Approach of Message Communication Using Fibonacci Series: In Cryptology

Syed Khutubuddin Ahmed Khadri
Dept of MCA, REVA Institute of Technology & Management, Bangalore, India

Debabrata Samanta
Dept of MCA, Acharya Institute of Technology, Bangalore, India

Mousumi Paul
Dept of CSE, National Institute of Technology, West Bengal, India

***Abstract*—The objective of cryptography is to make it feasible for more than one person to do secure communication without intrusion. In the process of sending messages, security of the message is an important challenge as the messages are more vital or secret and protecting data stored in and transferred between distributed components from unauthorized access is very important. Cryptography provides various ways to safe guard messages but here the proposed method will be more concerned with a technique of encoding the text in such a way that the recipient can only discover the original message without any data loss or without any alteration or data getting leaked. In this paper highlights the problem and provides some possible approach to solve this problem using Fibonacci series. The Encryption of data is done by combining the original data with Fibonacci numbers to get a Cipher text which is non-understandable to any intruder. Only the receiver knows the logic to do so.**

***Index Terms*—encryption, decryption, fibonacci, cipher text.**

I. Introduction

Communication today includes radio communication, telephonic communication, network communication and mobile communication. And Mobile Message communication/ email communication has become a daily routine and necessity of every individual or an organization as part of their work. But it gives more challenges to everyone to safe guard their information what they are sending to the reliable receiver.

As Network communication, especially over the internet, has emerged as one of the most powerful methods of communication with an over-whelming impact on our lives and Rapid advances in communication technology have also given rise to security threats to every individual and organization. Network communication is acting as a back bone for information technology applications such as ecommerce, e-banking, e-mail, medical databases, and many more but all of them require the exchange of private information which is crucial and can be hacked or leaked by any intruder. From many years Cryptography is serving the purpose by providing various methods and ways to safe guard the communication buy providing various algorithms.

Manuscript received November 4, 2013; revised August 1, 2014.

II. Problem Definition

Communication has become one of the primary ways we communicate, both in our personal and professional lives.

Message is a medium by which sender and receiver communicates to each other. But sometime it is essential to hide their own message from third party in such a way that only they two (Sender and Receiver) can understand the message, as contents of common SMS messages are known to the network operator's systems and personnel, or if the user is in the public then there is more chance of information getting leaked. For this reason sender should encode the data and then he can send the data to the receiver. The encoded form cannot be understood by third party. When receiver gets it, he/she convert it in to original message i.e. he/she decodes it. Here we also develop a C program to encode a data and we also develop a code to decode the data.

III. Process

User will input the message. The Input will be encoded by adding the Fibonacci numbers to the input message to generate a cipher text which is non-understandable. Example: if the message to be sent is “Job is done” then the input is encoded as shown below
Input details:

IV. Conversion process

If the user had given a message as “JOB”, we follow these steps to encode the message. Take the ASCII value of every character in the input. Take the Fibonacci series

doi: 10.12720/lnit.2.2.168-171

INPUT→	J	O	B		I	S		D	O	N	E
ASCII Value of Input	67	72	59	32	66	76	32	61	72	71	62
Fibonacci Value	0	1	1	2	3	5	8	13	21	34	54
Encoded Message (ASCII value+ Fibonacci Value)	(67+0) 67	(72+1) 73	(59+1) 60	(32+2) 34	(66+3) 69	(76+5) 81	(32+8) 40	(61+13) 74	(72+21) 93	(71+34) 105	(62+54) 116
Encoded Message shown is	J	P	C	"	L	X	(	Q	]	i	t

Add the every ASCII value one by one with the Fibonacci series number. Example: JOB DONE

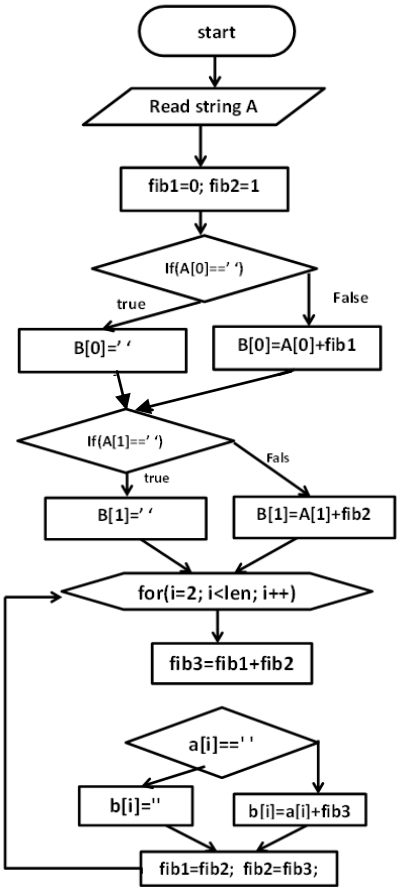
ASCII of J → 67 , O → 72, B→ 59, SPACE → 37 , D → 61, N → 71, E → 62

First Fibonacci numbers are 0, 1, 1, 2, 3, 5, 7, 13, 21, 34 …

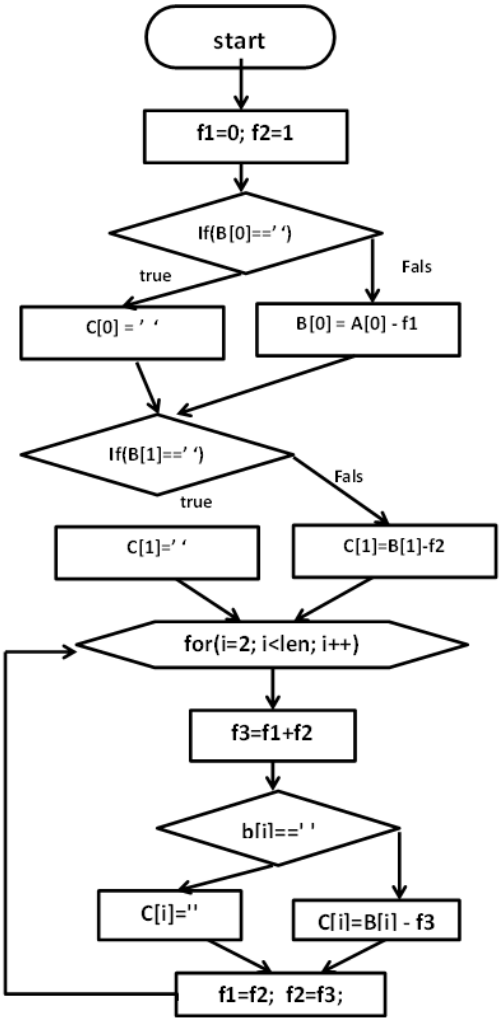
Encoding for J → 67 + 0 → 67
Encoding for O → 72 + 1 → 73
Encoding for B → 73 + 1 → 60
Encoding for SPACE → 37 + 2 → 39
Encoding for D → 61 + 3 → 64
Encoding for O → 72 + 5 → 77
Encoding for N → 71 + 7 → 78
Encoding for E → 62 + 13→ 75
Encoded Message shown is → JPC"Q]it

V. Flow of Work

For Sender:



For receiver:



VI. Methodology

Let us take the input string as
Logic at the Sender:
Array a →Bangalore
Array b[0]→ a[0] + Fib[0]

B + 0 → 59 + 0 = 59

b[1] → a[1] + Fib[1]

a + 1 → 97 + 1 = 98

b[2] → a[2] + Fib[2]

n + 1 → 110+1 = 111

Logic at Receiver:
Array b → Bboidqw z
Array b[0]→ a[0] + Fib[0]

B - 0 → 59 + 0 = 59 → B

b[1] → a[1] + Fib[1]

b - 1 → 98 - 1 = 97 → a

b[2] → a[2] + Fib[2]

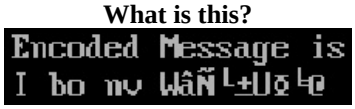
o - 1 → 111-1 = 110 → n

VII. Result and Discussion

Output-1

Message Entered by uses
I am in Bangalore

What is this?

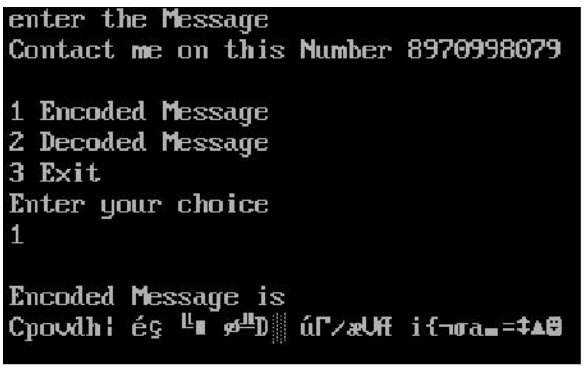


It's an Encoded message after adding the Fibonacci value with the ASCII value of each character from Input.

What is this?

It's an Decoded message after subtracting the Fibonacci value from the Encoded message.

Output-2



VIII. Conclusion

In this paper, we proposed a novel approach for secure way of message communication using Fibonacci series. The Encryption of data is done by combining the original data with Fibonacci numbers to get a Cipher text which is non-understandable to any intruder which give a higher level security to the message being hacked.

References

[1] L. B. Milstein *et al*., "On the feasibility of a CDMA overlay for personal communications networks," *IEEE J. Selecred Areas Commun.*, vol. 10, pp. 655-668, May 1992.

[2] E. G. Tiedemann, A. B. Salmasi, and K. S. Gilhousen, "The design and development of a code division multiple access (CDMA) system for cellular and personal communications," in *Proc. IEEE PIMRC'91*, London, UK, 1991.

[3] G. D. Fomey, Jr., "Maximum-likelihood sequence estimation of digital sequences in the presence of ISI," *IEEE Trans. Informat. Theory*, vol. IT-18, pp. 363-378, May 1972.

[4] S. K. Ahmed Khadri, D. Samanta, and M. Paul, "Secure approach for message communication," *International Journal of Advanced Research in Computer and Communication Engineering*, pp. 3481-3484, vol. 2, no. 9, September 2013.

[5] G. A. Miller, "The magical number seven, plus or minus two," *Some Limits on Our Capacity for Processing Information*, Psychological Review, vol. 63, pp. 81-97, 1956.

[6] R. Atkinson and R. Shiffrin, "Human memory: A proposed system and its control processes," *in the Psychology of Learning and Motivation: Advances in Research and Theory*, K Spence and J Spence, Eds., vol. 2, New York: Academic Press Best, 1995.

[7] Click to book. Digital Journal. [Online]. Available: http://digitaljournal.com/article/312789

[8] Comparing Floating Point Numbers. [Online]. Available: http://www.cygnus-software.com/papers/comparingfloats/comparingfloats.htm

[9] Floating Point Number Representation. [Online]. Available: http://www.cprogramming.com/tutorial/floating_point/understanding_floating_point_representation.html

[10] A. Joseph Raphael and V. Sundaram, "Secured crypto-stegano communication through unicode," *World of Computer Science and Information Technology Journal*, vol. 1, no. 4, pp. 138-143, 2011.

[11] D. K. Sarmah and N. bajpai, "Proposed system for data hhid-ing using cryptography and steganography," *International Journal of Computer Applications (0975 – 8887)*, vol. 8, no. 9, October 2010.

[12] S. Channalli and A. Jadhav, "Steganography an art of hiding data," *International Journal on Computer Science and Engineering*, vol. 1, no. 3, pp. 137-141, 2009.

Syed Khutubuddin Ahmed Khadri had received his MCA Degree from PES Institute of Technology, Bangalore under VTU (visvesvaraya technological university, Belgaum) in the year 2008. He has 5 year of teaching experience at post graduate level. He is currently working as Assistant Professor in REVA Institute of Technology & Management, Bangalore. His area of interest is Programming languages, DBMS, Data Structures & image processing. He had been awarded as the best faculty

in the year 2011 for academic excellent by KNS Institute of Technology and He had been awarded as practitioner of innovative teaching methodologies by Wipro technologies in a mission10X conclave program held in the year 2012 at VVIT Mysore.

Prof. Debabrata Samanta, a member of the IAENG, Board member of the Seventh Sense Research Group Journals (SSRGJ). He obtained B.Sc. (Physics Honors) in the year 2007, from the Vivekananda Collage, Takurpukur, under Calcutta University; Kolkata, India .He obtained MCA in the year 2010, from the Academy Of Technology, under WBUT. He has been working his PhD in Computer Science and Engg. from the year 2010 from National Institute of Technology, Durgapur, India in the area of Image Processing .He is presently working as a Assistant Professor Grade III of MCA dept in Acharya Institute of Technology, Bangalore, Karnataka, India from 19th Aug,2013. His areas of interest are Artificial Intelligence, Natural Language Processing and Image Processing. He has published 49 papers in International Journals / Conferences.

Mousumi Paul, is a member of the IAENG,a Member of the Machine Intelligence Research Labs (MIR Labs). She obtained her MCA in the year 2010, from the Academy Of Technology, under WBUT. She is presently working as a Lecturer of Computer Science & Technology in Elite Polytechnic Institute, West Bengal, India.Beside of this She is doing PhD from NIT Durgapur, West Bengal. Her research topic is "Vehicular Ad-Hoc Network" and she was working her research on this topic for last two years. She published 12 papers in International Journals / Conferences.