Secure Digital Cashless Transactions with Sequence Diagrams and Spatial Circuits to Enhance the Information Assurance and Security Education

Dr. Yousif AL-Bastaki
ACMSIG Teaching & learning
University of Bahrain
P.O. Box -32038
Kingdom of Bahrain

Dr. Ajantha Herath
ACMSIG Teaching & learning
University of Bahrain
P.O. Box -32038
Kingdom of Bahrain

Abstract— Often students have difficulties mastering cryptographic algorithms. For some time we have been developing with methods for introducing important security concepts for both undergraduate and graduate students in Information Systems, Computer Science and Engineering students. To achieve this goal, Sequence diagrams and spatial circuit derivation from equations are introduced to students. Sequence diagrams represent progression of events with time. They learn system security concepts more effectively if they know how to transform equations and high level programming language constructs into spatial circuits or special purpose hardware. This paper describes an active learning module developed to help students understand secure protocols, algorithms and modeling web applications to prevent attacks and both software and hardware implementations related to encryption. These course materials can also be used in computer organization and architecture classes to help students understand and develop special purpose circuitry for cryptographic algorithms.

Keywords-e-cashless; transactions; cryptographic; algorithms; Sequence diagrams, Spatial circuits.

I. INTRODUCTION

During the last decade Postal mail became E-mail, face-to-face Banking became Online Banking and Commerce transformed to E-Commerce. An electronic transaction is an agreement made using internet between a buyer and a seller. The user immediately becomes vulnerable to attacks or infiltration as soon as a computer starts to share the resources available on the web or local network. Confidentiality guarantees privacy, no loss of information from client or the server. Integrity assures no modifications of data, messages or impersonation. Authentication helps identify the user. The validation is provided by an authentication factor which is used to validate or authenticate the communicating person's identity. Confidentiality, Integrity and Authentication is achieved through encryption of the message. Authentication is implemented through encryption, signatures and certificates [1]. The Kerberos authentication service restricts access to authorized users all the time with single sign-on. It is secure and scalable to support a large number of clients and servers. Kerberos ticket generation resembles social systems such as an airline system where a user purchases a ticket to receive the service. Figure 1 illustrates online airline ticket purchase. Symmetric key cryptography consists of a private key that is used for both encryption and decryption. Faster symmetric key encryption algorithms like Advanced Encryption Standard, AES, are popular for larger data encryption.

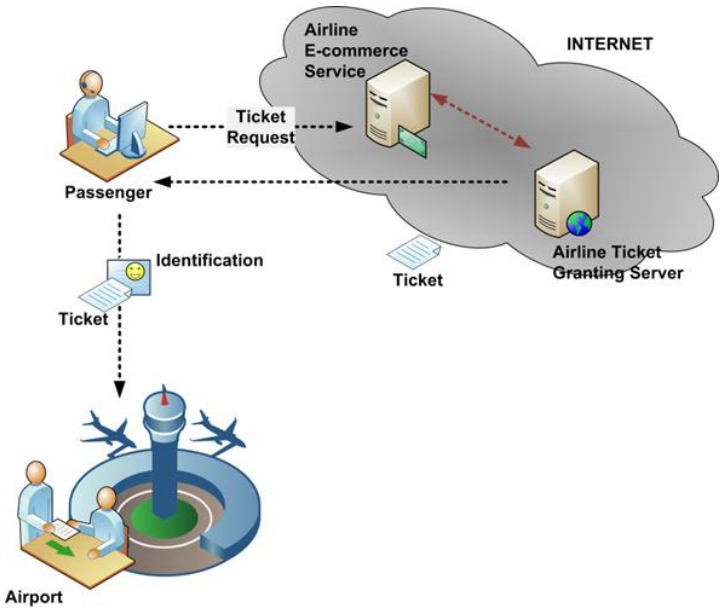

Figure 1: Airline Ticket Processing

The Kerberos authentication scheme consists of a client, Kerberos Authentication Server, Ticket Granting Service and a service provider. Kerberos communications are represented using a sequence diagram as shown in Figure 2. Encrypted keys and tickets help sharing symmetric keys.

Non-repudiation makes sure of the security of the E-Commerce transaction. It ensures participants online actions undeniable and no back out of their transaction later. Hence, the seller cannot change the agreed price or delivery time frame and the customer cannot change his/her mind of the product by considering the low price of other vendors after confirming the transaction. The digital certificate, encryption

and signature methods are useful in this matter because each party can validate the sender of the message and information.

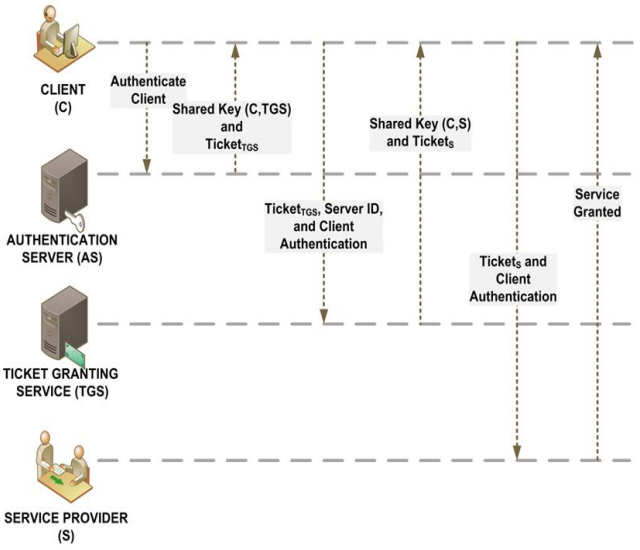

Figure 2: Kerberos Authentication

Availability ensures that the system responses promptly and the service and information is available when needed to authorize persons. Flooding machine with requests or filling up memory threatens the Availability. Denial of service is the consequence of such an attack. Availability of the service can be improved by providing fast, reliable and efficient service. The network security is the key feature of ensuring availability of the service. Therefore, deploying network security devices such as firewalls and configuring them along with associated protocols properly is the key to ensuring service availability.

Asymmetric key cryptography consists of a pair of public and private keys. The private key is kept secret whereas the public key is distributed for use by multiple parties.

Digital Signatures are used to provide authenticity. A message signed with merchant's private key can be verified by any consumer who has access to merchant's public key. David Chaum proposed the blind signature scheme based on RSA digital signature and its application for online electronic cash system. Thereafter, Okamoto developed the first practical divisible electronic cash system. A. Chan and Frankel further improved the divisible electronic cash system. This verifies that the signed message has not been tampered with by any unauthorized party.

A public key certificate contains the identity of the certificate holder such as name, public key and the digital signature of the certificate issuing authority. Public key certificate is used to validate the sender's identity. The certification authority attests that the public key indeed belongs to the sender.

Section 2 of this paper provides a brief description of an e-commerce transaction, derivation of a sequence diagram from the transaction that could be used in software system implementations and major threats that might be seen in an e-commerce transaction. Also, it discusses five major security concepts that can be used to avoid those threats. Section 3 presents some details of integration of confidentiality, integrity and authentication to the transaction. Section 4 describes the transformation of security equations in secure electronic transactions [2-4] to spatial circuits that could be used in hardware implementations. It also illustrates the working of dual signature. Section 5 describes other related work in electronic transactions.

II. E-Commerce Transactions

Major players of electronic cashless transactions are clients, internet service providers, merchant's servers, client's and merchant's banks, warehouses and deliver services. In a transaction diagram major players are represented by nodes and directed arcs present messages transferred. Purchase of goods from the internet can be represented using a sequence diagram as shown in Figure 3.

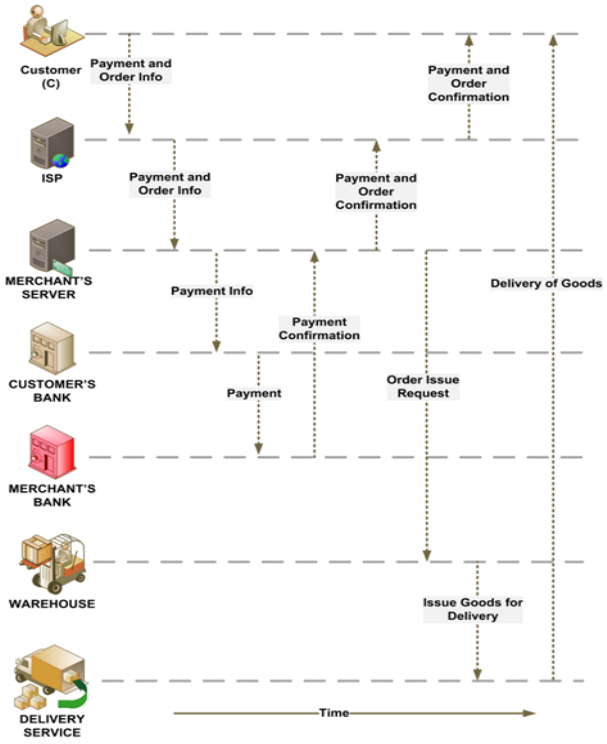

Figure 3 Sequence Diagram for an E-Commerce Transaction

The sequence diagram illustrates the snapshot of the sequence of events taking place represented in the vertical axis progressing from top to bottom and the particular time slot of the event taking place is shown in the horizontal axis from left to right. The Client first sends payment and order information to merchant's server via internet service provider. Then the Merchant's server sends payment information to client's bank. The client's bank then sends the payment to merchant's bank. Payment confirmation will be issued by the merchant's bank to the Merchant's server. Thereafter the payment and order confirmation will be sent to the client by the merchant's server via ISP. The Merchant's server sends the order issue request to the warehouse. Warehouse issues goods for delivery. The delivery service delivers the goods to the client.

Figure 3 also depicts the insecure e-commerce transaction. In this transaction any one can read or modify the payment

and order information. An intruder can interrupt, modify or initiate the transaction. Client's bank information can be stolen by a third party. Particularly, E-commerce transactions involve with client's and merchant's secure information such as credit/debit card numbers and private information. Most of the communications among the client, merchant and banks are done through the internet. Much of the message passing, billing and payments are done by electronic message transfers. There is a higher possibility of stealing, loosing, modifying, fabricating or repudiating information. Such systems and messages transmitted need extra protection from the eavesdroppers.

Many threats such as Denial of Service, DoS, Distributed Denial of Service, DDoS, Trojans, phishing, Bot networks, data theft, identity theft, credit card fraud, and spyware can be seen in these systems. These attacks might cause the loss of private information or revelation of sensitive information such as credit card numbers and social security numbers, misinterpretation of users, gaining unauthorized access to sensitive data, altering or replacing of data. Sniffing can take place at vulnerable points such as ISP, Merchant's server, client's bank, merchant's bank or at the internet back bone.

III. Consolidation of Integrity, Confidentiality and Authenticity in Applications

Providing confidentiality is vital in e-commerce. Figure 4 shows the transaction with confidentiality. The transaction can be made secure by converting the plain text message to cipher text so that the holders of the keys can decrypt and read the messages. Common algorithms used to achieve this encryption and decryption goal are AES, DES with single symmetric keys and RSA with public/private asymmetric key pairs.

Encryption will prevent strange third party to have client's credit/ debit card numbers, passwords, pin numbers or personal details. But in the internet world there are many possibilities that an unauthorized third party can obtain this sensitive and private information and violate the privacy of the people, particularly in e-commerce service, the privacy of the consumer and the merchant. Thus, this e-commerce system needs to be assured that the information is not to be spread to the unauthorized people in order to provide a genuine and reliable service. The symmetric encryption plays a key role in assuring confidentiality of the data because even though an unauthorized third party intercepts the message, usage of the unique session key, which can be accessed only by the two parties involved, prevents that person from viewing the message. Hence, the encryption of the information is not only guaranteed by the authentication of the information but also it assures confidentiality of the information.

To make the transaction secure the data need to be received free from modification, destruction and Repetition. When we consider the security of the electronic transaction, data integrity is another significant feature, because changing address, order information, or payment information may have possibly happened in this system. Therefore, to get the message free from modifications the e-commerce system should provide protection to the message during transmission. This can be achieved by using encryption and message digesting.

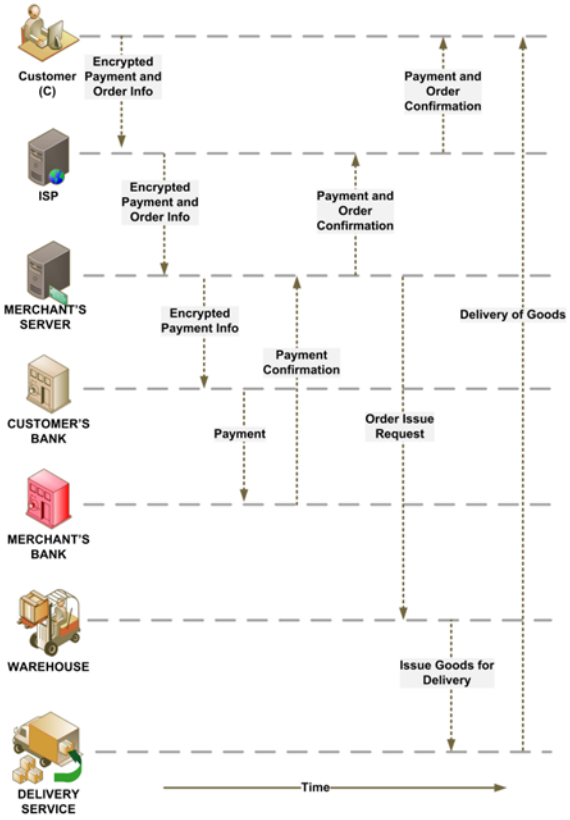

Figure 4 E-commerce Transaction with Confidentiality

A unique message digest can be used to verify the integrity of the message. Hash functions take in a variable length input data and produce a fixed length unique outputs that are considered as the fingerprint of an input data/message. Thus, it is very likely that if two hashes are equal, the messages are the same. Hash functions are often used to verify the integrity of a message.

The sender computes hash of the message, and concatenates the hash and the message, and sends it to the receiver. The receiver separates the hash from the message and then generates the hash of the message using the same hash function used by the sender. The integrity of the message is said to be preserved if the hash generated by sender is equal to the Hash generated by the receiver. This implies that the message has not been altered or fabricated during the transmission from sender to receiver.

Encryption algorithms such as AES, DES could be used to generate message digests. In addition there are special purpose hash functions such as SHA-3 [5] for this purpose. SHA-3 is the message-digest algorithm developed by the National Institute of Standards and Technology and the National Security Agency. SHA-3 will be selected from five new Hash functions, BLAKE, Groestel, Skein, JH and Keccek. Grooestel is similar to AES. SHA-1 is secure but slower than MD5. MD5 produces the digest of 128 bits whereas SHA-1 produces

a 160-bit message digest and is resistant to brute force attacks. It is widely used for digital signature generation.

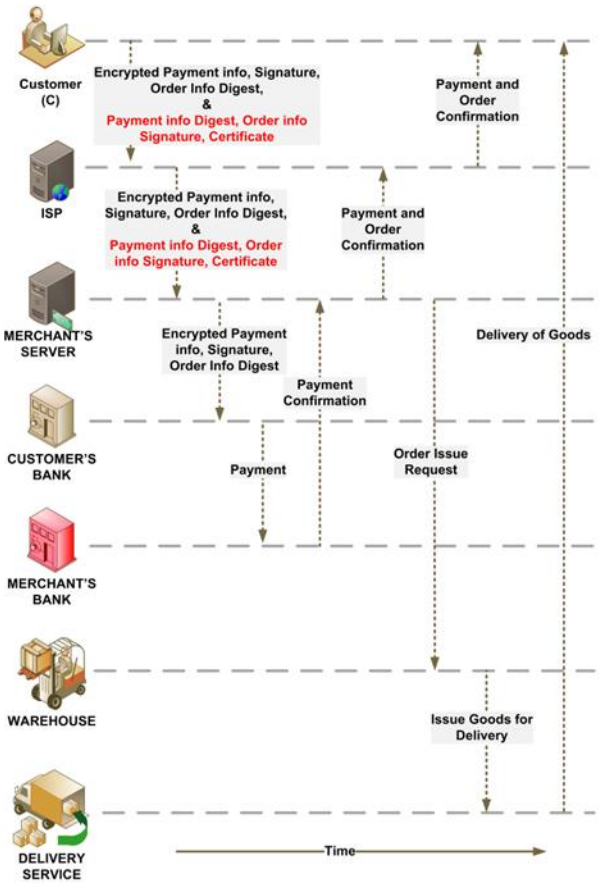

Figure 5 Secure Transaction

The Figure 5 shows how the authenticity, confidentiality and integrity can be used in our example. It uses the encryption, message digest, digital signature and digital certificate to ensure the authenticity, confidentiality and integrity of the order and payment information. Fig. 6 represents the transaction with symbols.

One of the most important aspects of the security of the transaction is authenticating that the suppliers and consumers are who they say they are and assure the trustworthiness of the sources they are exchanging. This is really important in cashless e-commerce transactions because of the supplier and consumer never meet face to face. Authentication can be presented in different ways. Exchanging digital certificates helps seller and buyer verify each other's identity so that each party knows who is at the other end of the transaction. The digital signature is another method to be certain that the data is indeed from a trusted party. In addition, symmetric encryption can also be used in certifying the authenticity. In this way, the receiver of the information can make sure that the information that they have received is sent by a trusted party, because the key that is used to encrypt and decrypt the information is shared only by the sender and the receiver.

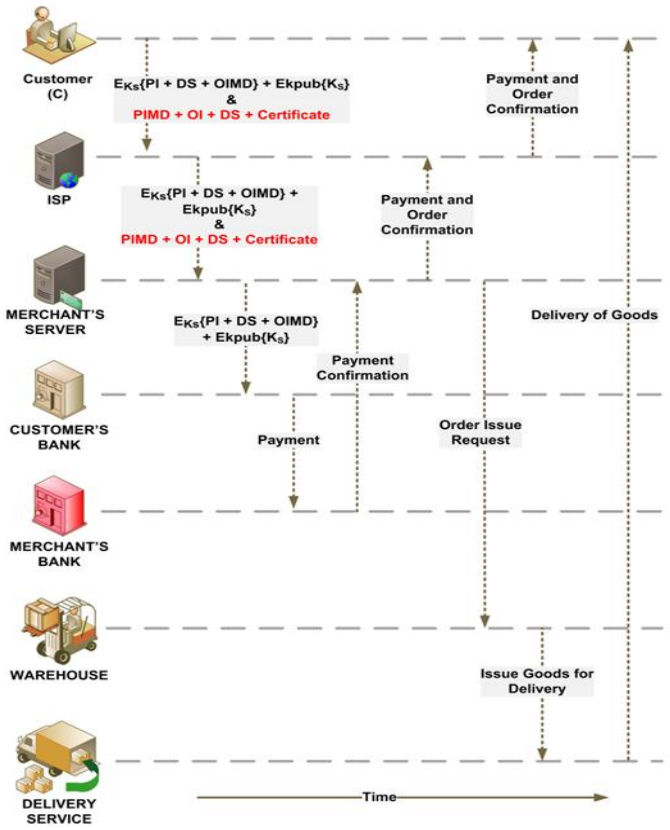

Figure 6 Secure Transactions with Symbols

In Figures 5, 6 and 7
PI = Payment Information
DS = Dual Signature
OIMD = OI message digest
Ks = Temporary symmetric key
PIMD = PI message digest
OI = Order Information
Certificate = Cardholder Certificate.

IV. Symbolic Representations and Algorithms to Spatial Circuits Transformation

The equation in Figure 5

$$\mathbf{E_{ks}\{PI + DS + OIMD\} + E_{k\ pub\ B\{}\{K_s\} \ \& PIMD + OI + DS + Certificate}$$

summarizes the message generation in Secure Electronic Transaction protocol, an application of hashing and encryption algorithms in providing integrity, confidentiality and authentication for messages.

This message consists of two parts: one for the client's bank and the other for the merchant. The request message part **{PI + DS + OIMD}** is encrypted by using the session key $\mathbf{K_s}$. The Digital Envelope consists of the session key encrypted by using the public key of the Bank $\mathbf{K_{pubB}}$. Secure transactions use both public and private key encryption methods for message exchange between the merchant and the consumers. The DES – Data Encryption Standard algorithm is used by most financial institutions to encrypt Personal Identification

Numbers. Light-weight-crypto algorithms such as Simplified-DES take an 8-bit block of plaintext and a 10-bit key as input to produce an 8-bit block of ciphertext. A spatial circuit can be easily drawn from this representation as shown in the Figure 6:

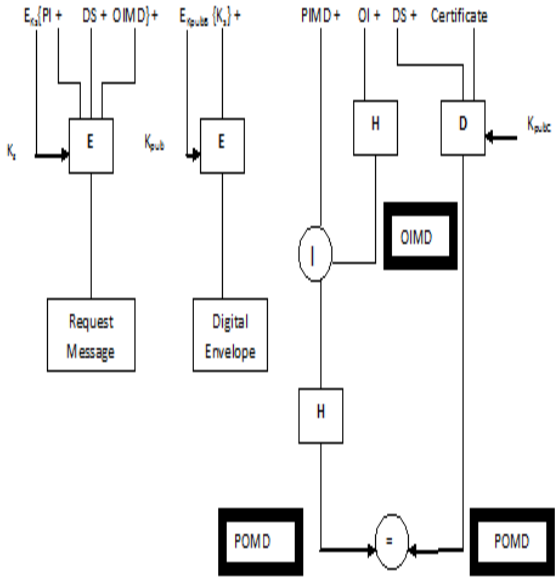

Figure 7 Cardholder Sends Purchase Request / Merchant Verifies

In Figure 7
POMD = Payment order message digest
D = Decryption (RSA)
H = Hash function
E = Encryption (RSA for asymmetric and DES for symmetric)
KpubB = Bank's public key-exchange key
KpubC = Customer's public signature key.

The goal of dual signature generation and use is to send a message that is intended for two different recipients. Each recipient has access to the message, however only a part of the message can be read by each. In case of SET protocol, the customer sends the order information (OI) and payment information (PI) using dual signature. The merchant can only see the OI and the bank can only access PI. Figure 6 shows how the order information and payment information is securely delivered to the two recipients – merchant and bank using Dual Signature, DS.

In Figure 8
PI = Payment Information
OI = Order Information
PIMD = PI message digest
OIMD = OI message digest
POMD = Payment order message digest
H = Hash function (SHA-1)
|| = Concatenation
E = Encryption (RSA for asymmetric and DES for symmetric)
K_{priC} = Customer's private signature key

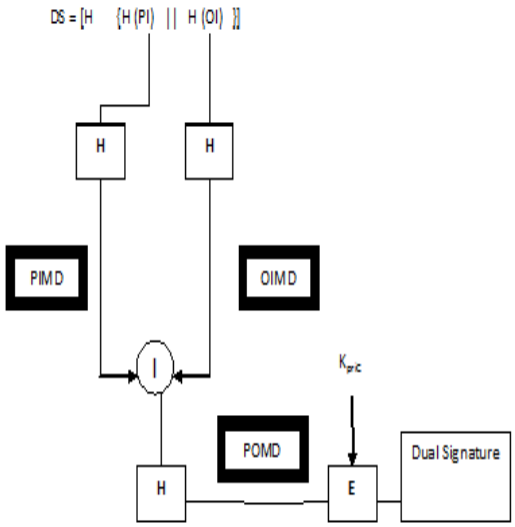

Figure 8: Construction of Dual Signatures in SET

Figure 8 illustrates the spatial circuit drawn for the dual signature generation. The digital envelope combines the speed of DES and efficient key-management of RSA. The envelope and the encrypted message is sent to the recipient who decrypts the digital envelope using his private key to generate the symmetric key and then uses this symmetric key to regenerate the original message.

Similarly, encryption and decryption algorithms can be easily transformed into spatial circuits. An algorithm to hardware transformation is an important concept to introduce in system security courses. Students learn cryptographic algorithms faster if they know how to transform equations and high level programming language constructs, such as arithmetic expressions, for loops and algorithms into spatial circuits or special purpose hardware. Figure 9 shows the *for* loop and the final round of the Blow Fish encryption algorithm

For i = 1 to 16 do
REi = LEi-1 Ex-OR Pi
LEi = REi-1 Ex-OR F (REi)
Final Round
LE17 = RE16 Ex-OR P16
RE17 = LE16 Ex-OR P17 .

V. Other Related Work

There are other electronic cashless payment protocols such as credit card, e-cash, e-check, smartcard and micropayment used over the Internet. In credit card based platforms, the consumer uses a card containing card holder's financial information issued by a bank. This credit card is used to purchase items over the Internet. E-cash is a digital form of money provided by a certified financial institution. Consumers need to install software on their machine called e-wallet. The e-wallet contains consumer's financial information that can be accessed using an ID and password. Consumers can use this

account to transfer funds online and withdraw from or deposit to banks.

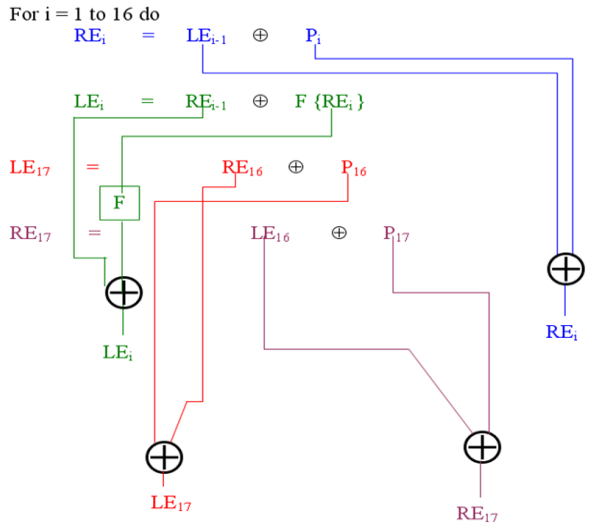

Figure 9 Algorithm to Spatial Circuit – BlowFish Encryption

PayPal is the most successful e-wallet application used in the industry today. It operates in many countries, manages millions of accounts and allows consumers to send, receive and hold funds in different currencies worldwide.

E-check is similar to e-cash except that it uses a check instead of digital money. E-check contains consumer's bank information such as account number, bank's routing number, check number, amount paid and the date of authorization. This information is used by the merchant to authenticate the consumer and the consumer's bank uses this information to authorize the payment. One advantage of e-check is that they can clear much faster than conventional check.

Micropayment systems are more practical for environments with low-cost transactions. Several platforms available in the industry today include CyberCoin, NetBill, PayWord and MicroMint. The biggest difference between micropayment and other payment systems is their operating costs. In order to make the payment system profitable, various payment approaches are used such as service prepayment, reduction of computational load, offline authorization and grouping of micropayments before financial clearance.

One common way of achieving this computational reduction is by using symmetric encryption algorithms over public key algorithms whenever possible. Using one key for both encryption and decryption will reduce the number of keys generated for the total transactions in a given day. Offline authorization can reduce computational load. This can be done by not doing any online verification with the verification center until each individual transaction is grouped offline. Another advantage is that it gives consumers partial anonymity for individual transactions.

VI. Conclusion

This paper summarized mathematical representations used in security as well as spatial circuits to represent cryptographic algorithms, providing examples related to confidentiality and integrity and their combinations. The active learning module developed can be easily adapted and effectively used in a classroom with senior undergraduate or graduate students in Computer Science, Engineering and Information Systems to teach other symmetric key algorithms and help students understand quickly. Both reading and interpreting equations are important in Computer Security classes. To survive in a highly competitive internet world the service provider need to be able to offer fast, reliable and secure service to their customers. In addition, providing trustworthiness among the merchant, the consumer, and the credit or economic institution is always required. We can assume that these e-commerce transactions are safe and trusted, but it is not easy to find out the degree of safeness and trustworthiness in the electronic world.

References & Bibliography

[1] Stallings, Williams. "Cryptography and Network Security Principles and Practice Second Edition" Prentice Hall, 2012

[2] "IBM International Technical Support." Secure Electronic Transaction: Credit Card Payment on the Web in Theory and Practice. Jun 1997. http://www.redbooks.ibm.com/redbooks/pdfs/sg244978.pdf

[3] Ganesh, Ramakrishnan. "Secure Electronic Transaction (SET) Protocol." Information Systems Control Journal, Volume 6. 2000

[4] Bella, G. Massacci, F. and Paulson, L. "Verifying the SET Registration Protocols." Proceedings of IEEE Journal of Selected Areas in Communications 2003. http://www.cl.cam.ac.uk/~lp15/papers/Bella/registration.pdf

[5] NIST's SHA-3 Contest: http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

[6] Yousif Albastaki Ajantha Herath E-Learning of Security and Information Assurance with Sequence Diagrams, ACM Gulf Region special Interest Group of research, HCCE-2012, The Joint International Conference on Human-Centered Computer Environments (HCCE) Aizu Japan

[7] A. Herath S. Herath et al, Learning Digital Cashless Applications with Consolidation of Authenticity, Confidentiality and Integrity using SequenceDiagrams, Conference on Computer Science, Engineering and Applications ICCSEA-2011) Dubai May 2011

[8] VISA Partner Network." Visa Authenticated Payment Program. Apr 2007. https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrievalId=118

[9] Andam, Z. (2003). e-commerce and e-business. Technical report, e-ASEAN Task Force and UNDPAPDIP.

[10] Androutsellis-Theotokis, Stephanos. Spinellis, Diomidis. "A survey of peer-to-peer content distribution technologies" ACM Computing Surveys (CSUR.). Dec 2004.

[11] Becker, A. (2008). Mobile commerce security and payment methods. In Electronic Commerce: Concepts, Methodologies, Tools and Applications, page 295. IGI Global.

[12] Bella, G. Massacci, F. and Paulson, L. "The Verification of an Industrial Payment Protocol: The SET purchase phase." Proceedings of 9th ACM Conference on Computer and Communications Security 2002

[13] Bella, G. Massacci, F. and Paulson, L. "Verifying the SET Registration Protocols." Proceedings of IEEE Journal of Selected Areas in Communications 2003. http://www.cl.cam.ac.uk/~lp15/papers/Bella/registration.pdf

[14] Bidgoli, H. (2002). Security issues and measures: Protecting electronic commerce resources. In Electronic Commerce: Principles and Practice, pages 363–394. Academic Press.

[15] Bollin, Sherrie. "E-commerce: a market analysis and prognostication." Communication Partners International, Carmel, CA. 1998

[16] Brustoloni, Jose. "Advertising and Security for E-Commerce: Protecting electronic commerce from distributed denial-of-service attacks." Proceedings of the 11th international conference on World Wide Web WWW '02. May 2002.

[17] Castelluccia, Claude. Mykletun, Einar. Tsudik, Gene "Improving secure server performance by re-balancing SSL/TLS handshakes" Proceedings of the 2006 ACM Symposium on Information, computer and communications security. Mar 2006.

[18] Chou, Jerry. Lin, Bill. Subhabrata, Sen. Oliver, Spatscheck "Minimizing collateral damage by proactive surge protection" Proceedings of the 2007 workshop on Large scale attack defense. Aug 2007.

[19] Cox, B.Tygar, J.D. and Sirbu, M., "NetBill security and transaction protocol." Proceedings of 1st USENIX Workshop on Electronic Commerce, New York. 1995

[20] Dai, Q. Kauffman, R. "Business Models for Internet Based E-Procurement Systems and B2B Electronic Markets: An Exploratory Assessment" 34th Annual Hawaii International Conference on System Sciences (HICSS-3))-Volume 7. Jan 2001.

[21] Wei, Kai. Chen, Yih-Farn and Smith, Alan. "WhoPay: A Scalable and Anonymous Payment System for Peer-to-Peer Environments." Department of Electrical Engineering and Computer Sciences Univeristy of California, Berkley, CA. May 2005.

[22] Hong, T. and Yuanzhi, Q. (2001). Legal guarantee of the security of electronic commerce. pages 167–170.

[23] D. Chaum, A. Fiat, M. Naor, Untraceable Electronic cash, Advances in Cryptology - CRYPTO '88, 1990.

[24] Yang, S., Su, S., and Lam, H. (2003). A nonrepudiation message transfer protocol for ecommerce. Proceedings of the IEEE International Conference on E-Commerce (CEC03), page 1.4

[25] Tanenbaum, Andrew. Steen, Maarten. "Distributed Systems Principles and Paradigms" Pearson Education. Oct 2006.

[26] Sherif, Mostafa H. "Protocols for Secure Electronic Commerce." CRC PRESS Advanced and Emerging Communications Technologies SERIES Second Edition. Nov 2003.

[27] Sirbu , M. Tygar, J.D. "NetBill: An Internet commerce system optimized for network delivered services" 40th IEEE Computer Society International Conference (COMPCON'95). Mar 1995.

[28] Shaw, M., Blanning, R., Strader, T., and Whinston,A. (2000). Virtual organization and e-commerce. In Handbook on Electronic Commerce, page 491. Spriner.

[29] Sherif , M.H. Serhrouchni , A. Gaid , A.Y. Farazmandnia, F. "SET and SSL: Electronic Payments on the Iner 1. D. Chaum, Blind signature for untraceable payments, Advances in Cryptology – Crypto - 82, Springer Verlag, p.p. 199-203.

[30] D. Chaum, A. Fiat, M. Naor, Untraceable Electronic cash, Advances in Cryptology - CRYPTO '88, 1990.

[31] T. Okamoto, "An Efficient Divisible Electronic Cash Scheme", Advances in Cryptology--Crypto 95, LNCS 963, Springer, pp.438-451, 1995.net" Third IEEE Symposium on Computers & Communications. Jun 1998.

[32] Makoto Matsumoto, Takuji Nishimura., () "Mersenne Twister: A 623-Dimensional Equidistributed Uniform Pseudo-Random Number Generator", ACM Transaction on Modeling and Computer Simulation 1998.

[33] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo., () "Statistical Test Suite for Random and Pseudo Random Number Generators for Cryptographic Applications", National Institute of Standards and Technology Publication. 2001

[34] Lih-Yuan Deng, Hongquan Xu., () "A system of high-dimensional, efficient, long-cycle and portable uniform random number generator", ACM Transaction on Modeling and Computer Simulation, 2003.

[35] Jean-Philippe Aumasson, Luca Henzen,Willi Meier, and Raphael C.-W. Phan. SHA-3 proposal BLAKE, version 1.3. http://131002.net/blake/blake.pdf

[36] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein Hash Function Family. http://www.skein-hash.info/sites/default/files/skein1.1.pdf

[37] Praveen Gauravaram, Lars R. Knudsen, Krystian Matusiewicz, Florian Mendel, Christian Rechberger, and Søren S. Thomsen Martin Schläffer.
Grøstl – a SHA-3 candidate. http://www.groestl.info/Groestl.pdf

AUTHORS PROFILE

Dr. Yousif AL-Bastaki is the Information Technology Advisor to the Hon. Deputy Prime Minster in the Kingdom of Bahrain. He has held several top rank administrative positions at the University of Bahrain and national level. He has edited, published research papers in international journals and conferences. He has written several books in e-government and well recognized as an excellent teacher, researcher and a very good speaker. Dr. Yousif earned his PhD from University of Nottingham, UK in 1996 and MSc from the University of Leeds, Currently he is an associate professor at the University of Bahrain. His research interests includes information assurance, neural networks, genetic algorithms E-Learning, e-commerce protocols secure network protocols, green computing and e-government strategies and implementation.

Dr. Ajantha Herath earned his PhD from the Gifu University, Japan, in 1997. His research interests include e-commerce protocols; secure network protocols, computer forensics and algorithm transformations to cryptographic hardware. He worked as the Professor at the University of Fiji's Department of Computer Science and Information Technology in 2011. At present he is teaching at the University of Bahrain. In 1988 he received the Monbusho research scholarship award. In 2007 he received the Outstanding Research Award for Commitment to Excellence in Computer Forensics and Development of Student Leaders and Researchers from the IEEE–Region 2 AIAA USA. He is a senior member of the IEEE. In 1986, Herath brothers established the Herath Foundation to help financially needy but talented students and awarded more than 7000 scholarships to continue their higher education.