Volume 4, Issue 6
December 2015

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

CRYPTOGRAPHY BASED TRUST MODELS FOR ELECTRONIC DATA INTERCHANGE (EDI)

Md. Safaet Hossain
Department of Computer Science and Engineering
City University, Dhaka Bangladesh
E-mail: safayeth@gmail.com

ABSTRACT

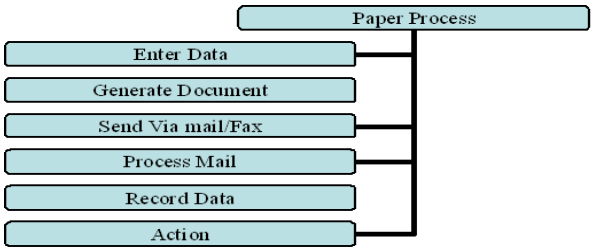
Electronic Data Interchange (EDI) is the electronic exchange of business documents in a standard, computer process able, and universally accepted format between-trading partners. EDI is quite different from sending electronic mail, messages or sharing files through a network. In EDI, the computer application of both the sender and the receiver, referred to as Trading Partners (TPs) have to agree upon the format of the business document which is sent as a data file over electronic messaging services. Everyone who works in a business organization where hundreds and thousands of standard forms, (e.g. invoices) and received and responded to, knows how difficult it is to manage this task. These forms should be entered in the computer for processing, and response, should be generated and posted to the concerned parties. During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. The focus of this paper is identifying essential aspect for secure communications of cryptography.

Keywords: ***EDI, Cryptography, PGP, B2B, EDIS, VAN***

1. INTRODUCTION

Electronic Data Interchange (EDI) is the computer-to-computer electronic exchange of business documents using standard format. It is one of the components in conducting electronic commerce (e commerce). Basically EDI is an acronym used to denote the utilization of computers and communications technology to expedite business processes. Computers are inherent devices for business and personal use. It is used to keep track of business information, ordering and correspondence.

In business communications (B2B), EDI is used in the exchange of business transactions in a computer accessible format covering applications such as inquiries, planning, purchasing, acknowledgement, pricing, order status, scheduling, test results, shipping and receiving, invoices, payments and financial status. Additional standards of EDI covers interchange of data relating to security, administrative data, trading partner information, specifications, contracts, production data, distribution and sales activities. In short all sorts of relevant information necessary for the conduct of business.



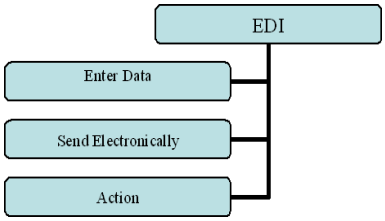


Figure 1: Comparison between paper process & EDI Source: The Why EDI Guide

The above table illustrates the increased efficiency by using EDI as opposed to paper based processes. Off hand, it could be seen that information are acted on faster, less chances of error as data need not be typed repeatedly and of course savings on paper and man-hours.

2. HOW EDI WORKS

The basis of EDI is the computer to computer exchange of business information in a structured format between business trading partners or between various units within an organization. The application of EDI involves the conversion of written documents into a structured, machine readable format so that a computer at the other end can receive, process the data and finally have the request acted upon.

The following Figure2 shows and expresses the basic requirements of EDI process source in international trade with message structure standards and with the implementation rules and protocols. Figure 3 expresses the sender and receiver work process and work flow where there are dependencies in their work.

Volume 4, Issue 6
December 2015

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

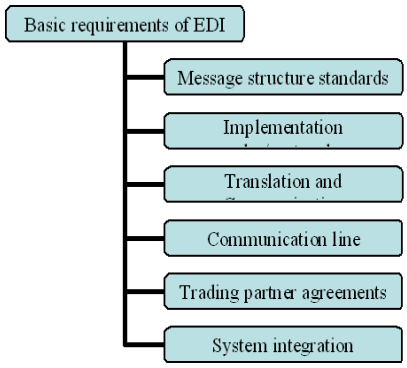


Figure 2: Basic EDI process Source: EDI in International Trade

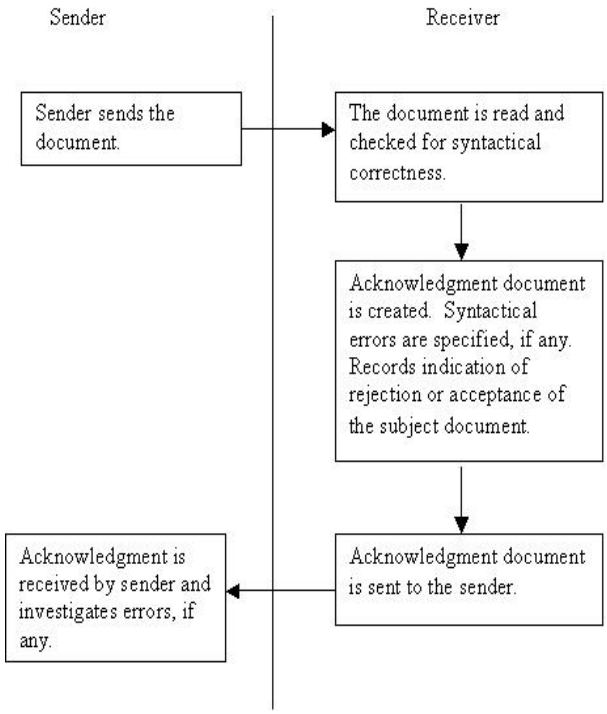


Figure 3: Acknowledgement by Sender and Receiver

3. LITERATURE REVIEW

C.H.Meyer, S.M.Mat.yas (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 sys–tern 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 [11]. 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 [12]. 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 [13]. Mohammed AbudallahMdAysan, 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 logx 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 [14].

4. EDI ACKNOWLEDGMENT

An acknowledgment is a document created and sent to the sender in response to the sender's document. It is to inform the sender of the documents receipt and validity. The acknowledgment also notifies the sender of what action has been taken -- whether the document has been rejected or if it has been accepted. When multiple documents are sent by the sender, an acknowledgment for each document can be created.

5. OVERVIEW OF EDI AND EFT SYSTEMS

EDI is a rapidly emerging technology that allows automated commercial transactions to be conducted within organizations and among enterprises. Using Electronic Document Interchange, a business document can be created as an electronic file in the sender's system, sent via any of several possible transmission modes, and processed directly by the recipient's computer. Little or no human intervention is required. EDI documents include, but are certainly not limited to, purchase orders, invoices, letters of credit, tariff filings, tax returns, bills of lading, insurance claims, financial reports, and requests for quotations. Organizations transacting business are known as trading partners.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Certain industries have well-developed EDI systems in place. They include retailing, apparel, textile and transportation industries. The health care industry is just beginning to implement EDI widely. Nearly every serious proposal for health care reform includes EDI as an integral component.
The standardization of EDI is continuing as many existing industry standards are being incorporated in national and international standards. Among the potential benefits of this technology are considerable cost savings, information accuracy, and improved timeliness.

EFT, a subset of EDI, is well-developed and tested. The use of Electronic Funds Transfer by the federal government is substantial. The social security checks of more than 22 million Social Security recipients are deposited electronically. Nearly half of federal salaries are now paid by electronic funds transfer (EFT). Most banks and savings and loans now offer electronic payment of mortgages, loans, and recurring bills. Automated teller machines, electronic deposit, and the rapid clearing of checks among banks are but the most visible benefits of electronic funds transfer (EFT) to the consumer.

The use of electronic funds transfer (EFT) at point of sale with debit cards is increasing rapidly with online debit networks introduced by VISA, Mastercard, and the Cash Station. Two-thirds of the nation's grocery stores now accept debit cards. Electronic Funds Transfer networks are now international in scope, allowing consumers to obtain cash worldwide and banks to transfer funds globally.

Security concerns are of paramount importance to the financial industry. Electronic funds transfer (EFT) systems have therefore made extensive and very effective use of cryptography to safeguard financial transactions.

6. ONE METHOD OF TRANSLATING EDI DOCUMENT:

Electronic Data Interchange (EDI) allows your company to communicate with your customers and vendors electronically, eliminating human error. EDITS™ provides complete EDI translation and transaction management services to help organizations deploy advanced electronic data technologies in a cost effective manner. EDI is widely used throughout the automotive and retail industries and EDITS™ application eliminates the e-Commerce communication headaches and the cost of Value Added Networks (VANs). EDITS™ simplifies the EDI process by providing and maintaining the infrastructure costs needed to run a full EDI system in-house.
A number of transaction types may be performed, including the following:

- Sale: where the cardholder pays for goods or service
- Refund: where a merchant refunds an earlier payment made by a cardholder
- Withdrawal: the cardholder withdraws funds from their account, e.g. from an ATM. The term Cash Advance may also be used, typically when the funds are advanced by a merchant rather than at an ATM
- Deposit: where a cardholder deposits funds to their own account (typically at an ATM)
- Cashback: where a cardholder withdraws funds from their own account at the same time as making a purchase
- Inter-account transfer: transferring funds between linked accounts belonging to the same cardholder
- Payment: transferring funds to a third party account
- Enquiry: a transaction without financial impact, for instance balance enquiry, available funds enquiry, linked accounts enquiry, or request for a statement of recent transactions on the account
- E top-up: where a cardholder can use a device (typically POS or ATM) to add funds (top-up) their pre-pay mobile phone
- Mini-statement: where a cardholder uses a device (typically and ATM) to obtain details of recent transactions on their account
- Administrative: this covers a variety of non-financial transactions including PIN change

The transaction types offered depend on the terminal. An ATM would offer different transactions from a POS terminal, for instance.

EDI software generally contains a translation component that maps data from the user's (i.e., originator's) application (i.e., record formats) to the Electronic Document Interchange standard message formats. The translation of messages in standard EDI formats to the recipient's application is performed by the recipient's EDI software. The communications component adds items to the message to form a complete interchange and interfaces to the underlying communications mechanism. This mechanism can be a low level protocol, such as bisync, or a full-blown messaging protocol, such as X.400.

Communications might flow directly to the recipient (i.e, point-to-point) or by means of a third party. There may also be components that handle report writing, management, audit, and printing functions. Nearly all existing EDI implementations, unlike those for electronic funds transfer (EFT), do not currently use cryptography for security. However, a substantial number of Electronic Document Interchange products offering encryption and digital signatures will filter into the market soon.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

An EDI interchange consists of the production, transmission, receipt of, and response to a formatted text message. Originator and recipient IDs and associated information, as well as one or more functional groups of business data, constitute a message. A functional group consists of one or more related transaction sets, each representing a common business document. For example, transaction set 813 is a tax return; 832 is a price or sales catalog. The transaction sets are usually composed of multiple data segments that provide such information as names, addresses, rates, and handling instruction in a specified sequence. Each data segment is uniquely designated by two or three letter identifiers.

Once prepared, an EDI document must be delivered to the trading partner. Data can be sent via high-speed data lines or lower speed dial-up lines, by magnetic tape or diskette, or on X.25 public switched data networks. The documents may be delivered directly, or more typically, by a third-party, value-added network (VAN) or clearinghouse—an EDI postal system. The use of a VAN simplifies the communications process substantially, because communications must be coordinated with one party rather than with all trading partners. The VAN can convert protocols and line speeds, enabling communication between otherwise incompatible systems. Some VANs also offer format translation, electronic forms, fax services, message switching, and access to a variety of data bases.

Typical VANs presently provide only a few useful security capabilities. Passwords or authorization codes are required to send or receive documents from electronic mailboxes. A VAN also tracks the movement of documents within its domain and can provide notification of delivery and an audit trail when required. The EDI documents originator logs on to the network by using a password. The uploaded document is placed in the recipient's electronic mailbox. The recipient, after meeting network security tests, retrieves mail periodically. Some VANs specialize in particular vertical markets; others are generalists. Examples include Advantis, EDI*Net,EDI*EXPRESS, and AT EasyLink. VANs typically support all public and industry specific standards.

7. AUTHORIZATION

EDI transactions require communication between a numbers of parties. When a card is used at a merchant or ATM, the transaction is first routed to an acquirer, then through a number of networks to the issuer where the cardholder's account is held.

A transaction may be authorized offline by any of these entities through a stand-in agreement. Stand-in authorization may be used when a communication link is not available, or simply to save communication cost or time. Stand-in is subject to the transaction amount being below agreed limits. These limits are calculated based on the risk of authorizing a transaction offline, and thus vary between merchants and card types. Offline transactions may be subject to other security checks such as checking the card number against a 'hotcard' (stolen card) list, velocity checks (limiting the number of offline transactions allowed by a cardholder) and random online authorization.

Trading partner agreements (TPAs) or interchange agreements are contractual agreements between two entities that conduct business electronically. They structure the electronic relationship between trading partners, dealing with standards, liability, responsibility, and fees. They are essential to reduce misunderstanding and act as the basis for enforcing future Electronic Document Interchange transactions. The use of Trading Partner Agreement is increasing between EDI users as various model agreements become available and EDI case law develops.

TPAs can and should explicitly define the security obligations of the two parties, because the EDI system's trustworthiness and reliability are inextricably tied to these obligations. The agreement should cover verification of message delivery, access control, use of cryptographic algorithms, use of digital signatures, notification, and remedial actions in the event of security breaches.
Model agreements can, over time, establish common trade practice. As case law develops around them, many trading partners find common provisions are considered to apply to their transactions without their explicit consent.
Third-party service provider agreements are similar in concept to TPAs but are contractual agreements between trading partners and VANs or other providers of communications services. The areas that third-party agreements should address include, but are not limited to, access to audit data, data storage periods, and the full range of access control and security procedures.

8. EDI MASSAGES-SECURITY AND TRUST MODELS

In relatively closed systems, such as within a company, it is easy to trace a path of trust back to the root. However, in the real world, users must often communicate with people outside of their corporate environment, including some whom they have never met, such as vendors, customers, clients, associates, and so on. Establishing a line of trust to those who have not been explicitly trusted by certified company is difficult. Companies follow one or another trust model, which dictates how users will go about establishing key validity. There are three different models:

- Direct Trust
- Hierarchical Trust
- A Web of Trust

As both Electronic Document Interchange and Electronic Funds Transfer become more widespread, so does the opportunity for misuse and corruption. With the increasing population of users, progressively more traffic will pass between organizations that have dissimilar backgrounds, security needs, and security controls. The speed with which EDI is being implemented into progressively smaller organizations that were previously little concerned with data security will leave many users vulnerable.

The open system can be interpreted as the conjunction of large networks of computer systems in which computer activity and data flow among the population at large. This understanding encompasses transorganizational computing and views all the world's networks as an aggregated system. This view is appropriate when considering electronic mail, EDI, and electronic commerce in general.

Old security paradigms called for a fortress approach in which corporate computing and information resources were structured around a central mainframe, or group of mainframes, concentrated in one or more sites. The goal was to make the site physically secure, to ensure that the networks that accessed the computer were well understood and appropriately secure, to require user validation with passwords, and then to ensure that users could access only programs and data pertinent to their work.

In open systems, everyone has a platform. There is no longer a central computer managed by computer security professionals. Even if all users in such organizations manage their own computer security carefully and diligently, all users outside the organization surely will not.

Old security paradigms cannot be discarded; they must be augmented. Security for the typical EDI system incorporates security paradigms perfected over the past 30 years and requires new ones as well. Public key cryptography is an essential one.

Threats to EDI or electronic funds transfer (EFT) systems include both those from outside the organization and those from within, those made deliberately and those made as the result of error. All can be devastating. Insider threats are estimated to be responsible for from 70% to 80% of the annual dollar loss attributable to all security threats. Much of that loss is attributable to error, accident, and omission; dishonest and disgruntled employees' actions are also responsible for sizable losses. Any security program that focuses exclusively on threats from the outside is misdirected. Deliberate threats include data destruction by deletion, with viruses or Trojan horses, wiretapping, the creation of bogus documents, and the rerouting or replaying of authorized documents. Accidental threats to an EDI system's security can include data entry errors, deletion of data, misfiling, and the misrouting of documents.

Many security threats can be effectively countered by traditional data processing security controls that safeguard entire systems (e.g., optimally scheduled data back-ups and secure physical access and password control). Other security threats must rely on innovative technologies, such as public key cryptography, for elegant solutions. In the data communication content security controls are known as security services. The five traditional services are confidentiality, integrity, authentication, nonrepudiation and access control.
Any security system for EDI should provide for confidentiality to ensure that sensitive or mission critical information is not disclosed or made available to unauthorized parties. The security of EDI documents must be ensured while they are stored on a computer system or are being transmitted between systems or trading partners.

As important as confidentiality is the need to ensure document integrity. This means preventing the accidental or deliberate alteration or destruction of data or even its delay in transit.
Authentication may be the most critical of the security concerns. Passwords and personal identification numbers have often been used for keeping unauthorized users from masquerading as legitimate. For high-value transactions, however, these measures are not sufficient, because the systems they run on may be vulnerable to password guessing, data line eavesdropping, and unauthorized disclosure. In the context of electronic business, nonrepudiation is a critical security requirement in two circumstances. If the sender of an electronic order or tax return can later deny responsibility for originating that transmission, the recipient may be potentially injured or the sender may benefit. Similarly, senders and receivers should try to avoid disputes over whether a document was delivered or when delivery took place.
Access controls attempt to restrict access to components of the system exclusively to authorized parties. Controls protect hardware, communications media, application software, and data. But access control, long the mainstay of corporate computing security efforts, is insufficient to protect against the roguish acts of authorized parties.

One additional capability that would be useful in EDI or electronic funds transfer (EFT) systems is authorization. After ensuring that a particular user signed a transaction, systems should ensure that user's authority to do so. This topic is a new area of interest in American National Standards Institute X9 standards and should eventually find its way into the X12 standards. The intent is to provide additional certification defining what an individual is allowed to do in the way of authorizing resources, such as expenditures, and how this authority is limited. For example, a user might be limited to signing only purchase orders for less than$50,000. Another important limitation would be a stipulation specifying that dual control (e.g., multiple signatures) is required to exercise monetary authority. Such mandated multiple signatures provide the electronic analogue to the tradition of dual controls designed to ensure that individuals cannot act against their organization's policies.

9. PRETTY GOOD PRIVACY (PGP) FOR DIFFERENT TRUST MODELS

Pretty Good Privacy (PGP) is one of today's most widely used public key cryptography programs. Developed by Philip Zimmermann in the early 1990s and long the subject of controversy, PGP is available as a plug-in for many e-mail clients, such as Claris Emailer, Microsoft Outlook/Outlook Express, and Qualcomm Eudora.
PGP can be used to sign or encrypt e-mail messages with the mere click of the mouse. Depending upon the version of PGP, the software uses SHA or MD5 for calculating the message hash; CAST, Triple-DES, or IDEA for encryption; and RSA

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

or DSS/Diffie-Hellman for key exchange and digital signatures.
When PGP is first installed, the user has to create a key-pair. One key, the public key, can be advertised and widely circulated. The private key is protected by use of a passphrase. The passphrase has to be entered every time the user accesses their private key.

Most logical access control software products for large systems and networks can restrict access based on an employee's classification. Even this basic feature, however, is underused by most organizations. The capability to encrypt the data on disk drives should be considered essential for systems housing financial, medical, or other sensitive data. This is true for companies using Electronic Document Interchange or electronic funds transfer (EFT), as well as for those with computerized payroll, accounting, purchasing, or electronic mail systems.

Security on individual platforms, such as a workstation, is addressed by the Department of Defense's Trusted Computer System Evaluation Criteria (TCSEC), also known as the Orange Book. The criteria cover only non classified environments and are primarily concerned with identification, authentication, and access control. The Trusted Computer Security Evaluation Criteria are currently undergoing revision to align them with their Canadian and European equivalents. The revision provides security requirements for various environments. It will more adequately address the needs of the commercial environment.

Security provisions should be integral to most TPAs. The parties should agree to the need for security, the level of security to be provided, and the form that security should take. Different EDI transactions have varying security requirements. Low-value or low-risk transactions have considerably different security needs than do high-value or high-risk ones. A transaction that provides a catalog of products and prices may require only assurance of document integrity, whereas a tax return or medical records require authentication, confidentiality, and integrity assurance.

The level of security required and the detail necessary in a TPAs is determined by a risk analysis for the types of transactions occurring between trading partners. Traditional risk analysis tools have a limited value in the present Electronic Document Interchange environment, and until EDI specific tools can be developed, such analysis must be based on limited experience and common sense.

In the EDI environment, cryptographic controls are still in their infancy. They were not deemed necessary when EDI was conducted directly with a minimum number of trusted trading partners. With the new standards and the capability to initiate ad hoc transactions, these cryptographic controls will quickly mature.

Electronic data interchange is emerging as one of the critical enabling technologies necessary for the rapid development of true global business capability. The spreading use of Electronic Document Interchange leaves many organizations vulnerable to a variety of attacks from both within and outside the organization. Security of the majority of existing Electronic Document Interchange systems is far from ideal. In addition to strengthening proven security safeguards, there is a need to provide new security capabilities. As will be seen in Part 2 of this two-part series, cryptography offers a number of elegant solutions to previously intractable security and legal problems.

10. CONCLUSION

This paper has briefly described how cryptography works in EDI. However, that there are a number of ways to attack every one of these systems; cryptanalysis and attacks on cryptosystems. In the words of Sherlock Holmes (ok, Arthur Conan Doyle, really), "What one man can invent, another can discover" ("The Adventure of the Dancing Men"). Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret.
The irony is that today, secrecy is not the key to the goodness of a cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well-documented because they are also well-tested and well-studied! In fact, time is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one. The strength of cryptography lies in the choice (and management) of the keys; longer keys will resist attack better than shorter keys. By further research can ensure more security for EDI.

REFERENCES

[1] W. Stalling, “Cryptography and Network Security”, Third edition, Pearson, 2003

[2] Dorothy Elizabeth Roblin Denning, “Cryptography and Data Security”, Chapter 1, Page 49.1999.

[3] Jorge Guajardo, “Efficient algorithms for elliptic curve cryptosystem”, Worcester Polytechnic institute, May 1997.

[4] Roger Clarke, “Introduction to Dataveillance and Information Privacy, and Definitions of Terms,” http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html, last visited Nov 2005.

[5] Arif Tumer, Asuman Dogac, and I. Hakki Toroslu, “Semantic-based User Privacy Protection Framework for Web services,”

[6] W. M. Farmer, J. D. Guttman and V. Swarup, “Security for Mobile Agents: Issues and Requirements,”In Proc. of the 19th National Information System Security Conference, Baltimore, MD, 1996, pp. 591-597.

[7] Morris Sloman and Emil Lupu, “Security and management policy specification,” IEEE Network, Special Issue on Policy-Based Networking Vol. 16, no. 2, 2002, pp. 10 – 19.

[8] A. Yao. “Protocols for secure computations,” In Proc. of the 23rd Annual IEEE Symposium on Foundations of Computer Science, 1982

[9] “Cryptography for the Internet,” by Philip R. Zimmermann. Scientific American, October 1998.

[10] “Privacy on the Line,” by Whitfield Diffie and Susan Eva Landau. MIT Press; ISBN: 0262041677.

[11] C.H.Meyer, S.M.Mat.yas,R.E.Lennon, “Required Cryptographic Authentication criteria for Electronic Funds Transfer System”, CH1629-5/81/089, IEEE, in 1981.

[12] Dan Zhu, “Security control in Inter-Bank Fund Transfer”, Journal of Electronic Commerce Research, VOL. 3, NO. 1, 2002.

[13] Mintu Philip,Asha Das, "Survey: Image Encryption using Chaotic Cryptography Schemes", IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011.

[14] Mohammed AbdallahMdAysan, Fareed Hassan Almalki , Abdullah Mohammed Almalki, "New Symmetric key cryptography algorithm using simple logarithm and binary digits", International Journal of Multidisciplinary Research Academy, Vol.4 issue 6, (in printing) Accepted in March 2014.

[15] Mohammed AbdallahMdAysan, Fareed Hassan Almalki , Abdullah Mohammed Almalki, "New Symmetric key cryptography algorithm using simple logarithm and binary digits", International Journal of Multidisciplinary Research Academy, Vol.4 issue 6, (in printing) Accepted in March 2014.

[16] Johnson, J. Z. "Network Security Programs: Process and Metrics for the Real-World", White paper, Internet SecuritySystems, Inc, 1998.

[17] Kalakota R., A. Whinston, "Frontiers of Electronic Commerce", Addision Wesley, MA, 1996.

[18] Ki HyoungKo, Sang Jin Lee, Jung HeeCheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park, "New Public-KeyCryptosystem Using Braid Groups, Advances in cryptology", 20th annual International CryptologyConference, Santa Barbara, California, USA, August 20-24, 2000.

[19] C.H.Meyer, S.M.Mat.yas,R.E.Lennon, "Required Cryptographic Authentication criteria for Electronic Funds Transfer System", CH1629-5/81/089, IEEE, in 1981.

[20] 2) Dan Zhu, "Security control in Inter-Bank Fund Transfer", Journal of Electronic Commerce Research, VOL. 3, NO. 1, 2002.

[21] Q.V. Lawande, B. R. Ivan, S. D. Dhodapkar, Chaos Based Cryptography: A New Approach to secure Communications Asian aerosol conference

[22] Mintu Philip,Asha Das, "Survey: Image Encryption using Chaotic Cryptography Schemes", IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011.

[23] Palmer, J. W. and Griffith, D. A. "An Emerging Model of Web Site Design for Marketing", Communication of the ACM, Vol. 41, No.3, pp. 45-51, 1998.

AUTHOR PROFILES

Md. Safaet Hossain had been working as Assistant Professor in the Department of Computer Science and Engineering at City University, Bangladesh. He has authored papers in national and international journals. His research interest includes Software Engineering, Ecommerce, Web Technology, Image Processing, Communication networks.