2 + 4x_3 + 7x_4 + 11x_5 = 2$ since 11>2, $x_5 = 0$

Since $2x_1 + 3x_2 + 4x_3 + 7x_4 = 2$ since 7>2 , $x_4 = 0$

Since $2x_1 + 3x_2 + 4x_3 = 2$ since 4>2, $x_3 = 0$

Since $2x_1 + 3x_2 = 2$ since 3>2, $x_2 = 0$

Since $2x_1 = 2$ obviously we have $x_1 = 1$.

Therefore the solution is 18 = 2 + 16.

In general to solve the knapsack problems for super increasing sequence $a_1, a_2, a_3, ...a_n$ i.e., to find the values of $x_1, x_2, x_3, ...x_n$ with $S = a_1x_1 + a_2x_2 + a_3x_3 + ... + a_nx_n$ and $x_i = 0$ or 1 for i=1,2,3,…….n. when S is given, we use the following algorithm

.

2. Algorithm:

Step: 1

First find x_n by noting that

$$x_n = \left\{ \begin{matrix} 1 : if\ "S \geq a_n" \\ 0 : if\ "S \leq a_n" \end{matrix} \right\}$$

Step: 2

Then find $x_{n-1}, x_{n-2}, ...x_1$ in succession using the equations

$$x_j = \left\{ \begin{matrix} 1 : if\ "S - \sum_{i=j+1}^{n} x_i a_i \geq a_j" \\ \sum_{j=1}^{n} x_j a_j = S \end{matrix} \right\} \quad \text{for} \quad \text{j= n-1, n-2, …… 1.}$$

3. Working Procedure of the Algorithm:

First note that if $x_n = 0$ when $S \geq a_n$, then $\sum_{i=1}^{n} x_i a_i \leq \sum_{i=1}^{n} a_i < a_n \leq S$ contradicting the condition $\sum_{j=1}^{n} x_j a_j = S$.

Similarly if $x_j = 0$ when $S - \sum_{i=j+1}^{n} x_i a_i \geq a_j$ then

$$\sum_{i=1}^{j-1} x_i a_i \leq \sum_{i=1}^{j-1} x_j + \sum_{i=j+1}^{n} x_i a_i < a_j + \sum_{i=j+1}^{n} x_i a_i \leq S$$

Which is again contradiction using this algorithm knapsack problems based on super-increasing sequence can be solved extremely quickly.

IV.THE CIPHERS THAT WE DESCRIBE HERE ARE BASED ON TRANSFORMED SUPER-INCREASING SEQUENCES:

This cipher system was introduced by Merkle and Hellman and was considered a good choice Key cypher system.

1. Procedure:

Step1: Let $a_1, a_2, a_3, a_4, a_5 a_6, ...a_n$ be super-Increasing Sequence

Step2: Let m be a positive integer with $\mathbf{m > 2a_n}$

Step3: Let w be an integer relatively prime to m with $\overline{w}$ modulo m

Step4: Form the sequence $b_1, b_2, b_3, ...b_n$ where $b_j \cong wa_j \pmod{m}$ and $0 < b_j < m$.

Step5: We cannot use a special technique to solve a knapsack problem of the type

$S = \sum_{i=1}^{m} b_i x_i$ Where S is a positive integer, since the sequence $b_1, b_2, b_3, ...b_n$ is not super Increasing.

However when $\overline{w}$ is known we can find $\overline{w}s = \sum_{i=1}^{m} \overline{w}b_i x_i = \sum_{i=1}^{m} a_i x_i \pmod{m}$

Since $\overline{w}b_j \cong a_j \pmod{m}$ form above equation we see that $S_0 = \sum_{i=1}^{n} a_i x_i$ Where S_0 is the least positive residue of $\overline{w}s$ modulo m

Step6: We can easily solve the equation $S = \sum_{i=1}^{n} b_i x_i$,Since $b_j \cong wa_j \pmod{m}$ and $0 \le b_j \le m$.

2. Example problem1:

The super Increasing sequence $(a_1, a_2, a_3, a_4, a_5) = (3, 5, 9, 20, 44)$

Now to find the m value based on the condition $m > 2a_n$ then m > 88 , let us take m=89.

Let us the value of w which is relatively prime to m that is w = 67,since (67,89) = 1

Now to find the sequence $(b_1, b_2, b_3, b_4, b_5)$ based on the $b_j \cong wa_j \pmod{m}, 0 \le b_j \le m$

$b_j \cong 67a_j \pmod{89}$

$j = 1, b_1 \cong 67(3) \pmod{89} \cong 201 \pmod{89} \Rightarrow b_1 = 23$

$j = 2, b_2 \cong 67(5) \pmod{89} \cong 335 \pmod{89} \Rightarrow b_2 = 68$

$j = 3, b_3 \cong 67(9) \pmod{89} \cong 603 \pmod{89} \Rightarrow b_3 = 69$

$j = 4, b_4 \cong 67(20) \pmod{89} \cong 1340 \pmod{89} \Rightarrow b_4 = 5$

$j = 5, b_5 \cong 67(44) \pmod{89} \cong 2948 \pmod{89} \Rightarrow b_5 = 11$

The sequence of $(b_1, b_2, b_3, b_4, b_5) = (23, 68, 69, 5, 11)$

Now to find $\overline{w}$ based on the formula $\overline{w}w \cong 1 \pmod{m}$

$w\overline{w} \cong 1 \pmod{m} \Rightarrow 67(4) \cong 1 \pmod{89} \Rightarrow \therefore \overline{w} = 4$

To solve the knapsack problem $23x_1 + 68x_2 + 69x_3 + 5x_4 + 11x_5 = 84$

We can multiply both sides of this equation by 4 an inverse 67 modulo 89.

$23\square 4x_1 + 68\square 4x_2 + 69\square 4x_3 + 5\square 4x_4 + 11\square 4x_5 = 84\square 4 \bmod ulo 89$

$92x_1 + 272x_2 + 276x_3 + 20x_4 + 44x_5 = 336 \bmod ulo 89$

$3x_1 + 5x_2 + 9x_3 + 20x_4 + 44x_5 = 69$

The solution of this easy knapsack problem is that $x_2 = x_4 = x_5 = 1, x_1 = x_3 = 0$.

Hence the original problem has its solution is that **68+5+11=84**.

3. Example problem2:

Find the sequence obtained from the super-increasing sequence (1,3, 5,10,20,41,80) when modular multiplication is applied with multiplier w : 17 and modulus m : 162.

Solution: The given super Increasing sequence

$(a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (1, 3, 5, 10, 20, 41, 80)$ and w=17 , modulo m=162. Now to find the sequence $(b_1, b_2, b_3, b_4, b_5, b_6, b_7)$ based on the formula $b_j \cong wa_j \pmod m, 0 \le b_j \le m$

$j = 1, \Rightarrow b_1 \cong 17 \times 1 \pmod{162} \cong 17 \pmod{162} \Rightarrow b_1 = 17$

$j = 2, \Rightarrow b_2 \cong 17 \times 3 \pmod{162} \cong 51 \pmod{162} \Rightarrow b_2 = 51$

$j = 3, \Rightarrow b_3 \cong 17 \times 5 \pmod{162} \cong 85 \pmod{162} \Rightarrow b_3 = 85$

$j = 4, \Rightarrow b_4 \cong 17 \times 10 \pmod{162} \cong 170 \pmod{162} \Rightarrow b_4 = 8$

$j = 5, \Rightarrow b_5 \cong 17 \times 20 \pmod{162} \cong 340 \pmod{162} \Rightarrow b_5 = 16$

$j = 6, \Rightarrow b_6 \cong 17 \times 41 \pmod{162} \cong 697 \pmod{162} \Rightarrow b_6 = 49$

$j = 7, \Rightarrow b_7 \cong 17 \times 80 \pmod{162} \cong 1360 \pmod{162} \Rightarrow b_1 = 64$

The sequence of $(b_1, b_2, b_3, b_4, b_5, b_6, b_7) = (17, 51, 85, 8, 16, 49, 64)$

Now to find $\overline{w}$ based on the formula $\overline{w}w \cong 1 \pmod m$

$w\overline{w} \cong 1 \pmod m \Rightarrow 17(143) \cong 1 \pmod{89} \Rightarrow \therefore \overline{w} = 143$

To solve the knapsack problem, we can multiply both sides of this equation by 143 an inverse 17 modulo 162

$17 \times 143x_1 + 51 \times 143x_2 + 85 \times 143x_3 + 8 \times 143x_4 + 16 \times 143x_5 + 49 \times 143x_6 + 64 \times 143x_7 = 153 \times 143$

$2431x_1 + 7293x_2 + 12155x_3 + 1144x_4 + 2288x_5 + 7007x_6 + 9152x_7 = 21879 \bmod 162$

$x_1 + 3x_2 + 5x_3 + 10x_4 + 20x_5 + 41x_6 + 80x_7 = 9$

The solution of this easy knapsack problem is that $x_1 = x_2 = x_3 = 1, x_4 = x_5 = x_6 = x_7 = 0$

Hence the original solution is **17+51+85=153**

V.THE ENCIPHERING AND DECIPHERING PROCEDURES OF THE KNAPSACK CIPHER BASED ON MODULAR ARITHMETIC:

Step1: Each Individual choose a super increasing sequence of positive integers of specific length N. $a_1, a_2, a_3, a_4, ...a_N$ as well as modulus m with condition $m > 2a_N$ and multiplier w with (m,w) = 1.

Step2: The transformed sequence $b_1, b_2, b_3, b_4, b_5, ...b_N$ when $b_j \cong wa_j \pmod m, 0 \le b_j \le m$, for j=1, 2, 3, 4,……N is made public.

Step3: When someone wishes to send a message P to this individual the message is first translated into a string of 0's and 1's using binary equivalence letters as shown below table.

letter	binary equivalent	letter	binary equivalent
A	00000	N	01101
B	00001	O	01110
C	00010	P	01111
D	00011	Q	10000
E	00100	R	10001
F	00101	S	10010
G	00110	T	10011
H	00111	U	10100
I	01000	V	10101
J	01001	W	10110
K	01010	X	10111
L	01011	Y	1 1000
M	01100	Z	11001

Step4:This string of zero's and one's is next split into segments of length N,if not, we can simply fill out the last block with all 1's.For each block ,a sum is computed using the sequence $b_1, b_2, b_3, b_4, b_5, ...b_N$; for instance of the block $x_1, x_2, x_3, ...x_n$;given $S = b_1x_1 + b_2x_2 + ... + b_Nx_N$ .Finally the sum generated by each block form the cipher message.

Step5:We note that the decipher text generated by knapsack cipher without knowledge of m and w require that a group of hard knapsack problems of the form $S = b_1x_1 + b_2x_2 + ... + b_Nx_N$ be solved on the other hand, when m and w are known the knapsack problem(S) can be transformed into an Easy knapsack problem.

$$\overline{w}S = \overline{w}b_1x_1 + \overline{w}b_2x_2 + ... + \overline{w}b_Nx_N$$

Since

$$\overline{w}S \cong a_1x_1 + a_2x_2 + ... + a_Nx_N \pmod m$$

where $\overline{w}b_j \cong a_j \pmod m$, $\overline{w}$ is an inverse of w modulo m,so that $S_0 = a_1x_1 + a_2x_2 + a_3x_3 + ... + a_Nx_N$

Where S_0 is the least positive integer residue of $\overline{w}S \pmod m$,we have equality (S_0),Since both sides of the equation are positive integers less than m which are congruent modulo m

.

1. Example the enciphering and deciphering procedure of knapsack cipher with an super-Increasing sequence:

We start with the super Increasing sequence

$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}) = (2, 11, 14, 29, 58, 119, 241, 480, 959, 1917)$

Take the value of m based on the condition $m > 2a_N = 2 \times 1917 = 3834$

Let us take m = 3837 as the enciphering modulus, so that $m > 2a_N$ and w = 1001 as the multiplier, so that (m,w) = 1 to transform the super increasing sequence into the sequence

$(2 \times 1001, 11 \times 1001, 14 \times 1001, 29 \times 1001, 58 \times 1001, 119 \times 1001, 241 \times 1001, 480 \times 1001, 959 \times 1001, 1917 \times 1001)$

$(2002, 11011, 14014, 29029, 58058, 119119, 241241, 480480, 959959, 1918917)$

After performing modulo 3837, we get the below sequence, i.e., the public key is

$(2002, 3337, 2503, 2170, 503, 172, 3347, 855, 709, 417)$

and the private key is $(2, 11, 14, 29, 58, 119, 241, 480, 959, 1917)$

The sender sends the message as follows:

To encipher the message "REPLY IMMEDIATELY"
First translate the letters of the message into their five digits binary equivalence in **above table and** group these digits into blocks of **ten**, to obtain the following
1000100100 0111101011 1100001000 0110001100 0010000011 0100000000 1001100100 0101111000
For each block of ten binary digits, we form a sum by adding together the approximate terms of the sequence
$(2002, 3337, 2503, 2170, 503, 172, 3347, 855, 709, 417)$
In the slots corresponding to positions of the block containing a digit equal to '1' this gives us
3360, 12986, 8686, 10042, 3629, 3337, 5530, 9529

Now the receivers decode the message as follows:

To decipher, we find the least positive residue modulo 3837 of 23 times each sum23 is an inverse of 1001 modulo 3837 and then solve the corresponding easy knapsack problem with respect to the original super increasing sequence
$(2, 11, 14, 29, 58, 119, 241, 480, 959, 1917)$
For deciphering the above block as follows
$3360 \times 23 \cong 540 (\text{mod } 3837)$

$12986 \times 23 \cong 3229 (\text{mod } 3837)$

$8686 \times 23 \cong 254 (\text{mod } 3837)$

$10042 \times 23 \cong 746 (\text{mod } 3837)$

$3629 \times 23 \cong 2890 (\text{mod } 3837)$

$3337 \times 23 \cong 11 (\text{mod } 3837)$

$5530 \times 23 \cong 569 (\text{mod } 3837)$

$9529 \times 23 \cong 458 (\text{mod } 3837)$
The decoded message is (540, 3229, 254, 746, 2890, 11, 569, 458)
Its equivalent binary decoded message is:
540 = 2+58+480 = 1000100100 =RE
3229 = 11+14+29+58+241+959+1917 = PL
254 = 2+11+241 = 1100001000 = YI
746 = 11+14+241+480 = 0110001100 = MM
2890 = 14+959+1917 = 0010000011 =ED
11=11 = 0100000000 = IA
569 = 2+29+58+480 = 1001100100 = TE
458 = 11+29+58+119+241 = 0101111000 = LY
The decoded message is: **REPLY IMM EDIATELY**.

2. Example:
Encipher the message BUY NOW using the knapsack cipher based on the sequence obtained from the super-increasing sequence (17, 19, 37, 81,160), by performing modular multiplication with multiplier w = 29 and modulus: m=331.

Sol: Given super Increasing sequence $(a_1, a_2, a_3, a_4, a_5) = (17, 19, 37.81, 160)$

and w = 29 and m = 331, here (m,w) = 1,so transfer the super increasing sequence into the sequence
$(29 \times 17, 29 \times 19, 29 \times 37, 29 \times 81, 29 \times 160)$

$(493, 551, 1073, 2349, 4640)\ \mathrm{mod}(331)$

$(162, 220, 80, 32, 6)$

The public key is: (162.220, 80, 32, 6) and Private Key is: (17, 19, 37, 81,160)

The sender sends the message as follows:

To encipher the message "BUY NOW"
First translate the letters of the message into their five digits binary equivalence in **above table and** group these digits into blocks of **five**, to obtain the following
00001 10100 11000 01101 01110 10110
For each block of ten binary digits, we form a sum by adding together the approximate terms of the sequence. In the slots corresponding to positions of the block containing a digit equal to '1' this gives us
(6,242,382,306,332,274) mod (331)
(6, 242, 51, 306, 1,274)

Now the receivers decode the message as follows:

To decipher, we find the least positive integer residue modulo 331, of 137 times sum 137 is an inverse of 29 modulo 331

i.e., $\overline{w}w = 1\ \mathrm{mod}(331) \Rightarrow 29\overline{w} = 1\ \mathrm{mod}(331) \Rightarrow \overline{w} = 137$

and then solve corresponding easy knapsack problem with respect to the original super increasing Sequence
For deciphering the above block as follows
$6 \times 137 \cong 160\ \mathrm{mod}(331) \Rightarrow 160$

$242 \times 137 \cong 54\ \mathrm{mod}(331) \Rightarrow 54$

$51 \times 137 \cong 36\ \mathrm{mod}(331) \Rightarrow 36$

$306 \times 137 \cong 216\ \mathrm{mod}(331) \Rightarrow 216$

$1 \times 137 \cong 137\ \mathrm{mod}(331) \Rightarrow 137$

$274 \times 137 \cong 135\ \mathrm{mod}(331) \Rightarrow 135$

The decoded message is : (160,54,36,216,137,135)
Its equivalent binary decoded message is:
160 = 160 = 00001 = B
54 = 17 + 37 = 10100 = U
36 = 17 +19 =11000 = Y
216 = 19 +37 +160 = 01101 = N
137 = 19+37+81 = 01110 = O
135 = 17+37+81 = 10110 = W
The decoded message is**: BUY NOW**

VI.A SEQUENCE OF PAIRS OF RELATIVELY PRIME INTEGERS BY USING MODULAR MULTIPLICATION

There are several possibilities for altering this cipher system to avoid the weakness found by Shamir. One such possibility is to choose a sequence of **pairs of relatively prime integers** $(w_1, m_1), (w_2, m_2), (w_3, m_3), ...(w_r, m_r)$ and then form the series of sequences

$$b_j^{(1)} = w_1 a_j \pmod{m_1}$$

$$b_j^{(2)} = w_2 b_j^{(1)} \pmod{m_2}$$

$$b_j^{(3)} = w_3 b_j^{(2)} \pmod{m_3}$$

.

.

.

$$b_j^{(r)} = w_r b_j^{(r-1)} \pmod{m_r}$$

for j = l, 2, ..., n. We then use the final sequence $(b_1^{(r)}, b_2^{(r)} .....b_n^{(r)})$ as the enciphering sequence. Involving sequences obtained by **iterating modular multiplications** with different moduli (although there are several promising methods for the production of such algorithms)

Example: **Find the sequence obtained by applying successively the modular multiplications with multipliers and moduli (7,92), (11,95), and (6,101), respectively, on the super-increasing sequence (3,4,8,I7,33,67)**

$$b_1^{(1)} \cong w_1 a_1 \pmod{m_1} \cong 7 * 3 (\mathrm{mod}\ 92) \cong 21 (\mathrm{mod}\ 92)$$

$$b_1^{(2)} \cong w_2 b_1^{(1)} \pmod{m_2} \cong 11 * 21 (\mathrm{mod}\ 95) \cong 41 (\mathrm{mod}\ 95)$$

$$b_1^{(3)} \cong w_3 b_1^{(2)} \pmod{m_3} \cong 6 * 41 (\mathrm{mod}\ 101) \cong 44 (\mathrm{mod}\ 101)$$

$$\therefore b_1^{(3)} = 44$$

$$b_2^{(1)} \cong w_1 a_2 \pmod{m_1} \cong 7 * 4 (\mathrm{mod}\ 92) \cong 28 (\mathrm{mod}\ 92)$$

$$b_2^{(2)} \cong w_2 b_2^{(1)} \pmod{m_2} \cong 11 * 28 (\mathrm{mod}\ 95) \cong 23 (\mathrm{mod}\ 95)$$

$$b_2^{(3)} \cong w_3 b_2^{(2)} \pmod{m_3} \cong 6 * 23 (\mathrm{mod}\ 101) \cong 37 (\mathrm{mod}\ 101)$$

$$\therefore b_2^{(3)} = 37$$

$b_3^{(1)} \cong w_1 a_3 \pmod{m_1} \cong 7 * 8 \pmod{92} \cong 56 \pmod{92}$

$b_3^{(2)} \cong w_2 b_3^{(1)} \pmod{m_2} \cong 11 * 56 \pmod{95} \cong 46 \pmod{95}$

$b_3^{(3)} \cong w_3 b_3^{(2)} \pmod{m_3} \cong 6 * 46 \pmod{101} \cong 74 \pmod{101}$

$\therefore b_3^{(3)} = 74$

$b_4^{(1)} \cong w_1 a_4 \pmod{m_1} \cong 7 * 17 \pmod{92} \cong 27 \pmod{92}$

$b_4^{(2)} \cong w_2 b_4^{(1)} \pmod{m_2} \cong 11 * 27 \pmod{95} \cong 12 \pmod{95}$

$b_4^{(3)} \cong w_3 b_4^{(2)} \pmod{m_3} \cong 6 * 12 \pmod{101} \cong 72 \pmod{101}$

$\therefore b_4^{(3)} = 72$

$b_5^{(1)} \cong w_1 a_5 \pmod{m_1} \cong 7 * 33 \pmod{92} \cong 47 \pmod{92}$

$b_5^{(2)} \cong w_2 b_5^{(1)} \pmod{m_2} \cong 11 * 47 \pmod{95} \cong 42 \pmod{95}$

$b_5^{(3)} \cong w_3 b_5^{(2)} \pmod{m_3} \cong 6 * 42 \pmod{101} \cong 50 \pmod{101}$

$\therefore b_5^{(3)} = 50$

$b_6^{(1)} \cong w_1 a_6 \pmod{m_1} \cong 7 * 67 \pmod{92} \cong 9 \pmod{92}$

$b_6^{(2)} \cong w_2 b_6^{(1)} \pmod{m_2} \cong 11 * 9 \pmod{95} \cong 4 \pmod{95}$

$b_6^{(3)} \cong w_3 b_6^{(2)} \pmod{m_3} \cong 6 * 4 \pmod{101} \cong 24 \pmod{101}$

$\therefore b_6^{(3)} = 24$

The final encipher sequence is : $(b_1^{(3)}, b_2^{(3)}, b_3^{(3)}, b_4^{(3)}, b_5^{(3)}, b_6^{(3)}) = (44, 37, 74, 72, 50, 24)$

VII.MULTIPLICATIVE KNAPSACK PROBLEM

A multiplicative knapsack problem is a problem of the following type: Given positive integers $a_1, a_2, a_3, a_4, a_5, ...a_n$ and a positive integer P, find the subset, or subsets, of these integers with product P, or equivalently, find all solutions of P , $P = a_1^{x_1} a_2^{x_2} a_3^{x_3} .....a_n^{x_n}$

Where $x_j = 0 or 1, for, j = 1, 2, 3, ...n$

Examples Problems

1. Find all products of subsets of the integers 2,3,5,6, and l0 equal to 60

Solution:
60 can be expressed as product of primes as follows

$60 = 2^{1} \square 3^{0} \square 5^{1} \square 6^{1} \square 10^{0} = 2 \square 5 \square 6 = 60$
$\therefore$ The possible subset is (2,5,6)

$60 = 2^{0} \square 3^{0} \square 5^{0} \square 6^{1} \square 10^{1} = 6 \square 10 = 60$
$\therefore$ The possible subset is (6,10)

$60 = 2^{1} \square 3^{1} \square 5^{0} \square 6^{0} \square 10^{1} = 2 \square 3 \square 10 = 60$
$\therefore$ The possible subset is (2,3,10)
The required possible subsets are: (2,5,6), (6,10), (2,3,10)

2. Find all products of subsets of the integers 8, 13,17,21,95,121 equal to 15960
Solution:

$15960 = 8^{1} \square 13^{0} \square 17^{0} \square 21^{1} \square 95^{1} \square 121^{0} = 8 \square 21 \square 91 = 15960$
The required possible subset is: (8,21,91).

.

VIII. CONCLUSION

Knapsack encryption provides a good approach to creating public and private keys, where there private key is easy to use, while the public key is difficult to compute. The method was outlined by Ralph Merkle in his search for a trap door function [13], but the glory of the sustainable trap door went to RSA, and soon cracks began to show when Adi Shamir [4] published methods to crack it.
Knapsack problems appear in real-world decision-making processes in a wide variety of fields, such as finding the least wasteful way to cut raw materials, selection of investments and portfolios, selection of assets for asset-backed securitization, and generating keys for the Merkle–Hellman and other knapsack cryptosystems.

One early application of knapsack algorithms was in the construction and scoring of tests in which the test-takers have a choice as to which questions they answer. For small examples, it is a fairly simple process to provide the test-takers with such a choice. For example, if an exam contains 12 questions each worth 10 points, the test-taker need only answer 10 questions to achieve a maximum possible score of 100 points. However, on tests with a heterogeneous distribution of point values, it is more difficult to provide choices. Feuerman and Weiss proposed a system in which students are given a heterogeneous test with a total of 125 possible points. The students are asked to answer all of the questions to the best of their abilities. Of the possible subsets of problems whose total point values add up to 100, a knapsack algorithm would determine which subset gives each student the highest possible score.

ACKNOWLEDGEMENT:

We would like to express my special thanks of gratitude to Secretary & Correspondent Dr.R Guru Prasad as well as our principal Dr.S.Rama Devi madam who gave me the golden opportunity to do this research paper, helping us improve the exposition through their interesting and very encouraging comments on this paper.

Secondly would also like to thank my family, parents and students who helped me a lot in finalizing this paper within the limited time frame.

REFERENCES

[1] Mathews, G. B. (25 June 1897). "On the partition of numbers" (PDF). Proceedings of the London Mathematical Society. 28: 486–490. doi:10.1112/plms/s1-28.1.486.

[2] Dantzig, Tobias. Numbers: The Language of Science, 1930.

[3] M. E. Hellman, "The mathematic of public-key cryptography," Scientffic American, Volume 241-(1979), 146-157.

[4] Shamir, "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem," proceedings of the 23rd Annual symposium of the Foundations of computer science, 145-152.

[5] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," communications of the ACM, Volume 2t (1979), tZO-126.

[6] Shamir, "How to share a secret," communications of the ACM, Volume 22 0979), 612-6t3.

[7] Shamir, R. L. Rivest, and L. M. Adleman, "Mental poker" The Mathematical Gardner, ed. D. A. Klarner, wads worth International, Belmont, California, 1981, 37-43.

[8] Elementary Number Theory and lts Applications Kenneth H. Rosen AT&T Information Systems Laboratories (formerly part of Bell Laboratories.

[9] L M. Adleman, C. Pomerance and R. S. Rumely, "On distinguishing prime numbers from composite numbers," Annals of Mathematics, volume 117 (1983), 173-2A6

[10] H. C. Williams, "The influence of computers in the development of number theory Computers and Mathematics Applications, Volume 8 (1982),75-9

[11] D. M. Burton, Elementary Number Theory, Allyn and Bacon, Boston, t976

[12] T. A. Apostol, Introduction to Analytic Number Theory, Springer Verlag, New York, 1976

[13] Merkle, Ralph; Hellman, Martin (1978). "Hiding information and signatures in trapdoor knapsacks". Information Theory, IEEE Transactions on 24 (5): 525–530. doi:10.1109/TIT.1978.1055927.