E-ISSN: 2664-8784
P-ISSN: 2664-8776
IJRE 2023; 3(1): 13-17

www.engineeringpaper.net
Received: 04-02-2023
Accepted: 07-03-2023

Noshin Un Noor
Department of Information and Communication Technology, Bangladesh University of Professionals, Dhaka, Bangladesh

Farjana Tumpa
Department of Information and Communication Technology, Bangladesh University of Professionals, Dhaka, Bangladesh

Md. Murshedul Arifeen
Department of Information and Communication Technology, Bangladesh University of Professionals, Dhaka, Bangladesh

Sm Rakibul Hasan
Department of Electrical and Electronic Engineering, AUST, Dhaka, Bangladesh

Dilshad Ara Hossain
Department of Information and Communication Technology, International Islamic University Malaysia Kuala lumpur, Malaysia

SM Salim Reza
Department of Information & Communication Technology, Bangladesh University of Professionals, Dhaka, Bangladesh

Correspondence Author;
Noshin Un Noor
Department of Information and Communication Technology, Bangladesh University of Professionals, Dhaka, Bangladesh

AES based security scheme to remove man-in-the middle attack in online banking

Noshin Un Noor, Farjana Tumpa, Md. Murshedul Arifeen, Sm Rakibul Hasan, Dilshad Ara Hossain and SM Salim Reza

DOI: https://dx.doi.org/10.33545/26648776.2023.v5.i1a.46

Abstract
For illuminating the man middle attack during authentication process of public key certification process, we have proposed an encryption scheme based on Advance Encryption Standard. This method is an efficient and secure form of encryption which keep users valuable information safe. Public- key cryptography which is based on the concept of a key compare, comprises of an accessible key and a exclusive key. Information that has been scrambled with an open key can be decoded as it were with the comparing private key.
Index Terms: AES, authentication, Public key certificate, Certification Authority, security, Man in the middle attack, online bank in.

Keywords: Compare, comprises, accessible

1. Introduction
Online banking is a procedure in which transactions are propulsion electronically over the internet. Online banking is an electronic transaction system using financial institutions website with a view to conduct customers transaction. It is constituted of a secure connection to provide banking information through the depositors home computer or another de- vice. Banks play a significant role in economic growth. People can store money in physical cash but there are many reasons for using a bank account. The main purpose of bank account is security. But online banking is not utterly secured. Online banking customers use persuasive information for transaction. The information of users can be forged by the attackers or hackers.
Identity theft via stolen login credentials is a major concern of online banking. Hackers can easily target online ac- counts. Online accounts can seem to hacker's easy targets, instead of robbing a bank, a criminal could simply whisk away money with a few keystrokes. Man in the middle or the scammer targets the substantive data that convey between end terminals. The goal of this attack is to steal personal information, account credentials, and credit card numbers etc. Targets are usually users of fiscal applications and other web- sites where providing personal information is necessary. The attacker uses the information for many concoctions including identity theft, unconstitutional depot transfers etc. Man-in-the middle attack is a type of eavesdropping attack which is used by the hacker to hinder with a communication session between the system and the user. Attacker use real time processing of the victim's consultations, transactions.
To eliminate this problem, we have proposed an encryption scheme based on public key certification. The certificate consists of information about the key, information about uni- formity of user and, the digital signature of a subsistence that has verified the certificates contents. If the conclusive signature identified by the software after interrogation, then the key will be used to acquaint securely with the certificates subject. The document of public key certificate constructed with furcated block of data that accommodate certificate holders credential and holders communal key as well as the digital signature of certification authority to ensure validation. Nowadays online banking is very popular because it allows users easy access to banking services. To access online banking users, use banking websites or mobile phones. Because of an online system, users can face various threats throw internet and users can be attacked via Web via mobile phone in various ways. There are several attacks in an online banking system. In Symmetric key encryption scheme same cryptographic key is used with fundamental algorithm by both sender and receiver. Without secure channel the key will be forged or changed.

In this paper we introduced an advanced approach of public key certificate authentication using AES algorithm. Two party authentication processes can be harmed by man-in-the-middle attack; our proposed method solved the concern. Simulation has been conducted in MATLAB.

2. Problems Statement

A man in the middle attack is usually attended in a client server environment. Client is a computer hardware or software that accesses the service made available by a server in the network. A server is another computer system whose services are accessed by the client through a gateway. A man in the middle attack is when a hacker gets in between two endpoints a client and a server. In such a situation, the person within the middle sent client email, pretending to be legitimate. This at- tack additionally involves phishing, obtaining users to click on the e-mail showing to return from bank. Attackers additionally created an internet site that appears a bit like users banks web- site; therefore, users would not hesitate to enter login credentials when clicking the link within the email. Surrendering user's credentials to the assaulter the man-in-the-middle attacks are available in two forms, one that involves physical proximity to the target, and another that involves malicious software system, or malware.

Table 1: Types of Attack

Name of Attack	Description
Replay Attack	When a cyber-criminal overhears on an impenetrable network communication
Phishing Attack	Phishing is the assiduity to obtain impressible Information.
Dictionary Attack	In distinction with a brute force attack, wherever an outsized pro- portion Key area is searched consistently.
Dos Attack	By inexorable and aimed machine with requests until normal traffic is incompetent to be processed is called Dos Attack.

3. Related Works

The Members of this paper introduced smart card-based password authentication scheme without a sensitive verification table which is stored on the server [14]. They proposed an effective and secure one-time password authentication scheme for wireless sensor networks [12]. Authors of this paper introduced a new scheme to increase reliability using format verification tool Proverif [15]. They broadly audit the writing on MITM to examine and categorize the scope of MITM assaults, considering both a reference show, such as the Open Frameworks Interconnection (OSI). Demonstrate [4]. Author inspected a range of technical, infrastructural, operational and management issues combined with the manipulation of PKI in this paper [10]. They introduced a new scheme to improve Inability of providing mutual authentication leads to gateway node bypassing attack and privileged insider attack. Wireless Sensor node has inadequate computing power, less storage and a module of communication where the resource constrained environment for remote user is principle concern [11]. The authors proposed a secure and convenient user- friendly two factor authentication scheme and discuss home banking system, to get the service the user device's Bluetooth must be enabled to provide user id and password to access to the system. It is a simple and efficient two-party authentication protocol-based system [5]. They proposed three protocols such As-Registration of the user with username and password, smart application activation scheme where the system and the user install the system on their remote premises and lastly new service registration is provided. The patient's information is saved in digital format in the system. Workstations of the system which are user devices connected to the local system with any type of physical network [13]. The authors of this particular paper approached Scheme is more efficient and secure where numerous attacks can be protected through successful user authentication by three message exchanges. The two-factor user authentication protocol in wireless sensor network is attack prone where the sensor of the network has limited storage consistency and energy limitations [9]. To increase security in mobile banking applications an appropri- ate foundation is needed. The authors proposed framework ensures personal identification integrity and message integrity [8]. They proposed solution to these problems where user produces multiple OTPs from initial seed in user 's device in parallel process. The three main part of the scheme is- Registration phase, Login Authentication Phase, Numerical Illustration. The proposed scheme provides cost efficiency and security [7]. The authors proposed to observe the understanding factors that influences mobile banking adoption from future prospects which results in developing a risk benefit model by extending TAM [1]. They displayed a number of assaults, a few unused, on open key conventions. They moreover progress a number of standards which may offer assistance creators avoid many of the pitfalls, and offer assistance assailants spot blunders which can be misused.- [2]. The authors proposed and explored the notion of key-insulated security whose objective is to play down the damage caused by secret-key exposures [6]. They expanded on a modern formal show of CLPKE and build a CLPKE conspire that does not depend on the bilinear pairings [3]. They presented the idea of certificate- based encryption.

4. Proposed Method

A. Public Key Certification

Public key certificate provides a secure and efficient way for associate degree entity to adrift its public key to be utilized in uneven cryptography. The public key certificate avoids the subsequent situation: if the other person creates public key and personal key, she will claim that she's Alice and send her public key to Bob. Bob is going to be able to communicate with hacker. The Certificate Authority is an entity which issues and revokes certificates. A certificate authority (CA) is an association that stores open keys and their proprietors, and each gathering in a correspondence confides in this association.

B. Advanced Encryption Standard

Advanced Encryption Standard (AES) is an efficient and protected form of encryption which keeps users valuable information safe. Advanced Encryption Technique works better to encrypt easily and within a certain range of time and around capacities, counting its execution on both equipment and program, ease of execution and its level of security is undeniable. AES information encryption could be a more numerically proficient and exquisite cryptographic

algorithm, but its primary quality rests within the alternative for different key lengths. AES permits you to select a 128-bit, 192-bit or 256-bit key, making it exponentially more grounded.

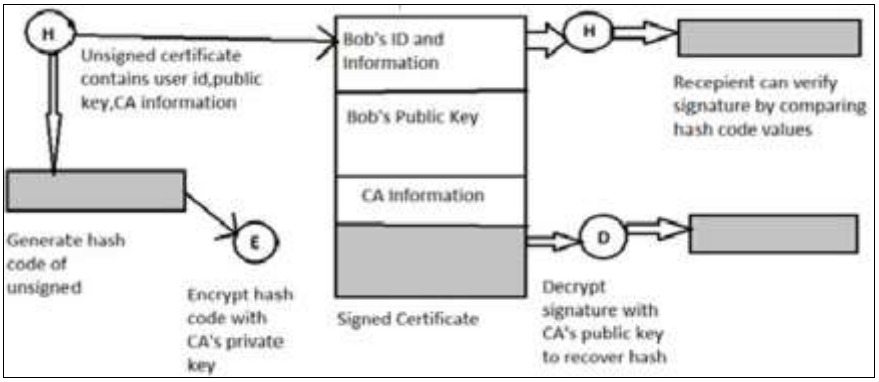

Fig 1: Public Key Certification

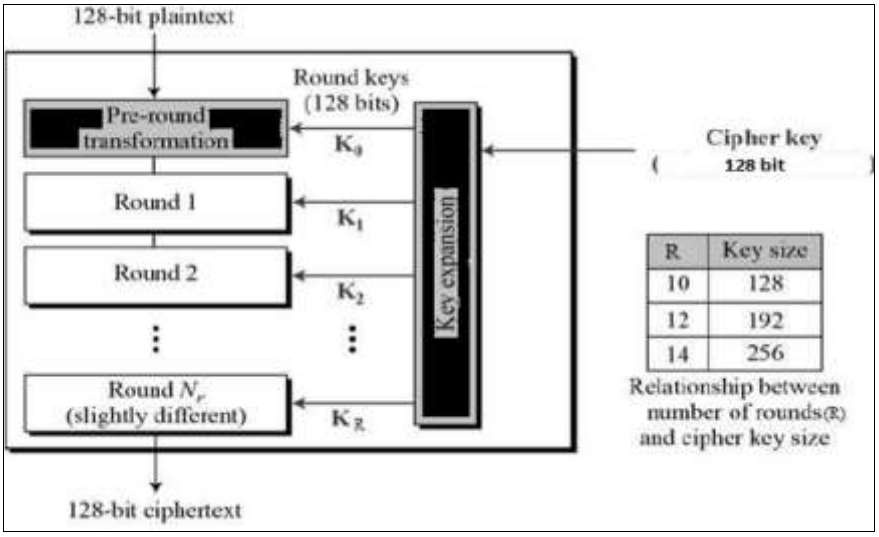

Fig 2: AES encryption process

5. Simulation

We have implemented our proposed scheme in MATLAB. We considered a signal as input the AES algorithm and encrypted it. Then using AES decryption algorithm, we have decrypted the signal and recovered the original signal.

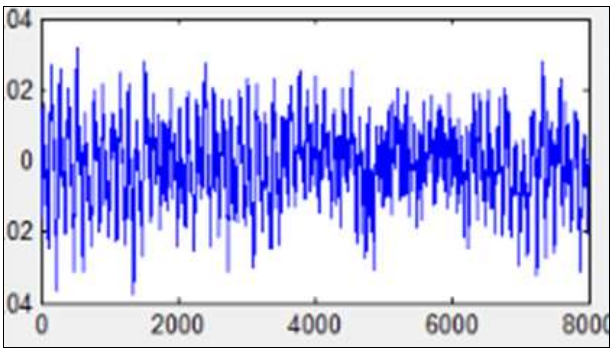

Fig 3: Original Signal

Algorithm 1 AES encryption

1. Cipher (byte inp [4 Nby], byte outp [4 Nby], word wd [Nby (Nrd+1)])
2. Begin byte condition [4, Nby]
3. Condition = inp
4. Add Round Key (condition, w[0, Nby-1])
5. For roundtrip = 1 step 1to Nrd-1
6. Sub Bytes (condition)
7. Shift Rows (condition)
8. Mix Columns (condition)
9. Add Round Key (Condition, wd [Round trip Nby, (roundtrip+1) Nby-1])
10. End for
11. Sub Bytes (condition)
12. Shift Rows (condition)
13. Add Round Key (condition, w [Nrd Nby, (Nrd+1) Nby-1])
14. Outp = condition
15. End

Algorithm 2 AES key expansion

1. Key Expansion (byte key [4 Nky], word wd [Nby (Nrd+1)], Nky)
2. Begin
3. Word pd
4. p = 0
5. While (p¡Nky) wd[p] = word (key [4 p, key [4 p+1], key [4 p+2], key [4 p+3])
6. p = p+1
7. End
8. While
9. p = Nky
10. While (p ¡ Nby (Nrd+1)] pd = wd[p-1]
11. If (p mod Nky =0) pd = SubWord (pd)) xor Rcon

[p/Nky] else if (Nky ¿ 6 and i mod Nky = 4)
12. pd = SubWord (pd)
13. end if
14. wd [p] = wd [p-Nky] xor pd
15. p = p + 1
16. end while
17. end

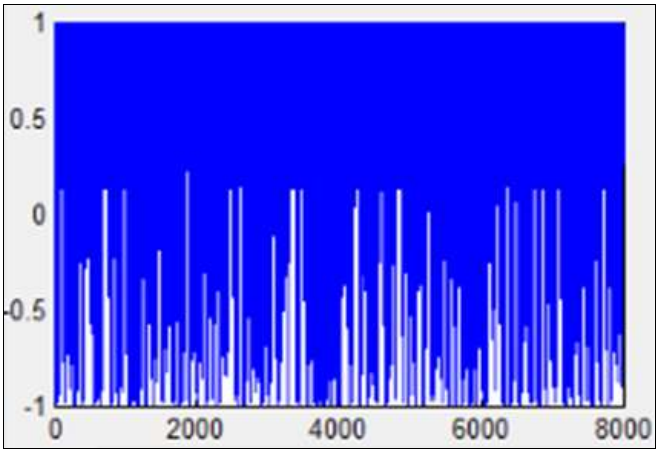

Fig 4: Encrypted Signal

Algorithm 3 AES decryptin

1. InvCipher (byte inp [4 Nby], byte out [4Nby], word wd [Nby (Nrd+1)])
2. Begin byte condition [4, Nby]
3. Condition = inp
4. Add Round Key (condition, wd [Nrd Nby, (Nrd+1) Nby-1])
5. For roundtrip = Nrd-1 step -1 down to 1
6. Inv Shift Rows (condition)
7. Inv Sub Bytes (condition)
8. Add Round Key (condition, wd [roundtrip Nby, (roundtrip +1) Nby-1])
9. Inv Mix Columns (condition)
10. End for
11. Inv Shift Rows (condition)
12. Inv Sub Bytes (condition)
13. Add Round Key (condition, wd [0, Nby-1])
14. Out p = condition
15. End

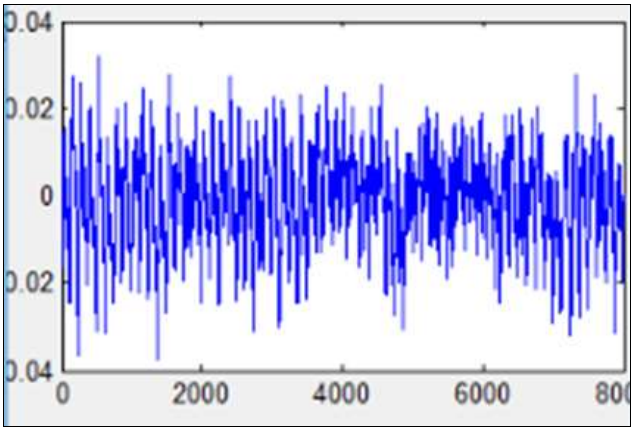

Fig 5: Decrypted Signal

6. Conclusion

Security is never again an idea in retrospect in anybody's product plan and advancement process. AES is a significant standard and utilizing and understanding. It significantly builds the unwavering quality and security of our product frame- works. Utilizing field GF was a generally excellent choice. The backwards of the expansion activity was itself, making a big deal about the calculation simple to do. Truth be told, each activity is convertible by structure. Likewise, the square size and key size can shift making the calculation versatile. By utilizing AES strategy, we can guarantee progressively solid correspondence then previously.

7. References

1. Akturan U, Tezcan N. Mobile banking adoption of the youth market: Perceptions and intentions. Marketing Intelligence & Planning. 2012;30(4):444-459.
2. Ross Anderson and Roger Needham. Robustness principles for public key protocols. In Annual International Cryptology Conference, Springer; c1995. p. 236–247
3. Baek J, Safavi-Naini R, Susilo W. Certificate less public key encryption without pairing. In International Conference on Information Security, pages 134–148. Springer; c2005.
4. Conti M, Dragoni N, Lesyk V. A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials. 2016;18(3):2027-2051.
5. Di Pietro R, Gianluigi ME, Strangio MA. A two- factor mobile authentication scheme for secure financial transactions. In International Conference on Mobile Business (ICMB'05), IEEE; c2005. p. 28–34.
6. Dodis Y, Katz J, Xu S, Yung M. Key- insulated public key cryptosystems. In International Conference on the Theory and Applications of Cryptographic Techniques, Springer; c2002. p. 65–82.
7. Eldefrawy MH, Alghathbar K, Khur-ram Khan M. Otp-based two-factor authentication using mobile phones. In 2011 Eighth International Conference on Information Technology: New Generations, c2011. p. 327–331. IEEE;
8. Hayikader S, Hadi FN, Ibrahim J. Issues and security measures of mobile banking apps. International Journal of Scientific and Research Publications. 2016;6(1):36-41.
9. He D, Yi G, Chan S, Chen C, Bu J. An enhanced two-factor user authentication scheme in wireless sensor networks. Ad hoc & sensor wireless networks. 2010;10(4):361-371.
10. Hunt R. Pki and digital certification infrastructure. In Proceedings. Ninth IEEE International Conference on Networks, ICON; c2001. p. 234–239. IEEE
11. Khan MK, Alghathbar K. Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'. Sensors. 2010;10(3):2450-2459.
12. Chung-Huei L Cheng-Chi L, Yang CC, Min-Shiang H. A secure and efficient one-time password authentication scheme for WSN. IJ Network Security. 2017;19(2):177-181.
13. Siddiqui Z, Abdullah AH, Khan MK, Alghamdi AS. Smart environment as a service: Three factor cloud based user authentication for telecare medical information system. Journal of medical systems. 2014;38(1):9997.
14. Wang D, He D, Wang P, Chao-Hsien C. Anony- mous two-factor authentication in distributed systems:

Certain goals are beyond attainment. IEEE Transactions on Dependable and Secure Computing. 2014;12(4):428-442.
15. Qi X, Dong N, Wong DS, Hu B. Cryptanalysis and security enhancement of a robust two-factor authentication and key agreement protocol. International Journal of Communication Systems. 2016;29(3):478-487.