A Survey on Password Authentication Using Godel Number

Dr.A.S.N.Chakravarthy* **Prof.S.Balaji**** **M.Pavani*****

* (Professor, Department of Electronics and Computer Engineering, KL University, India)
**(HOD,Department of Electronics and Computer Engineering, KL University, India)
*** (Research Scholor, Department of Electronics and Computer Engineering, KL University, India)

ABSTRACT

Password Authentication is the most commonly accepted means for entity authentication. In this paper, a novel approach is designed for Password authentication using a technique called Godelization. There have been many proposals in recent years for password authentication. To meet the increasing need of preserving individual privacy, anonymous password authentication has been proposed recently, to augment password authentication with the protection of user privacy. The key which is to be transmitted is transformed into a sequence called Godel Number Sequence (GNS) using a new technique called Godelization. Digital watermarking and Steganography techniques are used to address these types of problems like protecting information and concealing secrets. As these techniques suffer from various limitations, we use Godelization technique.

Keywords - Password Authentication, Godelization, Godel Number Sequence

I. INTRODUCTION

Security is the degree of protection against danger, damage, loss, and crime. Securities as a form of protection are structures and processes that provide or improve security as a condition. Network security can be constructed by defining its two components, security and networks. Security may be given a wide variety of definitions. Security is the freedom from danger or anxiety. Security can also be defined as follows:

- A situation with no risk, with no sense of threat
- The prevention of risk or threat
- The assurance of a sense of confidence and certainty

Security is described through the accomplishment of some basic security properties, namely confidentiality, integrity, and availability of information. Confidentiality is the property of protecting the content of information from all users other than those intended by the legal owner of the information. The non intended users are generally called unauthorized users. Other terms such as privacy have been used almost synonymously with confidentiality. However, the term privacy represents a human attribute with no quantifiable definition. Integrity is the property of protecting information from alteration by unauthorized users. Availability is the property of protecting information from non authorized temporary or permanent with holding of information.

In simple terms, authentication is identification plus verification. Identification is the process whereby an entity identity, rather than one-way authentication, where by only one principal verifies the identity of the other principal, is usually required.

There are three main types of authentication in a computing system[1]:

a. Message content authentication -verifying that the content of a received message is the same as when it was sent; in a computing environment.

b. Message origin authentication - verifying that the sender of a received message is the same one recorded in the sender field of a message; and

c. General identity authentication - verifying that a principal’s identity is as claimed.

Password Authentication [2] is one of the simplest and the most convenient authentication mechanisms to deal with secret data over insecure networks. It is more frequently required in areas such as computer networks, wireless networks, remote login systems, operation systems, and database management systems. The use of passwords is the primary means of authenticating a user. Unfortunately, it is also the weakest form of authentication. In today's digital world, the ways to bypass this form of security are trivial. While many enterprises focus on strengthening passwords, these efforts are by and large meaningless in the face of the tools that attackers can use. The tools provide criminals with easy ability to hack, trap, or crack most passwords easily.

Type of Password Authentication is Dynamic Authentication. One-time password techniques primarily use some sort of cryptographic primitives (crypto random number generators, one-way hash functions, symmetric encryption/decryption, etc.) to generate a new unique password every time authentication is required. There are three prominent methods of implementing dynamic one-time password based authentication solutions in enterprises. They are Time-Synchronous Technique, Event Synchronous Technique, Asynchronous Challenge-Response Technique.

1.1 GODEL NUMBER

In theory of computation, it is extremely important to be able to code statements of a programming language into numbers. With the coding in place, you can then describe important concepts like universality and the unsolvability of the halting problem (assuming you have an acceptable programming system).

Anyway, one way of doing the coding is called Godel numbering. For a sequence of numbers, a1, a2, a3 ... aN, the Godel number, written (a1,a2,a3,...aN), is defined as

[a1,a2,a3,...aN] = p1^a1 * p2 ^a2 * p3^a3 * ... * pN^aN

The ‘a’ values are arbitrary numbers (each value represents one statement in the language). The p numbers are prime numbers. p1 = 2, p2 = 3, p3 = 5, etc. A Godel number takes each p and raises it the its corresponding a power, and multiplies all them together. The Godel number of (1, 3) is 2^1 * 3^3 = 54. As you can see, Godel numbers tend to get quite large.In this problem, we'll be converting Godel numbers to their sequences, and taking sequences giving their Godel numbers. For this problem, you may assume that you will need, atmost, the first 80 primes

Input:

Each test case spans multiple lines. The first line of a test case will consist of exactly one character, either a G or an I.

If the first line had a G on it, the next line will be a number, N. N is between 1 and 80 inclusive. Following that line, will start a string of N numbers, separated by an arbitrary amount of white space. The list of numbers may span multiple lines. However, after the last number, there will be a end of line character (i.e., another test will not start on the same line that the previous case ended on). All numbers are positive integers.

If the first line had an I on it, the next line will contain a single number. That number is a Godel number of some sequence, and is greater than 0.

There are multiple test cases in the input. No blank lines will ever appear. No characters, other than the ones described above will appear. .

Output:

For `G' input, print the Godel number of that sequence. The Godel number will fit within an unsigned 32 bit integer.

For `I' input, print the sequence determined by that Godel number. Print, at most, 20 numbers per line. Each number should be separated by a space. There should be no trailing 0s in your sequence (although, there may be 0s in your sequence, there should be none at the end).

No blank lines should appear in your output.

Sample Input:

```
G
2
1 3
G
10
1 0 0   0 0 0   1
1 0
1
I
498
Sample Output:
54
18734
1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 1
```

1.2 Overview of Gödel number sequence

The logician Kurt Gödel [3] developed an encoding scheme to assign numbers to statements and formulas in an axiomatic system. The first step is to encode sequences of numbers as a single number. This scheme depends on a theorem called prime factorization theorem, which states that every positive integer greater than one can be factored into primes, and this factorization is unique except for difference in the order of the factors. For any finite sequence x_o, x_1, x_2,….x_n of natural numbers, the Gödel number of the sequence is the number generated as GN(x_o,x_1, x_2,….x_n) = 2xo3x15x2…(PrNo(n))x_n where PrNo(n) is the nth prime.

II. RELATED WORK

As digitization of audio, video and other works are rapidly increasing; the ease with which perfect duplicate copies can be made is also increasing. The Internet has become so user friendly that it has become an excellent distribution system for digital media. However, content owners see a high risk of piracy and so they eagerly seek technologies that promise to protect their rights. Cryptography, Information hiding, Steganography, Digital watermarking are some of the techniques which are playing a significant role in the field of security.Steganography hides the very existence of a secret message and in the best nobody can see that the parties are communicating in secret. Steganography can be used to hide important data inside another file so that only the parties intended to get the message knows a secret message exists. Watermarking places the information within the content where it is never removed during normal usage. In fact, watermarking techniques are particular embodiments of Steganography. Steganography is not robust while watermarking has an additional feature, which is robustness (resistant to any type of distortions).

This paper proposes a novel methodology to overcome a few limitations by converting the image into a Gödel Number Sequence [4] and transmitted securely using encryption methods. In our proposed method we have devised a new combinational approach for data hiding and transmitting it securely using public key encryption methods. Data is transformed into strings of Godel numbers. To decrease the size of each string we compress the strings using the alphabetic coding technique which encodes the string like run length encoding scheme.

2.1 GÖDELIZATION:

The logician Kurt Gödel [3] developed an encoding scheme to assign numbers to statements and formulas in an axiomatic system which is based on prime factorization method. According to the proposed Gödelization method, it is a process of converting any positive integer which is greater than 1 into a sequence called Gödel Number Sequence(GNS)[4]. For any positive integer n>1, define GNS(n) = (x0,x1,……xk) where n= 2x0 * 3x1 * 5x3 … Pxk is the prime factorization of n. For example GNS(198) = (1,2,0,0,1) because 198 = (21)*(32)*(50)*(70)*(111). Although Gödel Numbering has been used for many applications, we use this scheme for encoding of digital images. Every digital image can be viewed as a sequence of intensity values ranging from 0 to 2m - 1 for some positive integer m. Thus if any image is represented by intensity values(i1, i2,……. in), then each of these intensity values can be converted into a Gödel Number Sequence GNS[2]. Then GNS(i1)$GNS(i2)$......$GNS(in) is called the Gödel String of the image.

2.2 ALPHABETIC CODING(AC):

Alphabetic coding is a process of compressing a given string of numbers. If an image has N intensity values then the Gödel String consists of the digits 0 to [log2N](apart from $ symbol).Normally N will be 255 and hence the Gödel string of any image will have numbers ranging from 0 to 7. Now 0,1,…,7 are replaced by A,B,….,H. If 3 or more characters are encountered in a sequence, then it is represented as KX where k is the number of occurrences of character X. So the string $100000001$0200000001 is encoded as $B7AB$AB7AB$. Here the length is reduced to 12 bytes from 21 bytes. With AC technique the length is reduced as well as second level of security is also provided.

2.3 ENCRYPTION:

This is a process of encoding a given text or a string into an unintelligible format. There are two types of encryption methods being used in literature, namely Symmetric Encryption and the Public Key Encryption[5]. In symmetric key encryption the sender uses a key (a secret string) to encrypt the message which upon receiving at the other end will be decrypted using the same secret key. That is, the secret key is known only to the sender and the receiver. However, in public key cryptography, both sender and the receiver will have two keys namely the public key and the private key. The sender encrypts the message using the receiver's public key and the receiver will decrypt it using his private key. Although any of the two methods may be used, in the proposed work symmetric key cryptography is adopted.

III. PROPOSED METHOD

The proposed technique involves three stages. The first stage consists of encoding the image into a Gödel String. In the second stage the Gödel string is compressed using Alphabetic coding which in the third stage will be encrypted using a symmetric key cryptosystem or a public key Cryptosystem. At the decoding end again there will be three stages to recover back the image which are the reverse process of the above three. The encoding, decoding algorithms and the schemes are given in the following sections.

3.1 ALGORITHM FOR GÖDELIZATION

The given image is converted to a Gödel string using the following algorithm.
Step 1: Read the intensity values of the input image.

Step 2: Generate the Gödel String of the image.

Step 3: Compress the Gödel String using Alphabetic coding technique.

Step4: Encrypt the string obtained in step3 using an symmetric key cryptosystem [5] with key K.

This encrypted string is transmitted to the other end. The scheme of the proposed encoding methodology is shown in Fig 1.

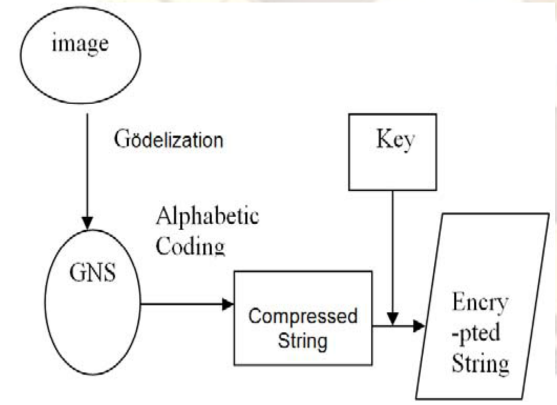

Fig1. Scheme for Gödelization Process

3.2 INVERSE GÖDELIZATION & INVERSE ALPHABETIC CODING TECHNIQUES

At the decoding end, there is a need to perform the inverse operations of Alphabetic coding and Gödelization techniques to obtain the original data. Inverse Alphabetic coding is the process of decompressing the string by replacing alphabets (A,B,…H) with digits(0,1,…7) and any substring KX is decompressed with K occurrences of X. The string obtained is in the form of GNS(i1)$GNS(i2)$......$GNS(in) which is the Gödel String of the image and inverse Gödelization is applied to the string to obtain the intensity values of the image which are calculated as GNS(i) = (x0,x1,……xk) where i= 2x0 * 3x1 * 5x3…. Pxk .

3.3 ALGORITHM FOR DECRYPTION

Once the encrypted form of the image is received the image can be reconstructed using the following algorithm:
Step 1: Decrypt the received string using the same symmetric key crypto system with the key K.
Step 2: Decompress the string using inverse Alphabetic Coding.
Step 3: Use inverse Gödelization for the string obtained in step 2 to get the intensity values of the image.
Step 4: Construct the image with the values obtained in step 3. The scheme of the proposed decryption methodology is shown in Fig 2.

IV. CONCLUSION

In this paper we have presented a technique for Password Authentication Using Godel Number which provides more security. This method is implemented using Encoding and Decoding methods.

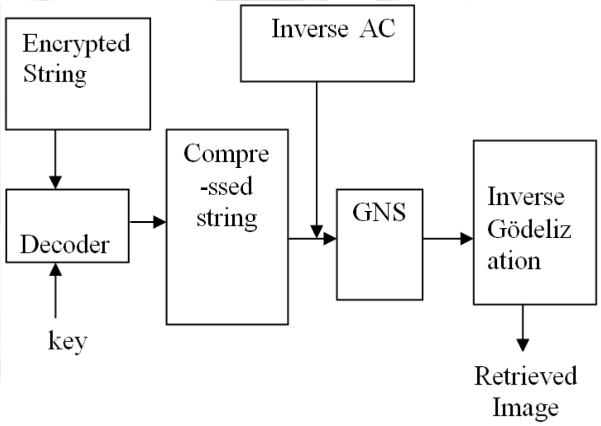

Fig 2. Scheme for decoding

ACKNOWLEDGMENT

The authors would like to thank everyone, whoever remained a great source of help and inspirations in this humble presentation. The authors would like to thank K.L. University management for providing necessary facilities to carry out this work

REFERENCES

1. Thomas Y.C. Woo and Simon S. Lam, "Authentication for distributed systems", IEEE transactions, pp. 39- 53, 1992
2. http://authenticationworld.com/password-authentication/index.html
3. John Martin, "Introduction to Languages and the theory of Computation", 3rd edition, TMH , pp no.462.
4. D.Lalitha Bhaskari, P.S.Avadhani, A. Damodaram, "A combinatorial Approach for Information Hiding Using Steganography And Godelization Techniques", Journal of IJSCI(International Journal of Systemics, Cybernatics and Informatics, pp 21-24, ISSN 0973-4864, 2007.
5. W. Diffie & M. Hellman, "New directions in cryptography", IEEE Trans. Information Theory, Vol.22, 1976, pp. 644-654.

AUTHORS PROFILE

Dr. A. S .N. Chakravarthy, currently working as Professor in Dept. of Electronics and Computer Engineering in K.L. University, Guntur. He has 24 papers published in various International journals and conferences. His research areas include Cryptography, Biometrics, and Digital Forensics. He is Editorial board member for various International Journals.

Prof. S. Balaji, currently working as HOD & professor in Dept. of Electronics and Computer Engineering in K.L. University, Guntur. He has published 21 papers in various national / international journals and conferences. His research areas are image processing, biometrics .

M.Pavani, pursuing M.Tech in Dept. of Electronics and Computer Engineering in K.L. University, Guntur.