Hybrid Cryptographic System for Network Security

Nan Wut Yi lai, Zin May Aye
University of Computer Studies (Mawlamyine)
wyutyi20.6@gmail.com,zinmay110@gmail.com

Abstract

With the fast evolution of digital data exchange, security information becomes much important in data storage and transmission. Due to the increasing use of digital data in industrial process, it is essential to protect the confidential data from unauthorized access. To address these security concerns, various security protocols that are of symmetric key and asymmetric key type have been developed. In this paper, we present a software implementation of hybrid cryptographic system that combines the symmetric algorithm, Advanced Encryption Standard (AES), and the asymmetric algorithm (ElGamal). This hybrid algorithm that has been implemented also considers how to take care of the integrity of data using Secure Hash Algorithm (SHA-1). AES is used to encrypt data and thanks to its efficiency and security; it can execute at high speeds, and consume less computer resources of memory and processor time. However, AES algorithm suffers the distribution problem. ElGamal algorithm is used to encrypt AES key for key security and to solve key distribution problem.

***Keywords**: AES, ElGamal, Integrity, Security, SHA-1*

1. Introduction

Nowadays, Data and Information security are very important in the world. As the information communication technology advances, there is a need for strong interest in information security. Cryptography is a tool that helps to keep information confidential and to ensure its integrity and authentication. Data encryption is widely used in commercial, government applications and e-commerce transaction that are growing at an explosive rate. Cryptography provides privacy, authentication, integrity and security. Various cryptographic algorithms have been developed. There are different types of cryptographic algorithms used to protect sensitive data including symmetric and asymmetric techniques.

There are two classes of key-based encryption algorithm, symmetric (or secret-key) and asymmetric (or public-key) algorithms. The difference is that symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), whereas asymmetric algorithms use a different key for encryption and decryption, and the decryption cannot be derived from the encryption key Symmetric key algorithms can be divided into stream ciphers and block ciphers. These are broadly classified as Symmetric key algorithm (DES, TDES, Blowfish, RC4 and AES) and Asymmetric key algorithm (RSA, ECC and ElGamal cryptosystem).

AES is an approved symmetric key cryptographic algorithm that is a block cipher. It is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits. The algorithm consists of four stages that make up a round which is iterated 10 times for a 128-bit length key, 12 times for a 192-bit, and 14 times for a 256-bit key. AES is efficient, secure and very fast symmetric algorithm. But AES has key distribution problem because of using the same key. Therefore, Elgamal is used to solve this problem because a pair of key is used instead of single key. The security of the ElGamal algorithm depends on the usage of a pair of key including public key and private key. The key length of the ElGamal can range from 256-bit to arbitrarily long. A key length ranging from 1024 to 2048 btis are considered safe for the next year. SHA-1is the version of SHA with a 160-bits message digest. It takes a message of length at most 2^{64} bits. If the length of a message is equal to or greater than 2^{64} bits, it will not be processed by SHA-1. SHA-1 is a little slower to execute and presumbly more secure because it produces a 160 bits digest as opposed to the 128 bits. In this paper, the symmetric key (AES) algorithm is applied to encrypt data and asymmetric key ElGamal cryptosystem to encrypt the AES key. Moreover, Secure Hash Algorithm (SHA-1) is used to achieve message digest for data integrity.

The rest of this paper is organized as follows: Section 2 summarizes the related work in the area of cryptography techniques. In section 3, some useful background theories are introduced. Section 4 presents the implementation of our hybrid cryptographic system for network security. Finally, section 5 is the conclusion of the paper.

2. Related Work

Janakiraman et al. [1] presented the combination of AES symmetric encryption algorithm, ECC asymmetric encryption algorithm and MD5 hash algorithm as a hybrid cryptographic algorithm for robust network. In this hybrid system, ECC is used for key encryption; AES for data encryption and

MD5 for message digest respectively. In paper [2], they show how data can be sent to a receiver on more secure ways through sending e-mail. In their system ElGamal Encryption Algorithm is used for encryption and authentication is performed by a unique hash function. H. M. Oo [3] presented the arrangement of secure examination questions based on ElGamal algorithm. M Gobi et al. [4] presented a new digital envelope approach for secure electronic medical records. In their system, they used the hybrid cryptosystem that combines MD5 hash algorithm, AES and Hyper Elliptic Curve Cryptosystem (HECC).

In this paper, we employed the advantages of Advanced Encryption Standard (AES), ElGamal Cryptosystem and Secure Hash Algorithm to construct the hybrid cryptographic system for network security.

3. Background Theory

In this section, the essential background theory concerned with the system is discussed.

3.1 Cryptography

Cryptography is usually referred to as "the study of secret", while nowadays, it is most attached to the definition of encryption. Encryption is the process of converting ordinary information (plaintext) into unintelligible cipher text to secure it against unauthorized access of data and decryption is the reversed, moving from unintelligible cipher text to plaintext. Basically, the two methods of producing cipher text are stream cipher and block cipher. Stream ciphers perform an encryption function on each individual character within the message. Block cipher splits a message into individual parts or blocks and then performs the encryption function on each block.

3.2 Advanced Encryption Standard (AES)

AES algorithm consists of four stages that make up a round, which is iterated 10 times for a 128-bit length key, 12 times for a 192 bit length key and 14 times for a 256 bit length key. However, AES allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate an array of bytes and organized as a 4x4 matrix called the state. Each transformation takes a state and creates another state to be used for the next transformation or the next round.

"SubBytes" transformation is a non-linear byte substitution for each byte of the bock, using a substitution table(s-box).

"ShiftRows" transformation cyclically shifts (permutes) the bytes within the block.

"MixColumns" transformation groups 4-bytes together forming 4-term polynomials and multiplies the polynomials with a fixed polynomial mod (x^4+1).

"AddRoundKey" transformation adds the round key with the bock of data.

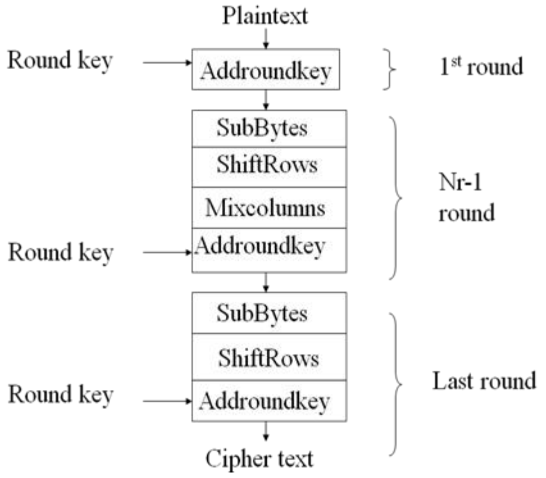


Figure 1. Encryption Process of AES Algorithm

Figure (1) shows the encryption process of the AES algorithm. The structure of each round consists of four transformations (SubByte, ShiftRow, AddRoundKey and MixColumn). The pre- round section uses only one transformation (AddRound Key) and the last round uses only three transformations (MixColumns transformation is missing)

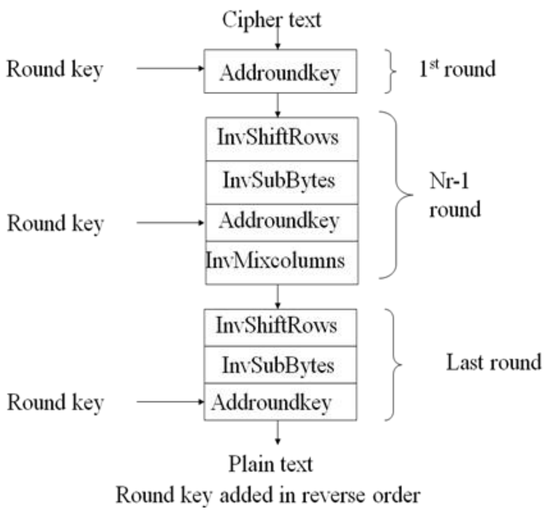


Figure 2. Decryption Process of AES Algorithm

Figure (2) shows the decryption process of the AES algorithm. Like encryption process, except the last, each round uses four transformations that are invertible. The inverse transformations are used: InvSubbyte, InvShiftRows, InvMixcolumns, and AddRoundkey (this one is self-invertible).

3.3. ElGamal Cryptosystem

In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public key cryptography. It was described by Taher Elgamal in 1985; ElGamal is based on the discrete logarithm problem. The ElGamal Cryptosystem is usually used in a hybrid cryptosystem i.e. the message is encrypted using a symmetric cryptosystem and ElGamal is then used to encrypt the key used for the symmetric cryptosystem. The security of the ElGamal cryptosystem depends on the difficulty of computing discrete logs in large prime modules. ElGamal can be used whenever RSA is used for key exchange, authentication, encryption and decryption. ElGamal Cryptosystem involves step A - key generation, step B - Elgamal encryption and step C - ElGamal decryption.

Step A: Key Generation

Step 1: Select a large prime p

Step 2: Select d to be a member of the group G=<Zp*, x> such that $1 \leq d \leq p-2$

Step 3: Select e_1 to be a primitive root in the group G=<Zp*, x>

Step 4: Compute $e_2 \leftarrow e_1^d \bmod p$, public key is ($e_1$, e2, and p) and private key is the (d_1).

Step B: ElGamal Encryption

Step1: Sender selects a random integer r in the group. G=<Zp*, x>

Step2: Compute $c_1 \leftarrow e_1^r \bmod p$, $c_2 \leftarrow (P \text{ x } e_2^r) \bmod p$

Step3: Then sender sends c_1 and c_2 to the receiver.

Step C: ElGamal Decryption

Step1: Receiver accepts the c_1 and c_2 from sender

Step2: Receiver uses private key (d) and compute $P \leftarrow [c_2 (c_1^d)^{-1}] \bmod p$ to decrypt message.

3.4 Secure Hash Algorithm (SHA-1)

SHA-1 proposed by NIST as a message digest function is the version of SHA with a 160-bits message digest. It takes a message of length at most 2^{64} bits and produces a 160 bits output. The processing consists of the following steps:

Step1: Appending padding bits: The message is padded so that its length is congruent to 448 modulo 512[length = 448(mod 512)]. Padding is always added, even if the message is already of the desired length. Thus, the number of padding bits is in the range of 1to 512. The padding consists of a single 1 bit followed by the necessary number of 0 bits.
Step2: Append length: A block of 64 bits is appended to the message. This block is treated as an unsigned 64 bits integer (most significant byte first) and contains the length of the original message (before the padding). At this point, the resulting message has a length that is an exact multiple of 512 bits.
Step3: Initialize hash buffer: A160 bits buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as five-32 bit register (a, b, c, d and e). These registers are initialized to the following 32 bit integers. <Hexadecimal values> A= 67452301, B=EFCDAB89, C=98BADCFE, D=10325476, E=C3D2E1F0
Step4: Process Message in 512 bit: (sixteen 32 bit words) block.
Step5: Output: After all N 512 bit blocks have been processed, the output from nth stage is 160 bit message digest.

4. Implementation of Hybrid Cryptographic System

The design and software implementation of hybrid cryptographic system was carried out in C# 2008. This hybrid cryptographic system is a combination of symmetric and asymmetric encryption techniques. . Figure 3 shows the overview of the system design.

P.T=Plaintext, AES(E)=AES Encryption, C.T=Cipher text, AES(D)=AES Decryption, ELG(E)=ElGamal Encryption, ELG(D)=ElGamal Decryption, Key(C.T)=Cipher text of AES key, MD=Message Digest, Comp=Compare.

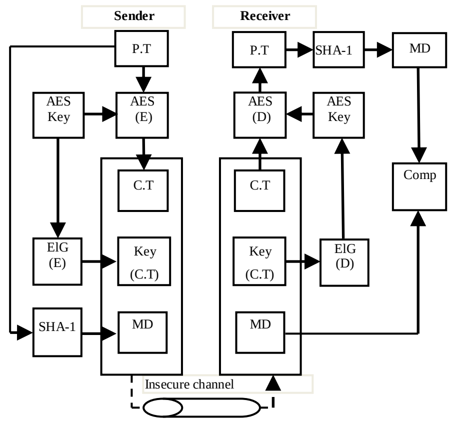


Figure 3. Overview of the system design

Figure 3 shows the overview of the system design. From the sender side, cipher text, AES cipher and message digest are sent through an insecure channel to the receiver. The message is encrypted with AES (symmetric) key. By using AES, there will be a key distribution problem. ElGamal (asymmetric) algorithm is used to encrypt the AES key to have a more secure key distribution over the network than using only AES encryption algorithm. Moreover, data integrity can be achieved by applied SHA-1.

4.1 Sequence of Operations in Sender Side

Figure 4 shows Sequence of operations in sender side. The operations are as follows:

Step1- The message (plaintext) that is to be transmitted is encrypted using the AES algorithm.
Step2- AES key used to encrypt the message is encrypted uisng ElGamal cryptosystem.
Step3- To ensure integrity of the transmitted message, it is subjected to SHA-1 algorithm. The message digest can be obtained by this process.
Step4- Then, sender sends ciphertext of the message, ciphertext of the AES key and message digest.

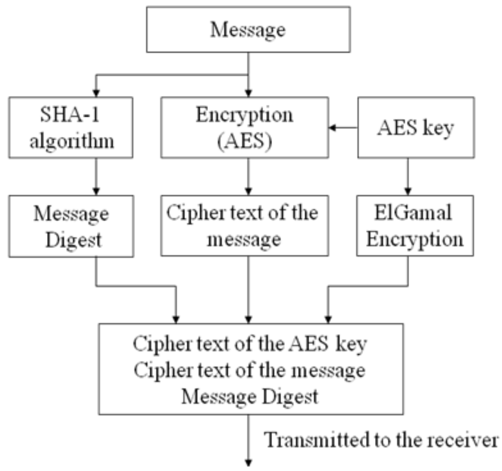
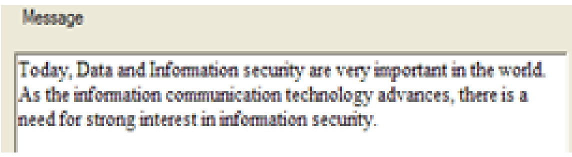


Figure 4. Sequence of Operations in Sender Side

The example message to be encrypted is shown in Figure 5.


Message

Today, Data and Information security are very important in the world. As the information communication technology advances, there is a need for strong interest in information security.

Figure 5. Plain Text

To ensure integrity of the transmitted message, it is subjected to SHA-1 algorithm. The message digest can be obtained by this process. Encrypted plain text byte and cipher text hex stream are shown in Figure 6.

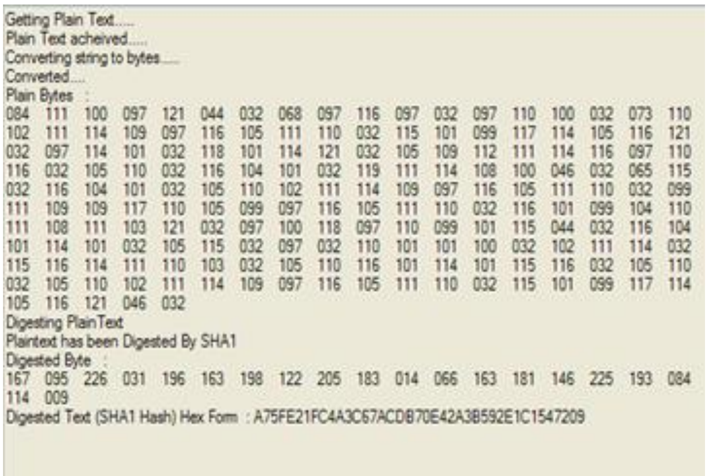

Getting Plain Text......
Plain Text acheived.....
Converting string to bytes.....
Converted.....
Plain Bytes :
084 111 100 097 121 044 032 068 097 116 097 032 097 110 100 032 073 110
102 111 114 109 097 116 105 111 110 032 115 101 099 117 114 105 116 121
032 097 114 101 032 118 101 114 121 032 105 109 112 111 114 116 097 110
116 032 105 110 032 116 104 101 032 119 111 114 108 100 046 032 065 115
032 116 104 101 032 105 110 102 111 114 109 097 116 105 111 110 032 099
111 109 109 117 110 105 099 097 116 105 111 110 032 116 101 099 104 110
111 108 111 103 121 032 097 100 118 097 110 099 101 115 044 032 116 104
101 114 101 032 105 115 032 097 032 110 101 101 100 032 102 111 114 032
115 116 114 111 110 103 032 105 110 116 101 114 101 115 116 032 105 110
032 105 110 102 111 114 109 097 116 105 111 110 032 115 101 099 117 114
105 116 121 046 032
Digesting PlainText
Plaintext has been Digested By SHA1
Digested Byte :
167 095 226 031 196 163 198 122 205 183 014 066 163 181 146 225 193 084
114 009
Digested Text (SHA1 Hash) Hex Form : A75FE21FC4A3C67ACDB70E42A3B592E1C1547209

Figure 6. Message Digest

The message (plaintext) that is to be transmitted is encrypted using the AES algorithm. Encrypted plain text byte and cipher text hex stream are shown in Figure 7.

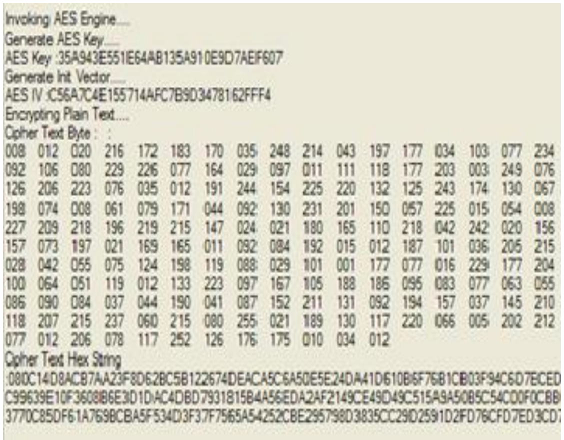

Invoking AES Engine....
Generate AES Key.....
AES Key :35A943E551E64AB135A910E9D7AEF607
Generate Int Vector.....
AES IV :C56A7C4E155714AFC7B9D34781 62FFF4
Encrypting Plain Text....
Cipher Text Byte : :
008 012 020 216 172 183 170 035 248 214 043 197 177 034 103 077 234
092 106 080 229 226 077 164 029 097 011 111 118 177 203 003 249 076
126 206 223 076 035 012 191 244 154 225 220 132 125 243 174 130 067
198 074 008 061 079 171 044 092 130 231 201 150 057 225 015 054 008
227 209 218 196 219 215 147 024 021 180 165 110 218 042 242 020 156
157 073 197 021 169 165 011 092 084 192 015 012 187 101 036 205 215
028 042 055 075 124 198 119 088 029 101 001 177 077 016 229 177 204
100 064 051 119 012 133 223 097 167 105 188 186 095 083 077 063 055
086 090 084 037 044 190 041 087 152 211 131 092 194 157 037 145 210
118 207 215 237 060 215 080 255 021 189 130 117 220 066 005 202 212
077 012 206 078 117 252 126 176 175 010 034 012
Cipher Text Hex String
:080C14D8ACB7AA23F8D62BC5B122674DEACA5C6A50E5E24DA41D610B6F76B1CB03F94C6D7ECED
C99639E10F3608B6E3D1DAC4DBD7931815B4A56EDA2AF2149CE49D49C515A9A50B5C54C00F0CBB
3770C85DF61A769BCBA5F534D3F37F7565A54252CBE295798D3835CC29D2591D2FD76CFD7ED3CD7

Figure 7. Generating Cipher Text

AES key used to encrypt the message is encrypted uisng ElGamal cryptosystem. Encrypted AES key byte and hex stream of the cipher text of AES key are shown in Figure 8.

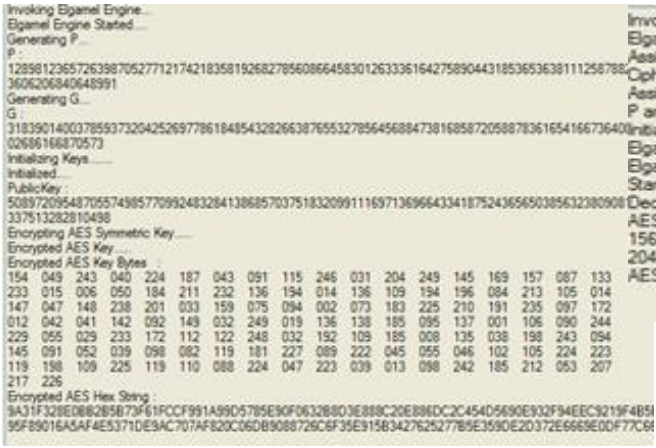


Figure 8. Generating AES Key Cipher

4.2 Sequence of Operations in Receiver Side

Figure 9 shows Sequence of operations in sender side. The operations are as follows:

Step1- Receiver accepts the ciphertext of the message, the cipher text of the AES key and message digest.

Step2- AES key is decrypted with ElGamal decryption.

Step3- The decrypted (AES) key is used to decrypt the ciphertext of the message to obtain the plaintext.

Step4- This plaintext is again subjected to SHA-1 hash algorithm to obtain message digest on the receiver side.

Step5- This message digest value is compared with the message digest sent from sender.

Step6- If both of them are equal, the message is accepted else rejected.

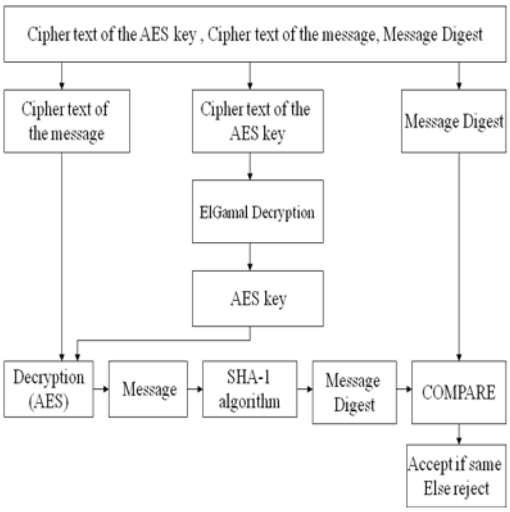


Figure 9. Sequence of Operations in Receiver Side

The decrypted (AES) key that is used to decrypt the ciphertext of the message to obtain the plaintext is shown in Figure 10.

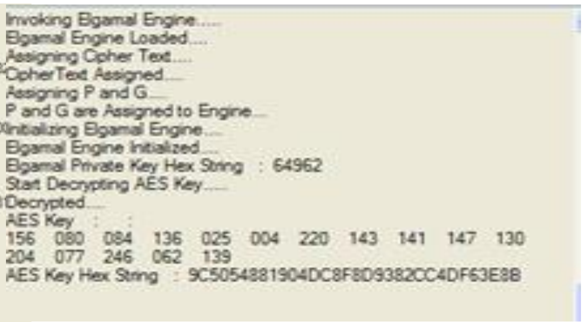


Figure 10. Decrypted AES key

The ciphertext of the message is decrypted with decrypted AES key. Byte stream and Hex stream of decrypted (original) message are shown in Figure 11.

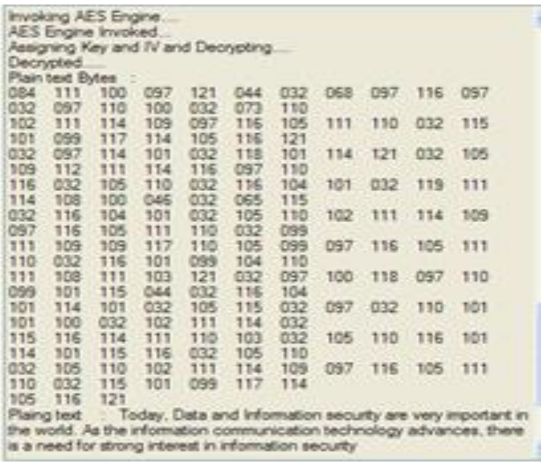


Figure 11. The original plaintext (Receiver Side)

The decrypted message is again subjected to SHA-1 hash algorithm to obtain message digest on the receiver side. This message digest value is compared with the message digest sent from sender. The message digest (Receiver Side) and comparing results of two message digest are shown in Figure 12.

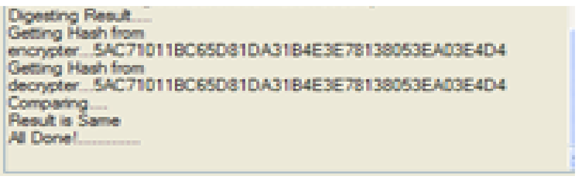


Figure 12. Comparing Digested Message Results

5. Conclusion

This paper, the hybrid cryptographic system which combines AES algorithm and ElGamal Cryptosystem for the data to be secured is implemented. To ensure message integrity, Secure Hash Algorithm (SHA-1) is applied. By using this system, we can obtain the security of confidential data and provide secure way for transmission of sensitive data. As a result, the hybrid cryptographic system can be applied in any critical applications, such as Military departments, Banking system and related areas.

References

[1] V.S. Janakiraman, R.Ganesan and M. Gobai, "Hybrid Cryptographic Algorithm For Robust Network Security", The International Congress for global Science and Technology, Coimbatore-641014, July 2007

[2] M. Dulgerler, M. N. Sarisakal, "A Secure E-mail Application using Elgamal Algorithm: MD Message Controller", Journal of Electrical & Electronics Engineering, Volume 3, number 1, 2003

[3] H. M. Oo, "Arrangement of Secure Examination Questions based on ElGamal algorithm", M.C.Sc (thesis) , May 2009

[4] M. Gobi and K. Vivekanandan, "A New Digital Envelope Approach for Secure Electronic Medical Records", IJCSNS International Journal of Computer Science and Network Security,VOL.9 No.1, January 2009

[5] U.S. Department of Commerce / National Institute of Standard and Technology. FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), November 2001

[6] C. Kaufman, R. Perlman, M. Speciner, "NETWORK SECURITY" PRIVATE Communication in a PUBLIC World, Second Edition, Prentice Hall Series in Computer Networking and Distributed Systems, USA, 2002,Pg 81-91, Pg 140-141