Application of Modulo-2 Arithmetic in Securing Communicated Messages

Okike Benjamin, Garba EJD

Abstract— Today, the word encryption has become very popular even among non-computer professionals. There is no doubt that some works have been carried out in this area, but more works need to be done. Presently, most of the works on encryption is concentrated on the sender of the message without paying any attention to the message recipient. However, it is a good practice if any message sent to someone is received by the particular person whom the message is sent to. This work seeks to ensure that at the receiving end of the message, there is a security to ensure that the recipient computes a key that would enable the encrypted message to be accessed. This key would be in form of password. This would make it possible for a given message to be sent to several people at the same time. When this happens, it is only those people who computes the key correctly that would be given the opportunity to access even the encrypted message, which can in turn be decrypted using the appropriate key

Index Terms— Communicated Messages, Decryption Algorithm, Encryption Algorithm, Information Security, Modul0-2 Arithmetic,

1 Introduction

Information Security is an area in the field of computing which has not been given the much deserved attention. Bearing in mind the growing awareness in the use of the Internet to transact businesses throughout the globe, there is also a need to secure the information contained in those transactions from Internet information hackers, which they sometimes use for fraud. When information is protected by the use of encryption techniques, passwords, firewalls, etc, such information is less likely to be accessed by those to whom such information is not meant for. Encrypting information would prevent genuine business executives from fallen victims to Internet fraudsters. Again, this could be achieved through all the parties that may be involved in the business deal. This work seeks to ensure that only generated passwords are made available to the message recipient. The other information contained in the message is hidden until a correct password is entered. When a correct password is entered, a sequence of generated random integer values and their assigned bit values are revealed. With this, a key would be computed by the message recipient so as to reveal the encrypted message. If the correct password is entered, then the message can be decrypted accordingly. This would add one level of security to the encrypted information and avoid concentrating security at just one end, but, rather at both the sender and the recipient sides. Information Security is an area in the field of computing which has not been given the much deserved attention. Bearing in mind the growing awareness in the use of the Internet to transact businesses throughout the globe, there is also a need to secure the information contained in those transactions from Internet information hackers, which they sometimes use for fraud. When information is protected by the use of encryption techniques, passwords, firewalls, etc, such information is less likely to be accessed by those to whom such information is not meant for. Encrypting information would prevent genuine business executives from fallen victims to Internet fraudsters. Again, this could be achieved through all the parties that may be involved in the business deal. This work seeks to ensure that only generated passwords are made available to the message recipient. The other information contained in the message is hidden until a correct password is entered. When a correct password is entered, a sequence of generated random integer values and their assigned bit values are revealed. With this, a key would be computed by the message recipient so as to reveal the encrypted message. If the correct password is entered, then the message can be decrypted accordingly. This would add one level of security to the encrypted information and avoid concentrating security at just one end, but, rather at both the sender and the recipient sides.

1.1 Aims and Objective

The aims of this research work are to ensure that messages being communicated from a source to a destination are not accessed illegally. Again, if accessed illegally, the true meaning of such message would not be revealed since the message has been scrambled upon using an encryption algorithm. It is only with the appropriate decryption algorithm that the message would come out in its original form. The objective of this research work is to advance information security a step forward by ensuring that both the message sender and the message recipient have some level of security rather than concentrating security only at the sender’s point.

1.2 Aims and Objective

Due to the growing use of the computer for businesses throughout the globe, there is a need to also extend the security level in the messages contained in the transactions. This research ensures that the encrypted messages would only be revealed if the accurate key is computed by the message recipient. .This will in turn improve on the existing information security that is mostly carried out only at the message source without considering what happens at the message destination.

2 LITERATURE REVIEW

Relevant literatures relating to the field of Information Security are to be revealed at this point of this research. This would enable the researcher to be well equipped to improve on the existing system.

2.1 Definitions of Terms

Cryptography today might be summed up as the study of techniques and applications that depend on the existence of difficult problems. Cryptanalysis is the study of how to compromise (defeat) cryptographic mechanisms, and cryptology (from the Greek word kryptós lógos, meaning ``hidden word'') is the discipline of cryptography and cryptanalysis combined. To most people, cryptography is concerned with keeping communications private. Indeed, the protection of sensitive communications has been the emphasis of cryptography throughout much of its history. However, this is only one part of today's cryptography [1].

Encryption - In PC and LAN Security [2] defined encryption as the ability to scramble data so that it is inaccessible without a password of some kind in order to protect it from prying eyes. Encryption is the transformation of data into a form that is as close to impossible to read without the appropriate knowledge of the key. Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data. Decryption is the reverse of encryption; it is the transformation of encrypted data back into an intelligible form .

Symmetric Encryption - This is an encryption model that employs the use of single key for both the sender and the message recipient. The symmetric encryption may be otherwise called conventional, private or single key encryption since the same key is used to encrypt and decrypt the message.

Asymmetric Encryption - This is a process whereby a pair of keys are used. One is used for encryption and the other for decryption. This type of encryption is also called public key encryption.

Encryption Algorithm - it performs mathematical operations to conduct substitutions and transformations to the plaintext.

Ciphertext - This is encrypted or scrambled message produced by applying an encryption algorithm to the plaintext message using a given key.

Decryption Algorithm - This algorithm generates the ciphertext and the matching key to produce the plaintext.

Plaintext – Is the created message in the plain language, example message that is in English language.

Digital Signature -According to David [3], a digital signature functions for electronic documents like a handwritten signature does for printed documents. A digital signature actually provides a greater degree of security than a handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been altered either intentionally or accidentally since it was signed. Furthermore, secure digital signatures cannot be repudiated; the signer of a document cannot later disown it by claiming that the signature was forged. In other words, digital signatures, which are codes unique to a particular message enable "authentication" of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

Protocol – This is a Set of rules governing the flow of information within a communication device.

Encryption key - is a randomly generated set of numbers/characters that is used to encrypt/decrypt information

Firewall - In Managing Internet Information Services, Cricket [4], specified that the main purpose of firewall is to prevent unauthorized access between networks. Generally, firewall is the means of protecting a site' s inner network from the Internet. Networks with firewalls enable decisions on what should and should not be allowed across the firewall. These decisions should stem directly from the site's security policy.

Address – Is a character or group of characters that specifies the recipient or originator of transmitted message.

Gateway – David in his Guide to Local Area Networking defined gateway as a combination of software and hardware that interconnects incompatible network devices.

ISO – is an acronym for International Standard organization. It is based in Geneva, and is responsible for many data communication standard.

Packet – This contains fixed amount of data and control instructions that is used to transmit data from source to destination.

Session – Is a set of packets to be transmitted in a network.

Router - Is a device that receives packets from one network and forwards them to another network.

2.2 Private key Encryption

With symmetric key encryption, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption. Implementations of symmetric key encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

With symmetric key encryption, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption. Implementations of symmetric key encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

Symmetric key encryption is effective only if the symmetric key is kept secret by the two parties involved. If anyone else discovers the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key not only can decrypt messages sent with that key, but also can encrypt new messages and send them as if they came from one of the two parties who were originally using the key.

By using highly complex encryption keys rather than simple substitution, it can prove quite effective in securing messages.

2.3 Public Key Encryption

1976 saw the introduction of a radical new idea into the field of cryptography. This idea centered around the premise of making the encryption and decryption keys different - where the knowledge of one key would not allow a person to find out the other. Public key algorithms are based on the premise that each sender and recipient has a private key, known only to the one and a public key, which can be known by anyone. Each encryption/decryption process requires at least one public key and one private key.

One solution to the use of symmetric encryption is in asymmetric encryption, also known as public key encryption. In this form of encryption, each person has a pair of keys. One key is a public key, which can be made freely available, even advertised in a directory for all to see. The other key, which is kept secret, is a private key. A message encoded with a particular public key can only be decoded using the corresponding private key, and vice versa.

2.4 Digital Signature

Digital signatures are created and verified by means of cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. For digital signatures, two different keys are generally used, one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form.

Suppose one (sender) wants to send a signed message to another (the recipient). The sender creates a message digest by using a hash function on the message. The message digest serves as a "digital fingerprint" of the message; if any part of the message is modified, the hash function returns a different result. After this, the sender, s private key is used to encrypt the message digest. This encrypted message digest is the digital signature for the message. After that, both the message and the digital signature is sent to recipient.

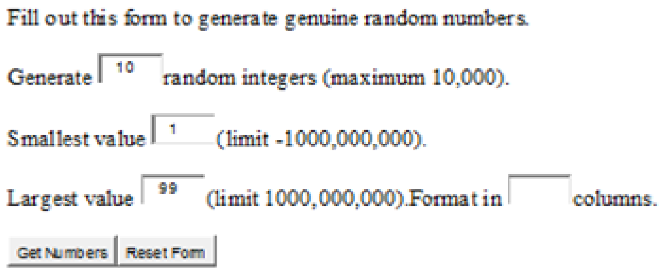
When the message and the message digest are received, the message digest is then decrypted using the sender’s public key. To verify the message, the recipient then hashes the message with the same hash function that the sender used and compares the result to the message digest he received from the sender. If they are exactly equal, the recipient can be confident that the message did indeed come from sender and has not changed since it was signed. If the message digests are not equal, the message either originated elsewhere or was altered after it was signed.

3 INFORMATION SECURITY USING MODULO-2 ARITHMETIC

Modulo-2 arithmetic in simple terms means to take the remainder of the number when divided by 2. In the application of modulo-2 in information security, the addition in modulo 2 arithmetic will be replaced by the exclusive OR (often written XOR or EOR) logic operation [5]. In XOR operation, the function is 1 when an odd number of its variables are one (1), and has a function as zero (0) when the number of its variables are even. This characteristic makes XOR function useful to check if the number of ones (1s) in a word is even or odd [6].

3.1 Random Sequence Generator

In order to make the code very difficult to decode, the researcher employed the use of integer random sequence generator. Presently, there are many Integer Random Sequence Generators. However, the researcher employed Random Integer Sequence generator by Mads as shown in figure 1 below [7]:


Fill out this form to generate genuine random numbers.

Generate 10 random integers (maximum 10,000).

Smallest value 1 (limit -1000,000,000).

Largest value 99 (limit 1000,000,000).Format in columns.

Figure 1: Random Integer Sequence generator by Mads

From figure 1 above, it is easy to see that each generation of random integer sequence may range from –1,000,000,000 to 1,000,000,000. Having examined some other encryption models and observed the complexities in some of those models, the researcher decided to restrict the figures that may be used for the encryption to only two digits.

To deploy the use of Modulo-2 Arithmetic operation in Information security, the steps are outlined below as follows:

i. Generate any ten (10) random integers (R/I) using appropriate tool

ii. Assign each of the random integer a bit value (B/V)

iii. Compute the binary values for the random integers

iv. Sum up binary values with bit values of zeros (0s) together using modulo-2 arithmetic (Exclusive Or (XOR) operation

v. Convert the result in (iv) to a decimal digit

vi. Send the decimal digit together with the generated random integers and the encrypted message, making only the decimal digit visible to the message recipient.

vii. On receipt of the message, the displayed decimal digit is used as a password to reveal the generated random integers and their assigned bit values

viii. Compute the binary values of the generated random integers and sum up the bit values of ones (1s) together

ix. Use the result of (viii) to reveal the encrypted message and decrypt it by the application of appropriate algorithm.

At this point, it would be necessary to use an example to illustrate how this works using the steps outlined above:

i. Generating any ten (10) random integers using appropriate tool. This is shown in table 1 below:

Table 1: Ten Random Integers

S/N	Random Integer
1	95
2	44
3	84
4	12
5	3
6	76
7	23
8	74
9	64
10	7

ii. Assigning each of the random integer a bit value as shown in table 2 below:

Table 2: Random Integers and Assigned Bit Values

S/N	Random Integer (RI)	Bit Value
1	95	1
2	44	0
3	84	0
4	12	1
5	3	0
6	76	1
7	23	1
8	74	0
9	64	1
10	7	0

iii. Computing the binary values for the random integers is shown in table 3 below:

Table 3: Random Integer, Assigned Bit Value and Computed RI Binary Values

S/N	Random Integer (RI)	Bit Value	RI Binary Value
1	95	1	1011111
2	44	0	0101100
3	84	0	1010100
4	12	1	0001100
5	3	0	0000011
6	76	1	1001100
7	23	1	0010111
8	74	0	1001010
9	64	1	1000000
10	7	0	0000111

iv. Summing up binary values with bit values of zeros (0s) together using modulo-2 arithmetic (Exclusive Or (XOR) operation

$$\begin{array}{c} 0101100 \\ 1010100 \\ 0000011 \\ 1001010 \\ \underline{0000111} \\ 0110110 \end{array}$$

v. Converting the result (iv) to a decimal digit by summing up place values of ON bits

32 + 16 + 4 + 2 = 54

vi. Send the decimal digit together with the generated random integers and the encrypted message, making only the decimal digit visible to the message recipient.

The decimal digit 54 is sent with the generated random integers and the encrypted message, but only the 54 will be displayed.

vii. On receipt of the message, the displayed decimal digit is used as a password to reveal the generated random integers and their assigned bit values

The recipient would use 54 as a password to reveal table 2 as earlier shown.

viii. Viii. Using table 3 to Sum up the binary values with bit values of ones (1s) together and convert to a decimal digit by adding the place values of ON bits.

$$\begin{array}{c} 1011111 \\ 0001100 \\ 1001100 \\ 0010111 \\ \underline{1000000} \\ 1001000 \end{array}$$

64 + 8 = 72

ix. Use the result of (viii) to reveal the encrypted message and decrypt it by the application of an appropriate algorithm.

The decimal digit 72 is used to access the encrypted message which can then be decrypted using an appropriate algorithm.

With the above technique, the same message could be sent to several recipients at the same time, but access to even the encrypted message can only be possible if accurate key is computed by the recipient of such message. This would in turn improve on information security.

4 SUMMARY

The researcher has been able to take information security to higher level whereby by the message recipient could only access encrypted message by computing appropriate key, otherwise, access to the encrypted message would be denied. Hence rather than ensure that information being communicated is secured at the source, the security of the information should also be ensured at the destination, thereby improving on information security.

Refernces

[1] M. Ajtai, and C. Dwork, “Public Key Cryptography”, 1997. http://axion.physics.ubc.ca/email-privacy.html

[2] C. Stephen, “PC and LAN SECURITY”, R. R. Donnelley & Sons, Indiana, pp.263- 276, 1998.

[3] Y. David, “Digital Signature”, 2002. http://www.megasign.nl/Helpdesk/introsignature.htm#1

[4] L. Cricket, “Firewall and Information Services”, O’Reilly & Associates, United States of America, pp. 498-500, 1994.

[5] B. Saleem, “Encryption- Information and Coding”, 1995. URL:http://www.cs.ucl.ac.uk/staff/s.Bhatti/De-notes/node33.html

[6] O. Obasogie, “Fundamentals of Digital and Analogue Computer Design”, Lamlak Nigeria Limited, Warri, P. 38, 1995.

[7] H. Mads. ‘True Random Numbers”, 2002. http://www.random.org/mads