A SECURED MESSAGE TRANSACTION APPROACH BY DYNAMIC HILL CIPHER GENERATION AND MESSAGE DIGEST CONCATENATION

M. Ismail Jabiullah[1], Md. Zakaria Sarker[2], Anisur Rahman[3] and M. Lutfar Rahman[4]
[1]Department of Software Engineering, Daffodil International University,
[2]Institute of Science and Technology, National University, Dhanmondi, Dhaka.
[3]Department of Computer Science and Engineering, Daffodil International University
[4]Department of Computer Science and Engineering, Dhaka University, Bangladesh.
E-mail: mijjabi@daffodilvarsity.edu.bd

Abstract: *Secured message transactions are very much desirable for electronic communications in so many ways. A secured message transaction technique has been designed, developed and implemented using Java programming language. For this, a symmetric key encryption technique dynamic Hill cipher has been used for message encryption-decryption with a dynamic key length. A square-matrix of the given key length has been generated with the property that modulo operation of the product of the matrix and the inverse of that matrix is identity. The intended message is converted into binary form. Performs the bitwise-XOR operation of the equal two halves of the binary form and repeats the operations 3 times to generate the message digest (MD), and concatenate it with the message. Encrypts them using the Hill cipher technique with the key matrix and then send them to the destination. In the receiving end, the reverse process is performed to retrieve the message in secured manner. This process can be applied in many cryptographic applications as well as research works.*

Key Words: *Security, Message Security, Message Digest, Hill Cipher and Cipher.*

1 Introduction

Secured message transactions are the procedures to transfer the messages among the communicating parties with message confidentiality, message authentication, and message integrity. Several approaches are used to implement the mentioned security services. Message encryption establishes the confidentiality and authentication in the message transaction [1]. Message encryption and concatenation of message digest performs the message integrity service. Any cryptographic system that performs all the security services is very much desirable for secured electronic communication [2]. To establish a safe and secured transaction system, one needs an encryption process, a message digest algorithm and the combing process. In this process, Hill cipher technique with dynamic key, the complex matrix operations, modular arithmetic operations and bit-wise XOR operations are used for better security strength [3]. In Hill cipher technique, the encryption algorithm takes m successive plaintext letters and substitutes for them m successive ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value. The encryption process composed of the product of the key matrix and the plaintext column vector and is expressed as C = KP mod T, where C is the ciphertext as column vector, K is the square matrix, P is the plaintext as the column vector and T is the index of the symbolic table. Decryption process requires using the inverse of the key matrix K. The inverse matrix K^{-1} of the key matrix K is defined by the equation $KK^{-1} = K^{-1}K = I$, where I is the matrix that is all zeros except for ones along the main diagonal from upper left to the lower right. It is easily seen that if the matrix K^{-1} is applied to the ciphertext, then the plaintext is recovered. In modular arithmetic operations, the mod n, operator maps all integers into the set of

Table 1 XOR Table of A and B

A	B	A XOR B
1	1	1
1	0	1
0	1	1
0	0	0

integers [4]. This suggests that the modular arithmetic exhibits the addition, subtraction and multiplication as the fundamental properties. In bitwise-XOR operation, the operation with the two 0 bits produces 0 and otherwise produces 1. This can be expressed as in the Table 1.

The plaintext message is broken up into blocks of length n in a Hill cipher encryption process, according to the m x n matrix chosen. Each block of plaintext letters is then converted into a vector of numbers and is treated it with the matrix. The results are then converted back to letters and the corresponding ciphertext message is produced from the plaintext. For decryption of the ciphertext message, the inverse of the encryption matrix must be found. Once found, the decryption matrix is then placed with each n-block of ciphertext message, that producing the plaintext message [5].

In this paper, a symmetric message transaction approach has been designed, developed and implemented by using the dynamic Hill cipher generation techniques. The key generation has been performed by mathematical operations of modular inverse matrices. The key is composed of only the matrices whose modular operations maintain the inverse properties. Here length of the matrix is selected dynamically. Symmetric key encryption/decryption operations are used as cryptographic mechanisms. For establishing the message integrity in the transacted message, bit-wise XOR operations are used to produce the message digest and concatenated to the encrypted message and then transmitted to the destination.

2 Conventional Message Transactions

Message encryption by itself can provide a measure of message authentication, and message confidentiality. Consider the straightforward use of symmetric-key encryption on the transmitted message. A message M transmitted from source A to the destination B is encrypted by a conventional cryptographic mechanism using a secret key K shared by the sender A and as well as receiver B. If no other party knows the secret key K and no other party can decrypt the transmitted message, then the confidentiality of the message is provided. Here none can recover the plaintext of the message. It is clear that B is assured that the message came was generated by the sender A. The message must have come from the sender A, because A is the only other party that possesses the secret key K and therefore the only other party with the information necessary to construct ciphertext that can be decrypted with the secret key [1]. Furthermore, if the transmitted message M is recovered, the receiver knows that none of the bits of the message M have been altered in the transit, became an opponent that does not know the secret key K would not know how to alter bits in the ciphertext to produce desired changes in the transmitted plaintext. So, it can be said that symmetric key encryption provides message authentication as well as the message confidentiality in the message transaction process.

However, this flat statement needs to be qualified. Consider exactly what is happening at the receiver B. Given a decryption function D and a secret key K, the destination will accept any input X and produce output Y = Dk(X). If X is the ciphertext of a legitimate message M produced by the corresponding

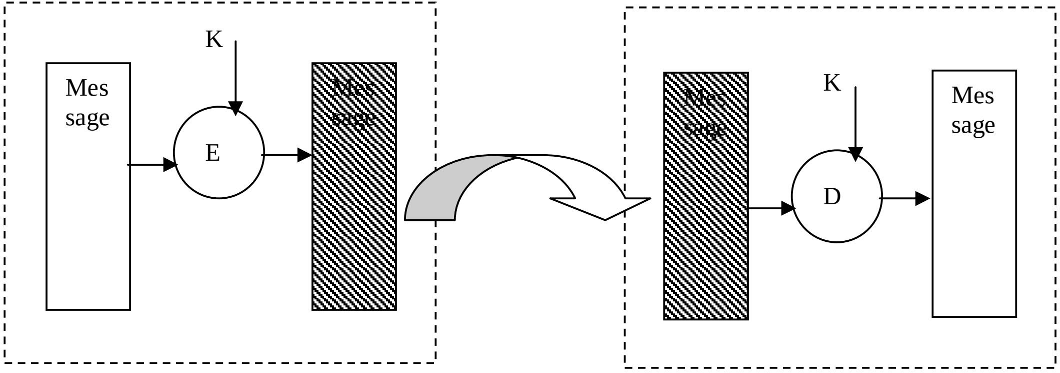

Fig. 1 Secured Message Transaction using Message Encryption

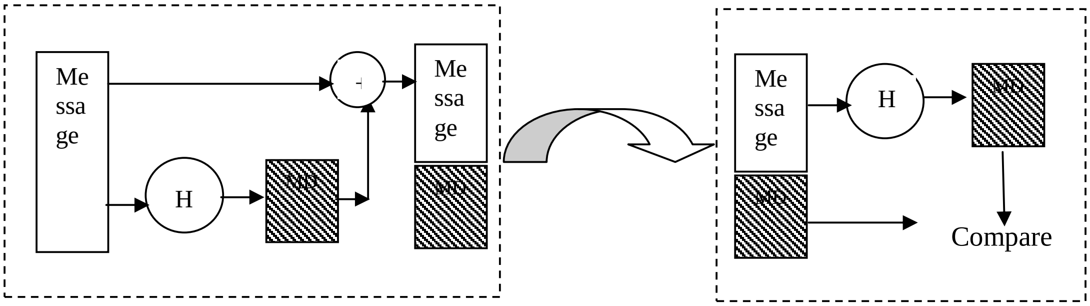

Fig. 2 Secured Message Transaction with Message Digest Concatenation

encryption function E, then Y is some plaintext message M. Otherwise, Y will likely be a meaningless sequence of bits. There may need to be some automated means of determining at sender B whether Y is legitimate plaintext and therefore must have come from A [6].

An alternative message authentication technique involves the use of hash function to generate a small fixed-size block of data, known as cryptographic check-sum or message digest (MD) that is appended to the message [7]. This technique assumes that the two communicating parties, say A and B, share the same process of digest generation. When A has a message to send to the destination B, it calculates the message digest (MD) of the message and concatenates it with the message [8]. The message plus the MD are transmitted to the destination B. Then B performs the same operations as the message digests function to produce the MD.

If only the receiver and the sender know the process of message digest generation technique and if the received MD and the generated MD matches, then:

(i) The receiver B is assured, that the message has not been altered. If an attacker alters the message but does not alter the digest MD, then the receiver's calculation of MD will differ from the received MD.

(ii) The receiver is assured that the message is come form the alleged sender. Because, no one else knows the message digest generation techniques, no one else could prepare a message with proper MD [9].

3 Methodology

In a Hill cipher encryption, the plaintext message is broken up into blocks of length n according to the m x n matrix chosen. Each block of plaintext letters is then converted into a vector of numbers and is dotted with the matrix. The results are then converted back to letters and the ciphertext message is produced. For decryption of the ciphertext message, the inverse of the encryption matrix must be found. Once found, the decryption matrix is then dotted with each n-block of ciphertext, producing the plaintext message [5, 10].

The developed process establishes the secured message authentication both by secret key encryption and by generating message digest generation.

Algorithm: The algorithm composed of the following steps:

Step 1: Sender selects a key length that is used as the length of the key matrix.

Step 2: Generate a square matrix (M) of length K which has an inverse matrix (M^{-1}) with the property that the product of the key matrix and the inverse matrix with modulo operation produces identity matrix (I). That is, M x M^{-1} = I. The matrix M is used as the K in the encryption process and the inverse matrix M^{-1} is sent to the destination to use for decryption.

Step 3: Enter the transmitting message (P) and perform Hill cipher encryption technique to produce ciphertext (C). That is, C = E_K(P).

Step 4: To generate message digest (D), performs the bit-wise XOR operation in the equal two halves of the message P. Then again perform the bit-wise XOR operation in the equal halves of the produced previous output and again perform the same operation in the last output and final output is the digest D.

Step 5: The generated message digest D is concatenated to the ciphertext (C) and is sent to the destination B.

Step 6: In the destination, receiver B first decrypt the ciphertext C using the received inverse matrix M^{-1} and the decryption algorithm Hill Cipher method to produce the plaintext P.

Step 7: Receiver B then performs the same operations bit-wise XOR on the plaintext and calculates new message digest MD' and compare it with the received message digest MD and determine the integrity of the message.

The process of the proposed system is given in Fig. 3.

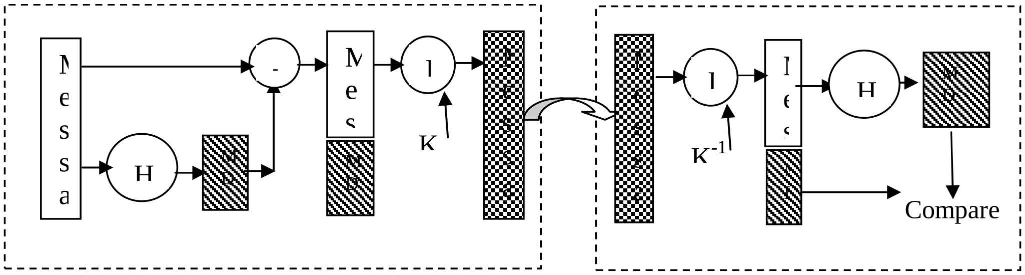

Fig. 3 Secured Message Transaction Dynamic Hill Cipher Encryption with Message Digest Concatenation

4 Implementation

The proposed method has been implemented using the Java programming language because of its simplicity, better security and its better interactive property with the users. If the program is run, then it takes 8 as the key length of the key matrix. The key matrix K is generated and also generated inverse matrix K^{-1}. If “PAY MORE MONEY” is inputted as the plaintext message (P), the message if first converted into binary form and perform bitwise-XOR operation on the two halves of the message to produce the message digest (MD) and concatenated it with the message and then encrypted it using the dynamic Hill cipher technique that produces the ciphertext (C) and sent it to the destination. The reverse operations are performed successfully that establishes the desired security services.

5 Security Analysis

Any security system performs the fundamental security services: confidentiality, authentication, integrity checking and non-repudiation. The proposed system performs all the security operations and is given in Table 2.

Table 2 Comparative Security Services

Systems	**Confidentiality**	**Authentication**	**Integrity**	**Non-repudiation**
Message Authentication with Encryption	Yes	Yes	No	No
Message Authentication with Message Digest	No	Yes	Yes	No
Proposed System	Yes	Yes	Yes	Yes

6 Conclusions

A secured message transaction technique has been designed, developed and implemented. A symmetric-key encryption technique Hill cipher has been used for message encryption-decryption with a dynamic key length. A square-matrix of the given key length has been generated with the property that modulo operation of the product of the matrix and the inverse of that matrix is identity. Then, the intended message is converted into binary form. The bitwise-XOR operation has been performed in the equal two halves of the binary form of the message and the operations have been repeated 3 times to generate the message digest (MD), and then concatenated it with the message. Encryption is performed on them using the Hill cipher technique with the key matrix and then has been sent them to the destination. In the receiving end, the reverse process has done to retrieve the message in secured manner. Here, key generation is dynamic and is fully depending on the length of the messages, computational complexity is harder because of matrix operations and can be developed for further improvement as dimensions. Only long messages can be encrypted-decrypted by using the proposed method. This process is suitable in many cryptographic applications as well as research works in the secured message transactions.

References

[1] W. Stallings, “Cryptography and Network Security – Principles and Practices”, 3rd Edition, 4th Indian Reprint, 2004, ISBN: 81-7808-902-5.

[2] M. Ismail Jabiullah, M. Abdullah Al-Shamim, M. rezaul Huq chowdhury, M. Humayun Kabir and M.L. Rahman, "Two-Level Message Authentication using Generated Session-key", In the Proceedings of Indonesia Cryptology and Information Security Conference, INA-CISC 2005, pp: , Jakarata, Indonesia, March 30-31, 2005.

[3] R. Islam, “Enhanced Security in Mobile IP Communication”, Masters Thesis, Department of Computer and System Sciences, Stockholm University, Royal Institute of Technology, February, 2005.

[4] “Mobile IP Security Survey”, www.docs\cse574-06\ftp\mobile_ip\index.html

[5] D.R. Stinson, Cryptography: Theory and Practice, 2nd ed. 2002, Boca raton: Chapman & Hall/CRC Press.

[6] M. Ismail Jabiullah, S. Rafique and M.L. Rahman, "Performance Study of Message Digest Algorithms: MD5, SHA and RIPEMD", In the Proceedings of the Regional Physics Conference, Atomic Energy Center, Dhaka, Bangladesh, February 11–13, 2006.

[7] L. Buttyan and J. P. Hubaux, “Security and Cooperation in Wireless Networks”, A Graduate Text Book, ISBN: 9780521873710, July, 2007.

[8] A. Menezes, P. van, Oorschot, and S. Vanstone. Handbook of Applied Cryptography, CRC Press, 1996.

[9] S. Goldwasser and M. Bellare, “Digital Signatures”, Lecture Notes on Cryptography, 1997, pp. 96-118.

[10] K.ITO, “Encyclopedic Dictionary of Mathematics”, 1987, The MIT Press.

Dr. M. Ismail Jabiullah is now working as a Professor and Head, Department of Software Engineering, Daffodil International University. He received his B.Sc. (Hons.), M.Sc. in Mathematics from Dhaka University and Ph.D. degrees in secured electronic transactions in the network environment. He has participated in several National and International conferences for presenting his research papers. The number of his publication is 24 in National and International Scientific Journals and 66 conference papers in National and International conferences. His research interest includes network security, artificial intelligence, e-learning and Expert system for last 18 years. He is the life member of BPS, BSES, BCS, BAAS, Bangladesh Ganit Samity, Dhaka University Registered Graduate Association and DUBatch83 Forum.

Md. Zakaria Sarker is a B.Sc.(Hons.) student in Computer Science of Institute of Science and Technology (IST) affiliated with National University, Bangladesh.

Anisur Rahman is now working as a Lecturer of Computer Science and Engineering Department at Daffodil International University. He has obtained his B.Sc.Engg. in Computer Science and Engineering from the University of Asia Pacific in 2002. He is about to complete his thesis based M.Sc. Engg. in Computer Science and Engineering from Daffodil International University. His research interest is Cryptography, Network Security, E-Learning, E-Governance, E-Commerce, etc.

Dr. M. Lutfar Rahman is now working as a Professor, Department of Computer Science and Engineering, Dhaka University. He is a founder chairman of the Department of CSE, Dhaka University, also the founder Director, IIT, Dhaka University and also the founder Vice-Chancellor, Begum Rokeya University, Rangpur. He has participated in many National and International conferences for presenting his research papers. The good number of publication in National and International Scientific Journals and also more than 100 conference papers are published in National and International conferences. His research interests are many scientific arenas for last 40 years.