IMPLEMENTATION OF ELECTRONIC FUND TRANSFER USING NEW SYMMETRIC KEY ALGORITHM BASED ON SIMPLE LOGARITHM

Mohammed Abdullah Mohammed Aysan*

Abstract: Electronic Fund Transfer involves electronic transfer of money by financial institutions. EFT is the groundwork of the cash-less and check-less culture where and paper bills, checks, envelopes, stamps are eliminated. EFT is used for transferring money from one bank account directly to another without any paper money changing hands. The most popular application of EFT is that instead of getting a paycheck and putting it into a bank account, the money is deposited to an account electronically. Cryptography has been used for years to secure electronic funds transfers. However, in the electronic data interchange environment, cryptographic controls are still in their infancy. In this paper, we examine the function and operation flow of the electronic funds transfer process as well as its security control mechanism. To evaluate telecommunication and data security techniques, a standard-leading inter-bank payment system called the Society for Worldwide Inter-bank Financial Telecommunications System is introduced.

Key words: Electronic Fund Transfer, EFT, Symmetric key, Bank, E-cash, Logarithm etc.

*Student, Computer Engineering & Networks Department, College of Computer Sciences and Information System, Jazan University, KSA
INTRODUCTION

Every day billions of dollars are transferred electronically between institutions and individuals in Electronic Funds Transfer (EFT) systems. EFT systems’ transactions cannot be processed securely unless user identities can be validated and the correct transmission of messages between system nodes can be assured [1].

Information security is considered one of the most critical concerns in today’s competitive digital economy. Web technologies provide an amazing infrastructure for electronic data interchange (EDI), direct marketing, and information retrieval [5]. In particular, electronic banking and financial services have immense growth potential via the Internet. Some of the most important security issues involve electronic money and digital cash. As more and more companies jump onto the information superhighway with interactive web sites, information security becomes an important issue in digital economy [2].

Cryptography is the science of protecting the privacy of information during communication under hostile conditions. In the present era of information technology and proliferating computer network communications, cryptography assumes special importance. Cryptography is now routinely used to protect data, which must be communicated and/or saved over long periods, to protect electronic fund transfers and classified communications [3].

Current cryptographic techniques are based on number theoretic or algebraic concepts. Chaos is another paradigm, which seems promising. Chaos is an offshoot from the field of nonlinear dynamics and has been widely studied. A large number of applications in real systems, both man-made and natural, are being investigated using this novel approach of nonlinear dynamics. The chaotic behavior is a subtle behavior of a nonlinear system, which apparently looks random. However, this randomness has no stochastic origin. It is purely resulting from the defining deterministic processes. The important characteristics of chaos are its extreme sensitivity to initial conditions of the system.

LITERATURE REVIEW

C.H.Meyer, S.M.Matyas (1981) discussed the personal verification processes at different institutions in an interchange environment are isolated from one another. It is assumed that only information stored on the bank card and information remembered by a system user are employed for personal verification. It is shown that only through the use of a secret
quantity stored on the bank card will the set of required criteria be satisfied. With a personal key, the same degree of isolation can be achieved for authentication of transaction request messages sent from the entry point to the issues [1].

Dan Zhu (2002) analyzed about modern financial institutions have cashed in on the electronic business opportunities of the Internet by developing numerous payment systems to meet various payment service requirements. In this paper, we examine the function and operation flow of the electronic funds transfer process as well as its security control mechanism. To evaluate telecommunication and data security techniques, a standard-leading inter-bank payment system called the Society for Worldwide Inter-bank Financial Telecommunications System is introduced. Some important security features are investigated in detail [2].

Mintu Philip, Asha Das (2011) Chaotic Encryption Method seems to be much better than traditional encryption methods used today. Chaotic encryption is the new direction of cryptography. It makes use of chaotic system properties such as sensitive to initial condition and loss of information. Many chaos-based encryption methods have been presented and discussed in the last two decades. In order to reach higher performance, these methods take advantage of the more and more complex behavior of chaotic signals[4].

Mohammed Abudallah Md Aysan, Fareed Hassan Almalki, Abdullah Mohammed Almalki (2014) This paper proposes a symmetric key cryptosystem based on the simple mathematical logarithm function. The proposed system benefits from the algebraic properties of log such as non-commutative, high computational speed and high flexibility in selecting keys which make the Discrete Logarithm Problem. Also the encrypted text converted into binary numbers to make harder to understand by the backer. This method will be suitable in any business house, government sectors, communication network, defense network system, sensor networks etc [6].

PROPOSED ARCHITECTURE

Electronic Fund Transfer essential for the Middle East country, in particularly Saudi. More than 7.5 million expatriate working in Saudi Arabia. Our proposed model enables transactions between customers with the help of banks or other third parties centre. ThisElectronic Fund Transfer system is secure and convenient alternative to bills and bank transaction. Electronic Fund Transfer is transferred immediately from one place to another
within fraction of second the recipient can collect the money immediately. Therefore, Electronic Fund Transfer transactions usually require no remote authorization or personal identification number (PIN) codes at the point of sale.

How a typical e-cash system works: A Banker or vendor signs up with one of the participating banks or financial institutions. The vendor receives specific software to install on his or her computer. Then the transaction procedure described in Figure 1 model transaction between two parties Mr. A and Mr. B. The first person wants to transfer the money to other person, though he approaches X-Bank or local vendor, the vendor or Banker processing Mr. A request and providing secret or symmetric key. Also X-Bank transfer Cipher text through web application to Y-Bank. At the same time Mr. A sending secret key to Mr. B through secured channel. Then Mr. B approach to the Y-Bank to pay the money, Y-Bank verifies the message with secret key and transfer money to Mr. B.

**IMPLEMENTATION**

Electronic funds transfer is one of the oldest electronic payment systems. EFT is the groundwork of the cash-less and check-less culture where and paper bills, checks, envelopes, stamps are eliminated. EFT is used for transferring money from one bank account directly to another without any paper money changing hands. EFT is considered to be a safe, reliable, and convenient way to conduct business and transfer the money. The implementation program allows the vendor or banker to install “electronic fund transfer” to his or her desktop. The software manages the secret key. The vendor software generates a cash transaction with our new proposed algorithm and secret key provided to the sender. The sender transfers the secret key to the recipient for appeal the cash in his
destination place. Recipient banker verifies the secret message with key and delivers the cash to the recipient.

**Sender Bank Process**
Here, we have taken some example of transferring money 5432 Saudi Riyal. As per the integer value 5 is 32, 4 is 31 and so on (A-Z=1 to 26, 0-9 is 27 to 36). Then we choose random Logarithm as a secret key and converting value to binary digits is cipher text message transfer to the recipient and secret key given to the sender. The entire sender bank process mentioned in the following table.

<table>
<thead>
<tr>
<th>Saudi Riyal</th>
<th>Integer Value</th>
<th>( \log_3 (X) )</th>
<th>Cipher text (binary value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>32</td>
<td>3.154649</td>
<td>11.00100111100101110001001110101101</td>
</tr>
<tr>
<td>4</td>
<td>31</td>
<td>3.12575</td>
<td>11.00100000001100010011011011101001</td>
</tr>
<tr>
<td>3</td>
<td>30</td>
<td>3.095903</td>
<td>11.00011000100110011001101011000</td>
</tr>
<tr>
<td>2</td>
<td>29</td>
<td>3.065045</td>
<td>11.000100001010011011011001011000</td>
</tr>
</tbody>
</table>

**Recipient Bank Process**
When the recipient claims his money with the secret key, we verify the binary digits and convert into integer value with secret key. The process of recipient claim mentioned in the table no. 2.

<table>
<thead>
<tr>
<th>Cipher text (binary value)</th>
<th>( Y=(X)^3 )</th>
<th>Integer value</th>
<th>Saudi Riyal</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.00100011100101110001001110101101</td>
<td>3.154649</td>
<td>32</td>
<td>5</td>
</tr>
<tr>
<td>11.00100000001100010011011101100101</td>
<td>3.12575</td>
<td>31</td>
<td>4</td>
</tr>
<tr>
<td>11.00011000100110001100110101011000</td>
<td>3.095903</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td>11.00010000101001101100101000000011</td>
<td>3.065045</td>
<td>29</td>
<td>2</td>
</tr>
</tbody>
</table>

**CONCLUSION**
Our New algorithm using symmetric key based on the simple logarithm function. The logarithm and mathematical power function has good relationship of inverse each
other. This Electronic Fund Transfer system easy to access, send for the short communication very quickly. Another advantage for the proposed structure is converting binary digits. This will make confusion and diffusion to the invader. Another innovative idea for our new algorithm, we are extending characters up to 37 letters. A-Z consider as 1 to 26 and 0-9 as 27 to 36. Most of the algorithm working based on the 26 alphabets, especially hill cipher or linear block cipher working based on the 26 alphabets only. In this chapter we are extending the text value up to 36. There is few highlight point about our experimental setup, we are converting logarithm value as a binary digits send to the recipient destination. Our proposed methods capture the new idea of general usage in commercial sector and all small scale shop.

ACKNOWLEDGEMENT

We are very grateful to Department of Computer Engineering and Networks, Jazan University to give us opportunity to work on Cryptography. Next, We would like to express my special gratitude to honorable Dean Dr. Mohammad Y Aalsalem as well as my supervisor Prakash Kuppuswamy and who gave me the opportunity to do this wonderful research article on the topic of my favorite subject Cryptography techniques, which also helped me in doing a lot of Research and I came to know about so many new things.

REFERENCES


