An Applications Of Number Theory In ISBN Numbering And Hashing Function

[1] Nirmaladevi.K , [2] Atchaya.R[2], [3] Ramya Devi.R, [4] Acshaya.L
[1]Assistant professor, Department of Mathematics, Sri Krishna Arts And Science College, Coimbatore-641008.
[2, 3, 4] UG scholars, Department of Mathematics, Sri Krishna Arts And Science College, Coimbatore-641008.
[1]nirmaladevik@skasc.ac.in, [2]atchayar16bma007@skasc.ac.in, [3]ramyadevir16bma045@skasc.ac.in,
[4]acshayal16bma002@skasc.ac.in

Abstract: *Cryptography is the process of securing the important informations and the study of secret codes. This paper aims to introduce some of the currently using real life application. In this paper, we investigate on the topic "An Applications Of Number Theory In ISBN Numbering And Hashing Function". In the field of mathematics, we have chosen number theory intimately which deals with cryptography and its applications.*

Keywords: *Cryptography, ISBN, Hashing function, Encryption and Decryption.*

1. INTRODUCTION:

Cryptography is the practice of creating and generating the codes which is essential in hiding the information. Number theory is widely used in some applications of cryptography. Number theory is an important concept in pure mathematics which deals with the study of positive integers. Initially, during twentieth century the term number theory was derived as arithmetic. And in modern times, it plays a vital role in many sectors. Let us briefly know about the validation and the way to find the check digit of ISBN, hashing function and the method of encrypting and decrypting the important secret codes which is very much essential in various fields.

2. MAIN WORK:

In this paper, we briefly solve the problems in the applications of

- ISBN – Code
- Hashing function
- Encryption And Decryption

3. PROBLEMS:

- **ISBN**

An ISBN is an International Standard Book Number. ISBN are calculated using a specific mathematical formula and include a check digit to validate the number.

3.1 Calculate the check digit of 13 digit ISBN.

ISBN -13 of 978-0-306-40615*

Solution:
The given number is 978-0-306-40615*
Multiplying the above ISBN by 1 and 3 alternatively,
We get,
=9*1 + 7*3 + 8*1 + 0*3 + 3*1 + 0*3 + 6*1 + 4*3 + 0*1 + 6*3 + 1*1 + 5*3
= 9+21+8+0+3+0+6+12+0+18+1+15
=93
The above value is a summed modulo 10 to give a value ranging from 0 to 9.
=93/10

=9 remainder 3.
Finally, subtracted from 10 leaves a result from 1 to 10.
=10-3
= 7.
Therefore, the check digit is 7.
The complete ISBN is 978-0-306-40615.

3.2 Checking whether the ISBN is valid or not.

ISBN 9781932698183

Solution:
The given number is 9781932698183.
Since the above ISBN is 13 digit , we multiply by 1 and 3 alternatively,
= 9*1 + 7*3 + 8*1 + 1*3 + 9*1 + 3*3 + 2*1 + 6*3 + 9*1 + 8*3 + 1*1 + 8*3 + 3*1
= 9+21+8+3+9+9+2+18+9+24+1+24+3
=140.
Dividing 140 by 14
$= \frac{140}{14}$
= 10
since the sum is divisible by 14.
The above 13 digit ISBN is valid.

- **HASHING FUNCTION:**

A hash function is any function that can be used to map a data of arbitrary size to data of a fixed size. It is used in cryptography for assuring integrity of transmitted data and HMACs, which provide message authentication.

1. **Find the memory locations which is assigned by the hashing function h(k) = k mod 101 to the records of an insurance company with these social security numbers.**
   104578690

Solution:
Consider,
104578690 mod 101
104578690 = 101 (x)
We need to divide 104578690 by 101
$\frac{104578690}{101}$ = 1035432.574
Multipying the above value by 101
104578690 = 101(1035432) + 58
Therefore,
104578690 mod 101 = 58.

2. 432222187

Solution:
432222187 mod 101
432222187≡ 101 (x)
Dividing 432222187 by 101
We get,
432222187/101 = 4279427.594
By Subtracting
=4279427.594 – 4279427
=0.5940594
Then, multiplying 0.5940594 * 101
= 59.9999994
Here,
432222187 = 101(4279427) + 60
Therefore,
432222187 mod 101 = 60.

➢ ENCRPTION AND DECRYPTION

Encryption is the method of transforming the secret messages. Decryption is to transform the encrypted information so that it is intelligible again.

1. **Decrypt the message RXJFKZYH**

Solution:
Let us consider A = 0, B = 1,…….., Z=25 respectively.
R = 17 =(17-21)mod 26 = 18 = S
X= 23 = (23-21)mod 26 = 4 = E
J= 9 =(9-21)mod 26 =2 = C
F= 5 =(5-21)mod 26 = 20 = U
K= 10 = (10-21)mod 26 = 17 = R
Z= 25 =(25-21)mod 26 = 8 = I
Y= 24 =(24-21)mod 26 = 19 = T
H= 7= (7-21)mod 26 = 24 = y
Thus, RXJFKZYH is decrypted as SECURITY.

2. **If we wants to encrypt a string of bits. we decides to encrypt using an LFSR as a generator in a stream cipher. A sequence bits m=m_1 …..$m_n$is encrypted to a sequence of ciphertext symbols c=c_1,c_2…….$c_n$by**

c_i= m_i+s_i', 1≤ i ≤ n
wheres'$_i$ = s'$_1$,s'$_2$ .....is obtained from the binary LFSR sequence s=s1,s2….using s'i=s_{2i} i=1,2…. Finally, s is generated by a length 4 LFSR with connection polynomial c(x)=1+x+x^4, with initial secret state (s1, s2, s3, s4)(the LFSR outputs first s1 then s2)
Eve observed the cipher text c=0, 1, 1, 1, 1, 1, 0. Also, she knows the plaintext starts as1, 1, 1,….i.e,
M=1, 1, 1, 1, m5, m6, m7.

Solution:
Here, we know that
S_{2i}=c_i+m_i, for 1≤ i ≤ 4
S_2=1, s_4=0, s_6=0, s_8=0.
S_i= s_{i-1}+s_{i-4} i≥ 4
We have,
S_5= s_4+s_1
S_6= s_5+s_2
S_7= s_6+s_3
S_8= s_7+s_4
This gives that s_5=s_2+s_6=1 and therefore s_1=s_4+s_5=1. Also, s_7=s_4+s_8=0 which gives s_3= s_6+s_7=0. Thus secret state is (s_1,s_2,s_3,s_4)=(1, 1, 0, 0)and we can find all the plaintext bits easily, to find m_5, m_6, m_7 we need to find s_{10}, s_{12}, s_{14}. Using recursion we compute
S_9= s_8+s_5=1
S_{10}= s_9+s_6=1
S_{11}= s_{10}+s_7=1
S_{12}= s_{11}+s_8= 1
S_{13}= s_{12}+s_9= 0
S_{14} = s_{13}+s_{10}= 1
Thus, m_5=c_5+s_{10}= 1+1=0, m_6=c_6+s_{12}= 1+1=0, m_7= c_7+s_{14}= 0+1= 1.

4. CONCLUSION :

In this paper, we perceive that number theory plays an important role in cryptography to hide the informations. Here, by using the number theory we found the easy way of calculating the ISBN and its validation, the methods of hashing functions, and to encrypt and decrypt the codes used in multiple sectors.

REFERENCES:

Books:

1. David Gries and Fred B. Schneider. *Applied number theory in computing/Cryptography. Edition-2.*
2. Hoffstein, J.(2008). *An Introduction to Mathematical cryptography. Edition-2.*

3. James S. Kraft and Lawrence C. Washington. (2008) *An Introduction to Number Theory with cryptography*. *Edition-2*.
4. Neal koblitz.*(2006) A Course In Number Theory And Cryptography* ,Springer.2nd edition.
5. William Stallings.*(2006)Cryptography and Network Security Principles*. published by Dorling Kindersley (pvt ltd).4th edition.

Web References:

6. www.math.uchicago.edu
7. www.encylopedia.com
8. http://web.math.pmf.uniz.hr