GUBJSE: ISSN: 2409-0476

A Double-key Based Encryption-Decryption Process for Stronger Secured Message Transactions

Md. Ismail Jabiullah, A. A. Md. Monzur-Ul-Akhir and Muhammad Rashiduzzaman

Abstract — A double-key based stronger secured electronic message transaction system has been designed and developed using Python programming language by performing encryption-decryption process. To do this, simple cryptographic encryption and decryption techniques are used with two keys avoiding vulnerabilities of a single key. First, the intended message is encrypted with the private key of sender (PR_a) and the output is again encrypted with a shared secret key (K_1) that generates ciphertext. The output ciphertext is again encrypted with another shared secret key (K_2) that generates a code that serves as Message Authentication Code (MAC), which is concatenated with the ciphertext. And again encrypted them with shared secret key K_1 that produced final ciphertext which is to be send to the intending recipient. The shared secret keys K_1 and K_2 are getting from the key distribution center (KDC). In the receiving end, receiver first decrypts the received information with the shared secret key K_1 that gives the ciphertext and MAC of the ciphertext, and then decrypts only the MAC to generate a new ciphertext′ and compare the new ciphertext′ with the received ciphertext that ensures the ciphertext authentication as well as message authentication; if ciphertexts are found same, then the ciphertext is decrypted with shared secret key K_2 and again is decrypted with the sender's public key (PU_a) and retrieve the message; otherwise discarded. This proposed system ensures the stronger authenticated message transactions among the communicants. Finally, a comparative study with the existing systems has also been performed and measured stronger security. This technique can be applied for any secured electronic information transfer system with stronger security services.

Index Terms — *Secret Key, Encryption, Decryption, Ciphertext and Message Authentication Code.*

I. Introduction

MESSAGE transaction in a secure fashion refers to the process of exchange message between communicating participants with message confidentiality, message integrity and message authentication. There are many techniques used to ensure the message security services. Message encryption technique ensures the confidentiality and authentication of message transaction [1]. Message encryption technique and concatenation of MAC, sometimes known as tag or cryptographic checksum which ensures the message integrity [2, 3]. Message authentication is a technique that permits communicating parties to verify the integrity of a message, i.e. message has not been modified or altered while in transit, and authenticity of a message, i.e. message came from an authentic sender [4, 5]. Message authentication is normally achieved by using MACs. A MAC is a cryptographic checksum generated based on a variable-length of message M using a secret key K shared only by sender and receiver. The process using MAC for authenticator is as follows:

$$MAC = E_K(M) \ldots \ldots \ldots \quad (1)$$

where MAC is message authentication code, E is encryption, K is the encryption key and M is the intended message.

If the sender A wishes to send a message M to the receiver B, and secures it with a MAC, both communicating parties must need to share a secret key K and agree on the MAC algorithm. Then, the MAC is calculated as a function (agreed algorithm) of message M using shared secret key K [6, 7].
Then, the sender A appends the MAC with message M and transmits to the receiver B. The receiver B calculates a new MAC called MAC′ by performing the same calculations on the message M and using the same secret key K. Then the receiver B, compare the received MAC with new code MAC′ to confirm the data integrity. As only communicating parties know the MAC algorithm and secret key; only the sender A is capable to calculate the MAC, hence the source authentication is also confirmed [8, 9]. Message authentication code (MAC) gives a systematic way to

This paper was received on 4 May 2020, revised on 4 October 2020 and accepted on 13 October 2020."

Md. Ismail Jabiullah is with the Department of Computer Science and Engineering, Daffodil International University, Bangladesh. E-mail: *drismail.cse@diu.edu.bd*.

A. A. Md. Monzur-Ul-Akhir is with the Department of Electrical and Electronic Engineering, Green University Bangladesh, Dhaka, Bangladesh, E-mail: *monzur@eee.green.edu.bd*.

Muhammed Rasheduzzaman is with Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh, E-mail: *rashid.shimul@gmail.com*.

message authentication. MAC also determines the authentication function from confidentiality. This feature is suitable for many applications where confidentiality is not mandatory. Message Authentication is one of the most important parts of network security. Message authentication is a procedure to verify that the received message has come from the stated source and the message has not been altered.

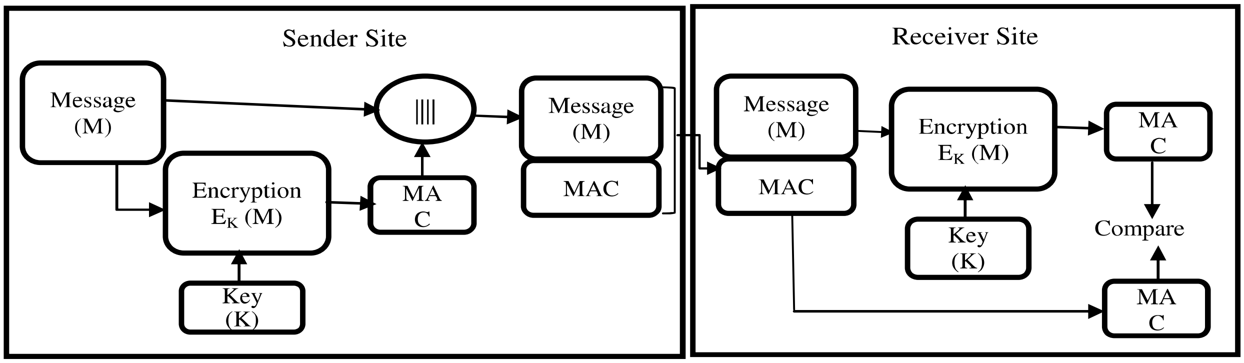


Fig. 1: Secured Message Transaction; Authentication Tied to Plaintext

A message authentication process uses a shared secret key to encrypt the message to produces a small fixed-size message authenticator or message digest or MAC, which is concatenated with the message and send to the intending destination. In the receiving end, the receiver applies the same operation on the received message with the same shared secret key to produces a new message digest or MAC. If we suppose that the shared secret key is only known to the sender and the receiver and the received MAC is found same with the new calculated MAC [10, 11], then:

(a) The receiver assumes that the message has not been altered or modified. If an attacker modifies the message but doesn’t modify the authentication code MAC, then the receiver’s generated MAC′ does not match with the received MAC. Assuming that the attacker does not know the shared secret key, so, the hacker can’t modify the MAC to correspond the MAC′ message.

(b) The receiver is confirmed that the message came from the intended sender. Since only the sender and receiver know the secret key, no one else can generate the MAC that was sent by sender without genuine message and secret key.

(c) If the message contains a sequence number, then the receiver can be confirmed of the actual sequence because a hacker can’t properly modify the sequence number.

To realize the process of message authentication, confidentiality, and integrity; conventional approaches are studied and reviewed [12]. In this paper, a better system for secured message transaction has been designed, developed and implemented in Python programming language to improve security services of the message transaction system. A comparative study between conventional system and proposed system has been performed.

II. Conventional Message Transaction System

For message authentication, two conventional systems have been reviewed. First method ensures the message authentication among the communicating parties. The message authentication diagram using message encryption with the shared secret key is shown in Fig. 1.

In this system, MAC is generated by encrypting the message with the shared secret key K. Then the MAC is concatenated with the message and sends to the intending destination [13]. In the receiver side, the receiver again encrypts the message with the same shared secret key K to generate another new MAC which is called MAC′ and compare it with the received MAC. If the MAC and MAC′ are found same, then the receiver confirms that the received message came from the stated sender and has not been altered or modified. This process provides message authentication in a secure fashion and allows confidentiality and non-repudiation security services. To ensure these security services, an additional security mechanism is required.

The second method ensures the ciphertext authentication and confidentiality as well as message authentication and confidentiality. This system uses two shared secret keys for message authentication and confidentiality is shown in Fig. 2.

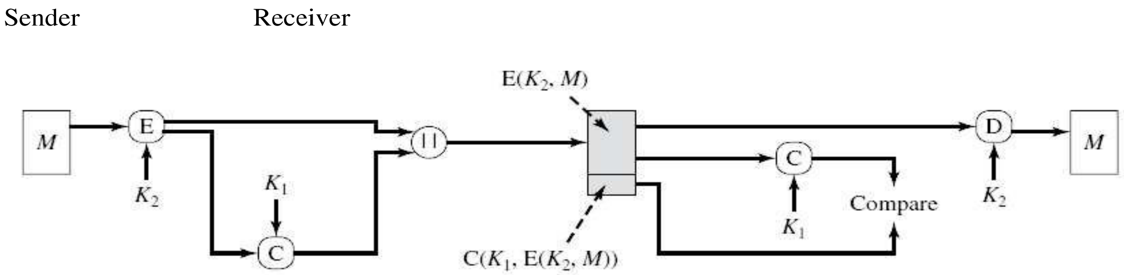


Fig. 2: Message Authentication and Confidentiality; Authentication Tied to Ciphertext.

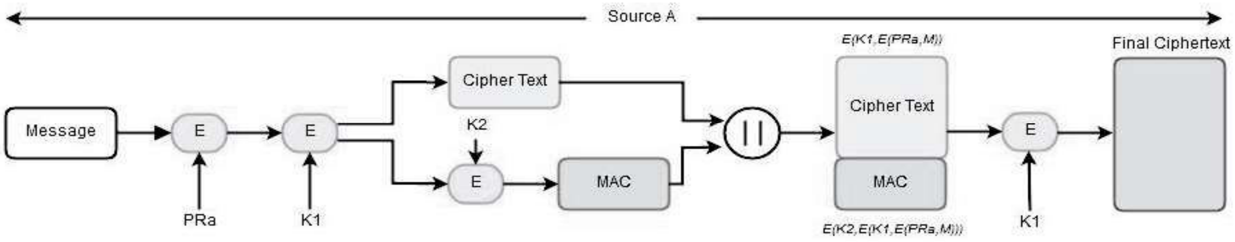


Fig. 3: Encryption Process of the Proposed System

The intelligible message is encrypted with shared secret key K_2, the output is called ciphertext, which is again encrypted with another shared secret key K_1, which produces MAC that is concatenated with the ciphertext and sent to the intended destination. In the receiving end, the receiver calculates the new MAC′ by encrypting the received ciphertext with the shared secret key K_1. Then the calculated MAC′ is compared with the received MAC.

If the MACs are found same, the receiver accepts it and decrypts the received ciphertext with shared secret key K_2 to get intelligible message; otherwise deny it. Hence the receiver is confirmed that the message is not altered and came from the stated source. In this case, the shared secret key K_2 is used for encryption and decryption to provide confidentiality of the message and the MAC. This provides a layer two security for the secure message transaction. Another part of the system establishes the message authentication for secured message transaction. In our paper, a better system of message authentication, confidentiality and integrity has been establishes by using two shared secret keys.

III. Proposed System for Message Transactions

A. *Methodology*

First, message is encrypted with the private key of sender PR_a and the output is again encrypted with a shared secret key K_1 that generates the ciphertext, which is again encrypted with another shared secret key K_2 that generates the MAC. Then the MAC is concatenated with the ciphertext and again encrypted with the shared secret key K_1 that produces final ciphertext which is to be sent to the intended recipient; Fig. 3.

In the receiving end, to retrieve the message, receiver decrypts the received information with the shared secret key K_1 that gives the ciphertext and MAC of the ciphertext, and then only decrypts the MAC part to generate a new ciphertext′ and compare the new ciphertext′ with the received ciphertext to ensure the ciphertext authentication as well as message authentication. If ciphertexts are found same, then the receiver decrypts the ciphertext with shared secret key K_1 and again decrypts with the sender's public key PU_a and retrieve the message; otherwise discard it, Fig. 4.

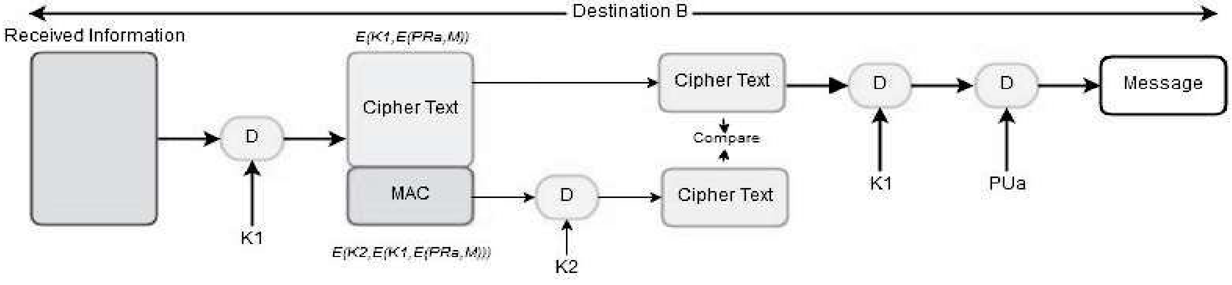


Fig. 4: Decryption Process of the Proposed System

B. Algorithm

Encryption Algorithm: The encryption algorithm of the proposed system consists of the following steps:

Step 1: Sender encrypts the message with his PR_a using RSA algorithm which produces an encrypted output.
Step 2: Output is again encrypted with shared K_1 which produce a ciphertext.
Step 3: Ciphertext is again encrypted with another shared K_2 that generates a message authenticator known as MAC.
Step 4: MAC is concatenates with the ciphertext to compose into a single block.
Step 5: Finally, the message containing the MAC concatenated with the ciphertext is encrypted with key K_1 that produces the final ciphertext, which is to be sent to the intended recipient.

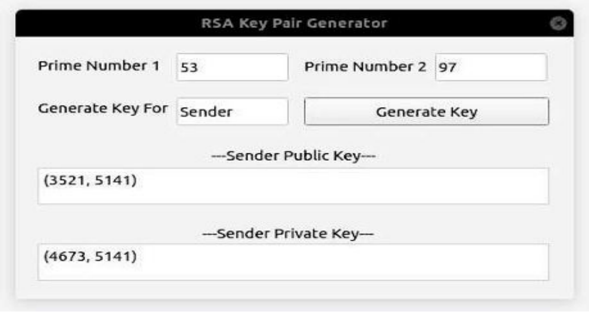
Decryption Algorithm:
The decryption algorithm of the proposed system consists of the following steps:

Step 1: Receiver at first decrypts the received information with the shared secret key K_1 that gives ciphertext and MAC of the ciphertext.
Step 2: Then the MAC is decrypted to produce a new Ciphertext′ to compare it with the received ciphertext that ensures the ciphertext authentication as well as message authentication.
Step 3: If ciphertexts are found same, then it is decrypted to produce encrypted message; otherwise discard it.
Step 4: Finally, the encrypted message is decrypted with the sender's key PU_a that establishes the digital signature.

Here PR_a, PU_a are the sender's private key and public key respectively and PR_b, PU_b are the receiver's private key and public key respectively. The secret keys K1 and K2 are both secret shared keys used by both sender and receiver.

IV. Implementation

The proposed system has been developed using Python programming language Version 3.6. The main aim of our implemented system is to ensure stronger security of the communicating messages. We have also developed a key generator to generate RSA (Rivest-Shamir-Adleman) public-private key pair algorithm. The developed system has run many times for different messages with different 16 bytes shared secret keys and public-private key pairs. The implemented results of the system were found satisfactory.



RSA Key Pair Generator

Prime Number 1: 53
Prime Number 2: 97
Generate Key For: Sender

---Sender Public Key---
(3521, 5141)

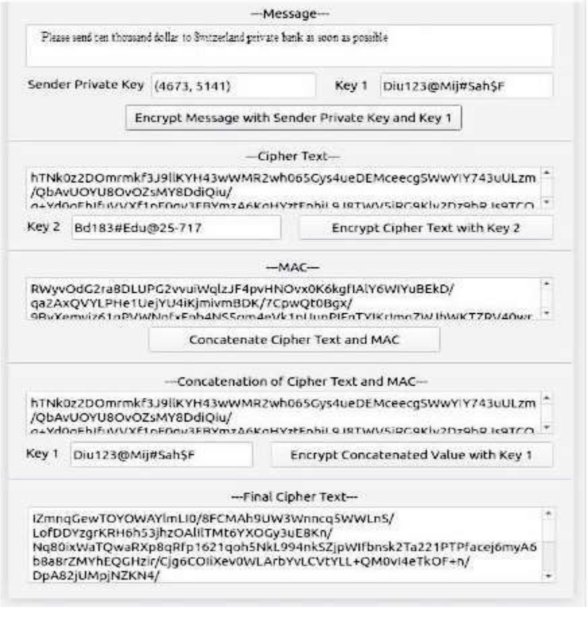
---Sender Private Key---
(4673, 5141)

Fig. 5: RSA Public-Private Key Generation for Sender

V. Experimental Result

The experimental input and output results of the system are given below. In our experiment, the intended message is "Please send ten thousand dollar to Switzerland private bank as soon as possible", which is to be send to the intended destination after performing some encryptions. For this, first the sender generates his public-private key pair using RSA algorithm; Fig. 5.

The sender publish his public key (3521, 5141) and kept secret private key (4673, 5141). Then encrypt the intended message with his private key (4673, 5141) and again encrypts with 16 bytes shared secret key K_1 "ddd123@mmm#Sah$F" that produces ciphertext, shown in Fig. 6.



---Message---
Please send ten thousand dollar to Switzerland private bank as soon as possible

Sender Private Key: (4673, 5141)
Key 1: Diu123@Mij#Sah$F

Encrypt Message with Sender Private Key and Key 1

---Cipher Text---

```
hTNk0z2DOmrmkf3J9lIKYH43wWMR2wh065Gys4ueDEMceecgSWwYIY743uULzm
/QbAvUOYU8OvOZsMY8DdiQiu/
```

Key 2: Bd183#Edu@25-717

Encrypt Cipher Text with Key 2

---MAC---

```
RWyvOdG2ra8DLUPG2vvuiWqlzJF4pvHNOvx0K6kgfIAlY6WIYuBEkD/
qa2AxQVYLPHe1UejYU4iKjmivmBDK/7CpwQt0Bgx/
```

---Concatenation of Cipher Text and MAC---

```
hTNk0z2DOmrmkf3J9lIKYH43wWMR2wh065Gys4ueDEMceecgSWwYIY743uULzm
/QbAvUOYU8OvOZsMY8DdiQiu/
```

Key 1: Diu123@Mij#Sah$F

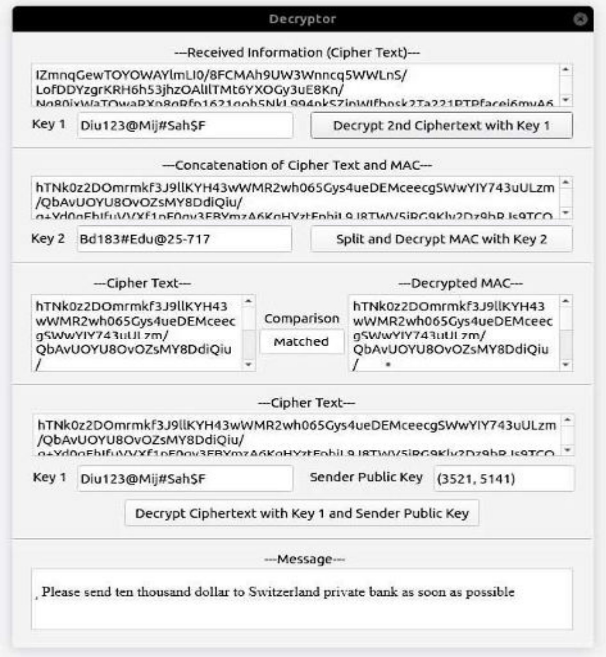
---Final Cipher Text---

```
IZmnqGewTOYOWAYlmLI0/8FCMAh9UW3Wnncq5WWLn5/
LofDDYzgrKRH6h53jhzOAlIlTMt6YXOGy3uE8Kn/
Nq80ixWaTQwaRXp8qRfp1621qoh5NkL994nkSZjpWIfbnsk2Ta221PTPfacej6myA6
b8a8rZMYhEQGHzir/Cjg6COIiXev0WLArbYvLCVtYLL+QM0vl4eTkOF+n/
DpA82jUMpjNZKN4/
```

Fig. 6: Encryption Process in the Sender End

Ciphertext is again encrypted with 16 bytes shared secret key K_2 "Bd183#Edu@25-717" that generates MAC. Then the ciphertext and the MAC are concatenated. The concatenated value is again encrypted with the 16 byte shared secret key K_1 “Diu123@Mij#Sah$F” that produce the final ciphertext, which is send to the destination.

In the receiver end, receiver decrypts the received information with the 16 bytes shared secret key K_1 “Diu123@Mij#Sah$F” that gives concatenated ciphertext and MAC. Then only MAC with 16 bytes shared secret key K_2 “Bd183#Edu@25-717” is decrypted, which generates the new ciphertext′ and compared with the received ciphertext; if the ciphertext and decrypted MAC are found same, then the ciphertext with the 16 bytes shared secret key K_1 “Diu123@Mij#Sah$F” is decrypted and again decrypted with the sender’s public key (3521, 5141) that produces the original message “Please send ten thousand dollar to Switzerland private bank as soon as possible”; the whole decryption process is shown in Fig. 7.


Decryptor
Decrypt 2nd Ciphertext with Key 1
Split and Decrypt MAC with Key 2
Comparison
Decrypt Ciphertext with Key 1 and Sender Public Key

---Received Information (Cipher Text)---

```
lZmnqGewTOYOWAYlmLI0/8FCMAh9UW3Wnncq5WWLnS/
LofDDYzgrKRH6h53jhzOAlIlTMt6YXOGy3uE8Kn/
Nq80ixWaTOwaRXo8qRfp1621qoh5Nkl994nkSZjpWIfbnsk2Ta221PTPfacei6myA6
```

Key 1 Diu123@Mij#Sah$F

---Concatenation of Cipher Text and MAC---

```
hTNk0z2DOmrmkf3J9llKYH43wWMR2wh065Gys4ueDEMceecgSWwYIY743uULzm
/QbAvUOYU8OvOZsMY8DdiQiu/
q+Yd0qFbIfuVVXf1pF0qv3EBYmzA6KqHYztFnbiL9J8TWV5iRG9Klv2Dz9hRJs9TCO
```

Key 2 Bd183#Edu@25-717

---Cipher Text---

```
hTNk0z2DOmrmkf3J9llKYH43
wWMR2wh065Gys4ueDEMceec
gSWwYIY743uULzm/
QbAvUOYU8OvOZsMY8DdiQiu
/
```

Matched

---Decrypted MAC---

```
hTNk0z2DOmrmkf3J9llKYH43
wWMR2wh065Gys4ueDEMceec
gSWwYIY743uULzm/
QbAvUOYU8OvOZsMY8DdiQiu
/
```

---Cipher Text---

```
hTNk0z2DOmrmkf3J9llKYH43wWMR2wh065Gys4ueDEMceecgSWwYIY743uULzm
/QbAvUOYU8OvOZsMY8DdiQiu/
q+Yd0qFbIfuVVXf1pF0qv3EBYmzA6KqHYztFnbiL9J8TWV5iRG9Klv2Dz9hRJs9TCO
```

Key 1 Diu123@Mij#Sah$F

Sender Public Key (3521, 5141)

---Message---

, Please send ten thousand dollar to Switzerland private bank as soon as possible

Fig. 7: Decryption Process in the Receiving End

VI. Security Analysis

Fundamental security services integrity, confidentiality, authentication and non-repudiation are the essential ingredients for any secured electronic information transfer system. A comparative study between the proposed system and the two conventional systems for secured electronic message transaction has been performed and presented, where our proposed system performs all the fundamental security services; as shown in Table 1.

Table 1: Comparative Security Services between two Conventional Systems and the Proposed System

Approaches	Confidentiality	Integrity	Authentication	Non-repudiation
System 1	Yes	No	No	No
System 2	Yes	Yes	Yes	No
Proposed System	Yes	Yes	Yes	Yes

VII. Conclusion

A better approach for secured electronic message transaction system has been designed, developed and implemented using Python programming language. It performs all the fundamental security services, which are confidentiality, integrity, authentication and non-repudiation for both communicating message and communicating participants. For this, simple cryptographic encryption and decryption techniques are used to the communicating messages. This approach can be very helpful for further research related to cryptographic applications. It performs secured electronic message transactions. The people who are interested to study on information security can be also benefited from this research. This technique can be applied anywhere of secured electronic communications. Several other additional security services are imposed as future study of the research .

References

[1] Kaufman, Charlie, Radia J. Perlman and Mike Speciner. “Network security - private communication in a public world.” Prentice Hall series in computer networking and distributed systems (1995).

[2] W. Stallings, Cryptography and Network Security Principles and Practice, 5th ed., Prentice Hall Press, Upper Saddle River, NJ, USA, 2010.

[3] Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw-Hill Education Private Limited, 2011.

[4] Bruce Schneier, “Applied Cryptography”, 2nd Edition, 2003, ISBN: 9971-51-348-X.

[5] C. Biswas, U. D. Gupta and M. M. Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography," 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox'sBazar, Bangladesh, 2019, pp. 1-5.

[6] D. P. Timothy and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, 2017, pp. 1-5.

[7] M. Ismail Jabiullah, Abdullah Al-Shamim and M. Lutfar Rahman, "Improved Message Authentication and Confidentiality Checking", Journal of Science and Applications, Bangladesh Atomic Energy Commission, Dhaka, Bangladesh, Vol. 14, No.1, June 2005, ISSN: 1016-197X, pp: 1-5.

[8] M. Ismail Jabiullah and M. Lutfar Rahman, "Review on Session-keys and Their Importance for Secured Electronic Transactions", International Journal of Soft Computing, Medwell Online, Pakistan, http://www.medwellonline.net, Volume 1, Issue Number 3, June-July, 2006 ISSN: 1816-9503, pp: 220-224.

[9] M. Ismail Jabiullah, Kamrul Ahsan, Jahangir Alam, ANM Khaleqdad Khan and M. Lutfar Rahman, “Elliptic Curve

Cryptographic Technique Implementation of Textmessage (SMS) Transaction in Mobile Phone", In the Proceedings of the Annual Conference, Central Auditorium, Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, Page: 70, May 04-05, 2007.

[10] M. Ismail Jabiullah, ANM Khaleqdad Khan and M. Lutfar Rahman, "An Improved Session-key Distribution Technique for the Key Distribution Center (KDC)", In the Proceedings of the Annual Conference, Central Auditorium, Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, Page: 73, May 04-05, 2007.

[11] Sydul Islam Khan, Md. Ismail Jabiullah and M. Lutfar Rahman, "An Approach for Strong Message Authentication and Confidentiality Checking", The 22nd Bangladesh Science Conference organized by Bangladesh Association for Advancement of Science (BAAS) and Bangladesh Council of Scientific and Industrial Research (BCSIR), Dhaka, Bangladesh on 27-29 September, 2012

[12] Md. Monowar Hossain, Anisur Rahman, Sydul Islam Khan and M. Ismail Jabiullah, "Improved CBC-Based Cryptographic Process for Message Transactions", National Conference on Communication and Information Security (NCCIS 2012), held at 31 March 2012, at the Auditorium, Daffodil International University, Dhaka-1000, Bangladesh, Pages: 59-63.

[13] Mago, Neeru. "PMAC: A Fully Parallelizable MAC Algorithm." (2016).

Md. Ismail Jabiullah is a Professor in the Department of Computer Science and Engineering Department at the Daffodil International University, Dhaka, Bangladesh. He received his PhD degree in Computer Science and Engineering from the University of Dhaka, Bangladesh. His PhD topic was in Cryptography and Network Security. He has published 68 research articles in reputed journals and more than 98 research papers in the International and National Conferences. He authored more than 26 books. His research interests include Network Security, Information Security, Cryptography, Cyber Security, Cryptocurrency, Steganography, Wireless Network, Mobile Network, Artificial Intelligence, Machine Language, Deep Learning, Software Security, Satellite Network, Image Processing, Software Testing and Neural Networks. He serves as a reviewer for various reputed journals and conferences annually.

Dr. A. A. Md. Monzur-Ul-Akhir was born in Dhaka. He is currently acting as an Assistant Professor in Electrical and Electronic Engineering Department, Green University of Bangladesh. He is also acting as an Associate Editor of the Green University of Bangladesh Journal of Science and Engineering (GUBJSE). He is an ex-Notredamian. He completed his Bachelors and Masters in EEEfrom the University of Dhaka. He also completed his MBA in Finance from the Institute of Business Administration (IBA) from the University of Dhaka in 2012. He got the prestigious merit scholarship from the Japanese Government-Monbukagakusho (Monbusho/MEXT) in 2014 to pursue his PhD in Nano and Functional Material Sciences from the University of Toyama. After his Ph.D. degree in 2018 he was then awarded with the "Marubun Research Promotion Foundation Grant 2017 " to complete his Postdoctoral research from 2018-2019 at the University of Toyama. His research interest includes Group III-V Compound Semiconductors, Thin-film growth, Spintronics, Solar cell, Solar Materials, Nanotechnology, Cryptography, Robotics, Electronic devices, Business studies, etc.
He has worked for different Private Universities in Bangladesh from 2009-2019. He has achieved the professional certificate of Diplomaed Associate of The Institute of Bankers, Bangladesh (DAIBB). He attended the international conference ICIEV 2019, Washington, Spokane, USA, and his submitted paper won the best paper award. He has several journal and conference publications.He is currently appointed as the Moderator of "Green Theater" -the theater club of the Green University of Bangladesh.

Muhammad Rashiduzzaman received his BSc degree from the Department of Computer Science and Engineering at Daffodil International University, Bangladesh. His research interests include Information Security, Blockchain Technology, Cryptography, Cyber security.