International Journal of Computing and Digital Systems

http://dx.doi.org/10.12785/ijcds/020204

Task based Interdisciplinary E-Commerce Course with UML Sequence Diagrams, Algorithm Transformations and Spatial Circuits to Boost Learning Information Security Concepts

Ajantha Herath [1] Yousif Al-Bastaki[2] and Suvineetha Herath[3]

[1]*IEEE. SIG Research Group (Teaching), University of Bahrain, Kingdom of Bahrain*
ajanthaherath1@gmail.com
[2]*IEEE. SIG Research Group (Teaching), University of Bahrain, Kingdom of Bahrain*
yalbastaki@uob.edu.bh
[3]*IEEE. SIG Research Group (Teaching), University of Bahrain, Kingdom of Bahrain*
suvineethah@gmail.com

Received 7 Mar. 2013, Revised 7 Apr. 2013, Accepted 25 Apr. 2013

Abstract: This paper describes a task based active learning module developed with projects to help students understand secure protocols, algorithms and modeling web applications to prevent attacks. We have been developing and continuously improving cyber security courses with methods for introducing important concepts for computing majors for more than a decade. Sequence diagrams (step by step diagram) , symbolic representations, and spatial circuit derivation from equations and algorithms are introduced to students to alleviate difficulties in mastering cryptographic algorithms. UML Sequence diagrams represent progression of events with time. Spatial circuits illustrate the transformation of equations and high level programming language constructs into special purpose hardware. These course materials can also be used in computer architecture or embedded systems courses to help students understand and develop special purpose circuitry.

Keywords: Task based Learning; E-Commerce; Cryptographic algorithms; symbolic representations; Spatial circuits ; e-wallet; PayPal; UML Sequence diagrams.

I. INTRODUCTION

E-commerce protocols simplified financial transactions such as receiving payments, paying bills, buying merchandise and writing checks. These protocols enable consumers to purchase items over the Internet without compromising their credit card security. E-commerce protocols achieve this goal by using several cryptographic techniques to process the information among the cardholder, merchant, payment-gateway, issuer and certification authority. Cryptographic algorithms such as AES [1], RSA [2], hashing, e-signatures and certificates are used to ensure confidentiality and integrity in communications. Confidentiality prevents unauthorized reading. Encryption algorithms such as AES, RSA could be used to generate unreadable messages. Integrity prevents unauthorized modification. 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 [3] for this purpose. Availability ensures that information is available when needed to authorize persons. Authentication mechanisms such as Kerberos validate communicating entity as the one that it claims to be. Security of RSA relies on the difficulty of factoring large numbers which are used as public-keys. Therefore factoring the largest possible numbers is not only a fascinating scientific challenge but also an indispensable only a fascinating scientific challenge but also an indispensable activity for validating and confirming the security of RSA-based cryptosystems. David Chaum [4] proposed the blind signature scheme based on RSA digital signature and its application for

online electronic cash systems. In 1998, Okamoto [5] developed the first practical divisible electronic cash system. In recent years, electronic voting protocol has been proposed as an alternative to the traditional paper based voting systems [6, 7].

Objectives of this paper are to introduce secure protocols using sequence diagrams, provide the ability to integrate crypto algorithms to design systems that solve real-world problems, implement those, test and document programs to enhance learning security. At the end of the course the students are able to:

1. Design and implement applications that use two or more aspects of security.
2. Apply basic security constructs such as confidentiality, integrity, authenticity, access control in correct programs.
3. Design, implement, test and document secure programs of moderate complexity.
4. Communicate both technical and non-technical aspects of student's work in formal and informal situations.
5. Design and implement crypto algorithms.
6. Solve problems by applying mathematical foundations of cryptography and cryptographic algorithms.
7. Implement cryptographic algorithms and protocols using software.
8. Demonstrate vulnerabilities of cryptographic protocols.
9. Master the essentials of new developments through self-study.

The following sections of this paper present the details of two major projects, a secure e-transaction system and a secure e-voting system, developed for this class. Section 2 describes the derivation of a sequence diagram from an e-commerce transaction. These diagrams could be used in software system implementations and to illustrate major threats that might be seen in an e- transaction. Section 3 describes symbolic representation of messages transferred in a protocol. Section 4 discusses the analogy between social and e-systems. Section 5 discusses attacks on systems. Section 6 presents integration of confidentiality, integrity and authentication to an e-system.

Also, it discusses five major security concepts that can be used to avoid those threats. Section 7 describes the other related work. Section 8 describes the transformation of equations in secure electronic transactions to spatial circuits that could be used in hardware implementations. Section 9 describes algorithm to spatial circuit transformation. Section 10 briefs the e-voting project. Section 11 presents the plan for future work and summary.

II. SEQUENCE DIAGRAM AS A TEACHING TOOL

During the last decade postal mail became e-mail, libraries became digital, banking became online and commerce transformed to e-commerce. The major players of electronic cashless transactions are clients, internet service providers, the merchant's servers, the client's and merchant's banks, warehouses and delivery services. The purchase of an item from the internet can be represented as a transaction diagram as shown in Figure 1. In this diagram each link is numbered to represent the order of the progression of events and communications. Label 1 represents the client sending the message to an internet service provider. Label 2 represents the ISP sending the message to the merchant's web server, located in the internet. Label 3 denotes the merchant's web server communications with the e-commerce server. Label 4 shows the merchant's e-commerce server communications with the payment gateway and the database server. Label 5 depicts the payment gateway communications with the client's bank. Label 6 shows the payment gateway communications with the merchant's bank. Label 7 denotes the merchant's e-commerce server sending a message to the warehouse. Label 8 presents the warehouse sending the items to the delivery service. Label 9 shows the delivery service sending the items to the client.

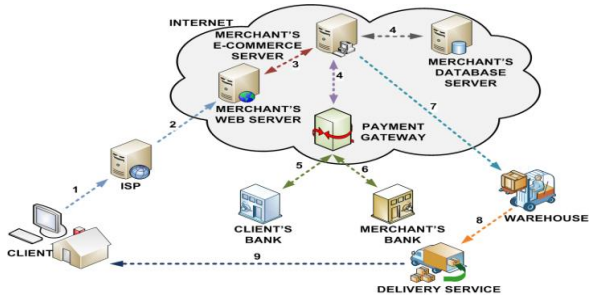

Figure 1. E-Transaction

Figure 2 illustrates the sequence diagram for the transaction described above [8,9]. The sequence diagram illustrates the sequence of events taking place in the transaction. In this diagram, entities are represented in the horizontal axis from left to right and the particular time slot of the event taking place is shown in the vertical axis progressing from bottom to top. The client first sends payment and order information to the merchant's server via his or her internet service provider. Then the merchant's server sends payment information to the client's bank. The client's bank then sends payment to the 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 the ISP. The merchant's server sends the order issue request to the warehouse. The warehouse issues goods for delivery. The delivery service delivers the goods to the client.

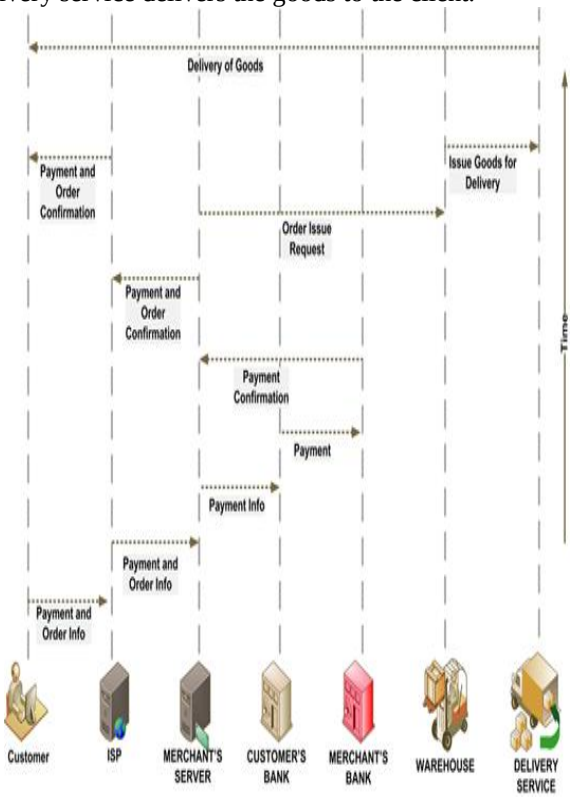

Figure 2. Sequence Diagram for the Transcation

III. Otway –Rees Proctol and Symbolic Representation

Figure 3 depicts the symbolic representation of Otway-Rees Protocol [10]. The Otway-Rees protocol is a server based protocol that provides authenticated key transport without requiring timestamp. The server S shares the keys KAS and KBS with users A and B respectively. It generates the session key KAB to share with users A and B. M is the session identifier which is chosen by user A. NA and NB are nonces chosen by users A and B respectively. Authentication is the validation provided by the communicating entity's identity as the one that it claims to be. It helps properly identify the user.

The validation is provided by an authentication factor which is used to authenticate the communicating person's identity. Confidentiality, integrity and authentication are achieved through encryption of the message. Authentication is implemented through encryption, signatures and certificates. The consequence of the misrepresentation of a user can be impersonation and forgery. 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.

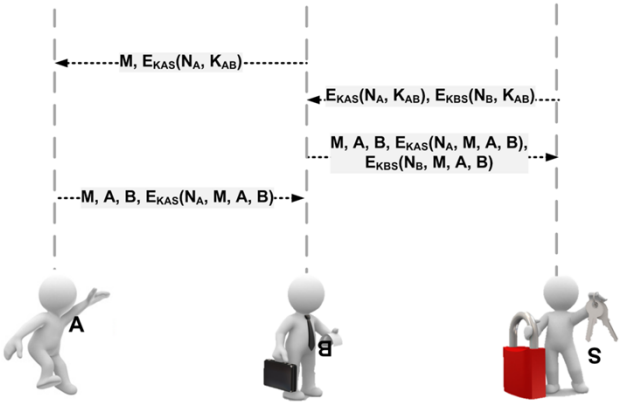

Figure 3. Symbolic Representation of Otway-Rees Protocol

IV. Analogy between Social and E Systems

Often e-systems are analogous to social counterparts. The Kerberos [11] ticket generation resembles social systems such as an airline system where a user purchases a ticket to receive the service. Figure 4 illustrates an online airline ticket purchase. The Kerberos authentication consists of a client, an Authentication Server, Ticket Granting Service and a service provider. It is secure and scalable to support a large number of clients and servers. Kerberos communications are represented using a sequence diagram as shown in Figure 5. Encrypted keys and tickets help sharing symmetric keys.

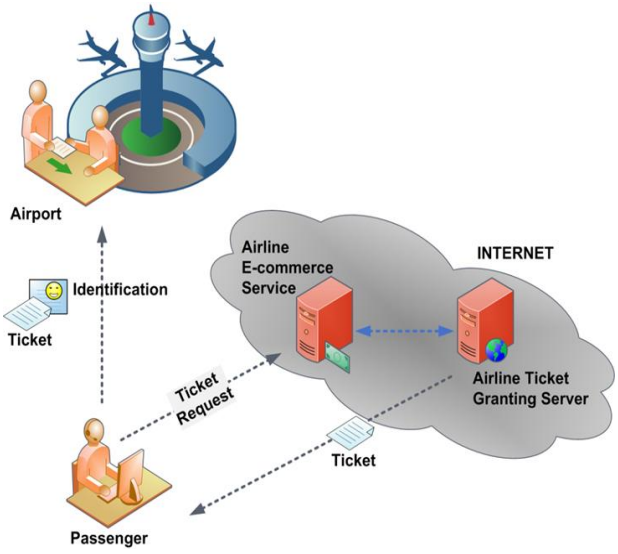

Figure 4. Airline Ticketing

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.

Non-repudiation ensures the 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 buying 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 the information.

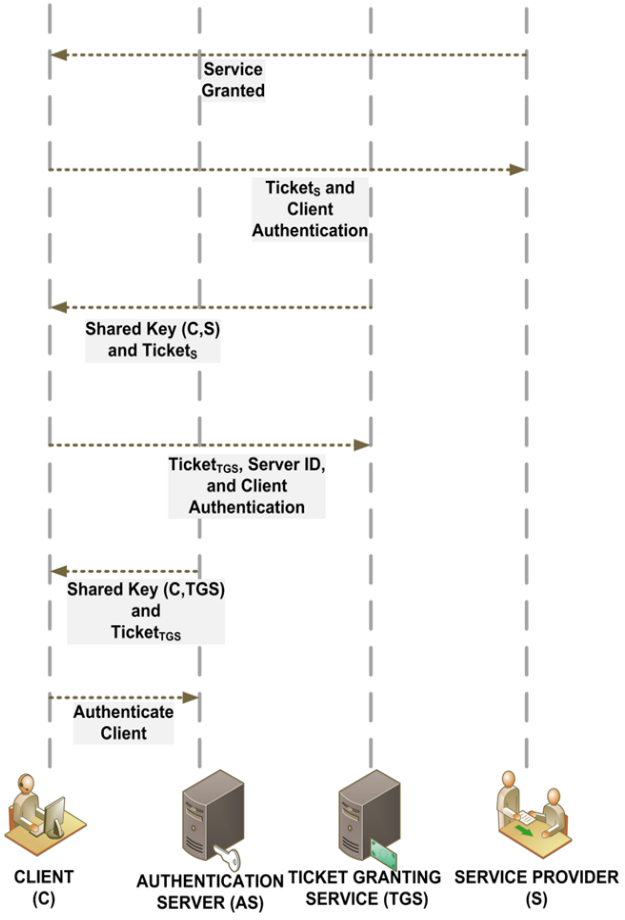

Figure 5. Kerberos Authentication

Availability ensures that the system responses promptly and the service and the information is available when needed to authorize persons. Flooding a server 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. 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. This authenticates that the signed message has not been tampered with by any unauthorized party. The blind signature scheme based on RSA digital signature and its application for online electronic cash system is proposed by Chaum.

Thereafter, Okamoto [5] developed a divisible electronic cash system and others further improved it.

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.

V. Attacks on E Systems

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 [12, 13]. Particularly, E-cashless transactions involve the 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 via the internet. Much of the communication, billing and payments are done by electronic message transfers. There is a higher possibility of stealing, losing, modifying, fabricating or repudiating information. Such systems and messages transmitted need extra protection from eavesdroppers. Many threats such as denial of service, distributed denial of service, 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 the data. Sniffing can take place at vulnerable points such as the ISP, the merchant's server, the client's bank, the merchant's bank or at the internet backbone. Figure 6 also depicts an insecure e-commerce transaction. In this transaction anyone can read or modify the payment and order information. An intruder can interrupt, modify or initiate the transaction. The client's bank information can be stolen by a third party.

Figure 7 illustrates the sequence diagram of another attack. Here, in message 1 an attacker introduces malicious scripts into a legitimate web server to steal sensitive information from users who access the page.

The website stores comments without checking the content. When a victim visits that website, message 2, the malicious script will execute on the victim's browser, messages 3 and 4, and the attacker can steal information from the victim, message 5. In addition, the attacker can also take over the session as illustrated in messages 6 and 7. Such attacks occur due to the poor security.

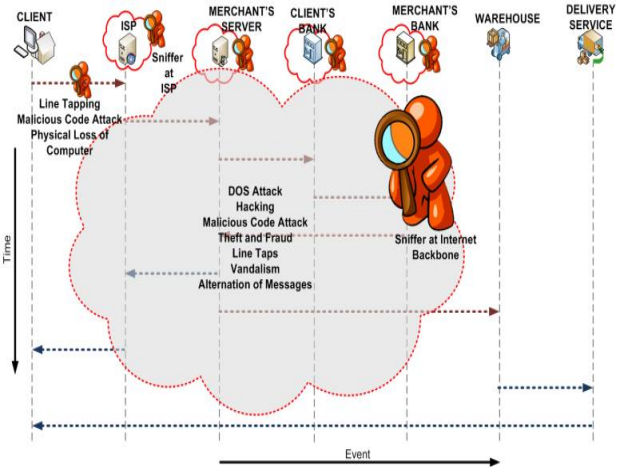

Figure 6. Attacks on E-Systems

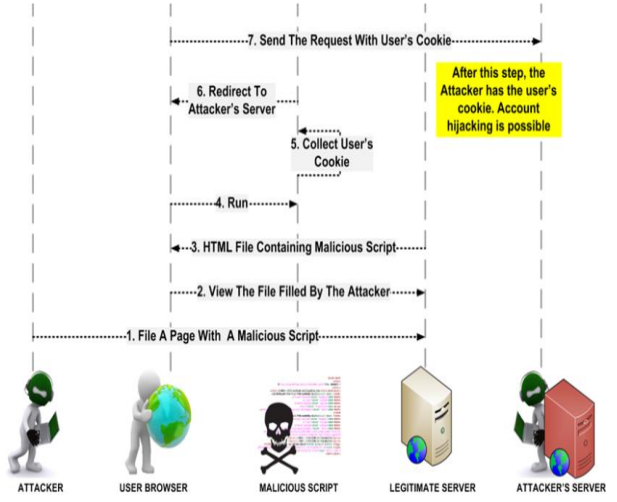

Figure 7. Cross-site Scripting

VI. Consolidation of Integrity, Confidentiality and Authenticity in Applications

Providing confidentiality is vital in secure systems. Figure 8 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 from having 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 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.

Confidentiality guarantees privacy, no loss of information from client or the server. Integrity assures no modifications of data, messages or impersonation. 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.

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 Keccak, the new SHA-3 [4] for this purpose. is the SHA-3. is announced by the National Institute of Standards and Technology and the National Security Agency selected Keccak from five new Hash functions [14], BLAKE, Skein [15], Groestel [16], JH and Keccak. Grooestel is similar to AES. MD5 produces the digest of 128 bits whereas the broken SHA-1 produces a 160-bit message digest.

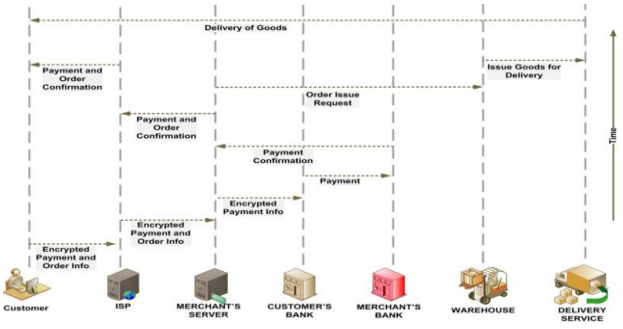

Figure 8. E-Transaction with Confidentiality

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.

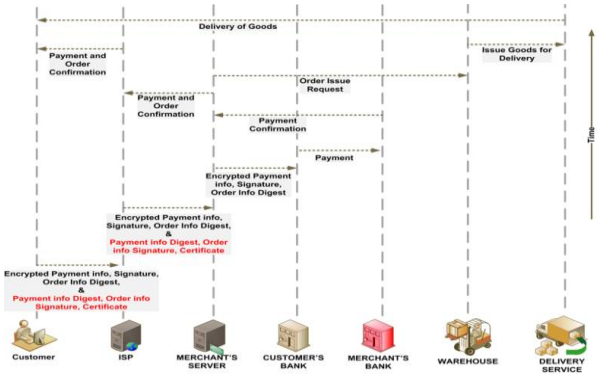

Figure 9. Secure Transaction

The Figure 9 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. 10 represents the transaction with symbols.

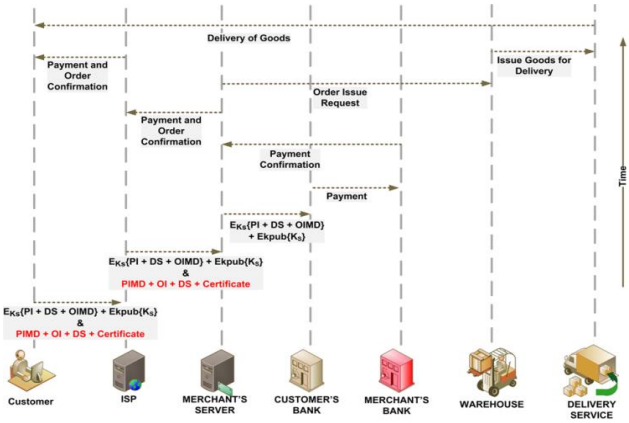

Figure 10. Symbolic Representation of Secure Transaction

In Figures 10, 11 and 12
PI = Payment Information
DS = Dual Signature
OIMD = OI message digest
POMD = Payment order message digest
Ks = Temporary symmetric key
PIMD = PI message digest
OI = Order Information
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.
Certificate = Cardholder Certificate.
|| = Concatenation
KpriC = Customer's private signature key

VII. 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 [17,18]. 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. 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.

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.

VIII. Symbolic Representations to Spatial Circuits

The equation in Figure 10

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

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 cipher text. A spatial circuit can be easily drawn from this representation as shown in the Figure 11:

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 [18]. The merchant can only see the OI and the bank can only access PI. Figure 11 shows how the order information and payment information is securely delivered to the two recipients – merchant and bank using Dual Signature, DS.

Figure 12 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.

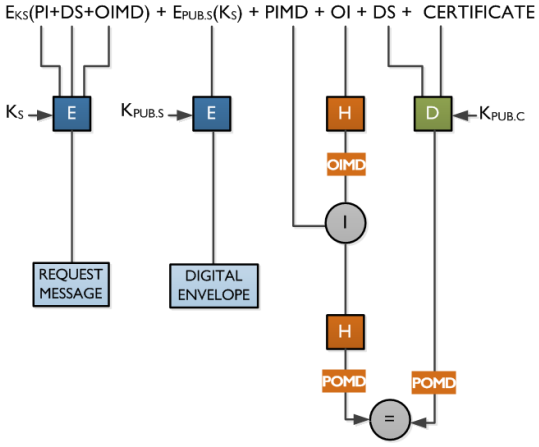

Figure 11. Cardholder Sends Purchase Request Merchant Veifies

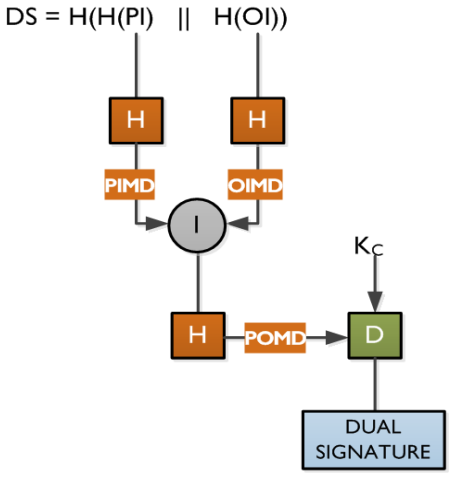

Figure 12. Construction of Dual Signaturees in SET

IX. Algorithms to Spatial Circuits Transformation

Algorithm to hardware transformation is an important concept to introduce in security courses. Encryption and decryption algorithms can be easily transformed into spatial circuits. 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 13 shows the *for* loop and the final round of the Blow Fish [19] 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

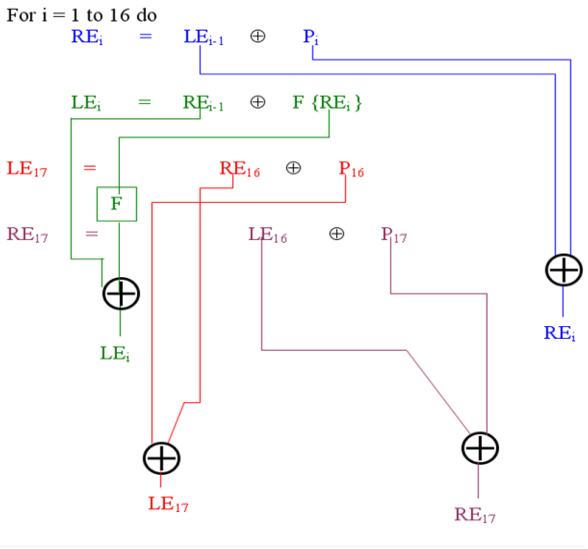

Figure 13. Algorithm to Spatial Circuit – BlowFish Encryption

X. ELECTRONIC –VOTING PROTOCOL

In electronic voting, the internet is used for casting a vote and counting votes. When teaching information assurance it is interesting to introduce various Internet-based electronic voting protocols to students and discuss their practicality. These protocols incorporate cryptographic techniques to satisfy a set of requirements to ensure security of the voting procedure and privacy of the voter. At the end of the semester, a web-based e-voting system is developed with added features such as identifying system defects, fraud committed with respect to specific properties of the system.

To get started we present DeMillo and Merritt's protocol [7]. We consider a voting scenario where voters V1, V2, V3 and V4 have to vote *yes* or *no*. Each voter has access to two public key encryption functions E and R. E is a regular public key encryption function whereas R embeds the message in a random string and then encrypts the result. R encryption provides secrecy and identifiability. D and Q are the corresponding decryption functions. Each voter chooses a vote, v and computes

$$R_{v1}(R_{v2}(R_{v3}(R_{v4}\ (E_{v1}(E_{v2}(E_{v3}(E_{v4}\ (V))))))))$$

using the public encryptions. All the encrypted votes are sent to voter V1. V1 then removes the first level of encryption from all ballots:

$$Q_{v1}\ (R_{v1}(R_{v2}(R_{v3}(R_{v4}\ (E_{v1}(E_{v2}(E_{v3}(E_{v4}\ (V)))))))))$$
$$= R_{v2}(R_{v3}(R_{v4}\ (E_{v1}(E_{v2}(E_{v3}(E_{v4}\ (V))))))))$$

Now, A forwards the ballots in a random order to voter V2, who checks for his ballot and decrypts one level, producing

$$Q_{v2}(R_{v2}(R_{v3}(R_{v4}\ (E_{v1}(E_{v2}(E_{v3}(E_{v4}\ (V)))))))))$$
$$= R_{v3}(R_{v4}\ (E_{v1}(E_{v2}(E_{v3}(E_{v4}\ (V))))))$$

The voter V2 sends this result to V3. Similarly, the voter V3 removes the third level of encryption and sends the ballots to V4. The voter V4 removes his level of encryption, signs and broadcasts all the votes to voters V1, V2 and V3.

The voter V1 removes one more level of encryption, checks to verify that his vote is still in the set, broadcasts the ballots to V2, V3 and V4. The voter V2 receives ballots from V1, which he decrypts and broadcasts to V1, V3 and V4. Similarly, the voter V3 removes E_{v3} and broadcasts to V1, V2 and V4. The voter V4 removes E_{v4} and broadcasts the results to V1, V2 and V3. Figure 14 shows the steps involved in the DeMillo and Merritt protocol for four voters.

Figure 15 shows the steps involved in the Mu and Vardharajan's first Secure Anonymous Voting scheme [6]. The minimum set of agents required for the environment of this system include Voters (*V*), a Trusted Certificate Authority (*CA*), an Authentication Server (*AS*) which authenticates each *V* and issues Voting Tickets, Voting Servers (*VS*) which collect Voting Tickets from each *V* and a Ticket Counting Server (*TCS*).

A voter sends message A to certificate authority CA. The CA sends voting certificate to the voter V using message B. To obtain a valid voting ticket the voter sends message C to trusted Authentication Server *AS*. The AS sends the voting ticket via message D. The voter sends his vote to Voting Server via message E. After collecting all votes the Voting Server will send to Ticket Counting Server TCS. The TCS counts all the votes and checks for double voting. The TCS sends message G to AS if it detects double voting. After receiving message G the AS identifies the identity of the voter.

As the anonymity of voters is the primary requirement of this protocol, *AS* should not have any information on the voting tickets and other parameters which could be used in further phases of voting. This is achieved using blind signatures. The public key encryption and digital signatures are based on the RSA algorithm. To maintain the credibility of voters, electronic voting uses blind signatures. This prevents from same person voting twice.

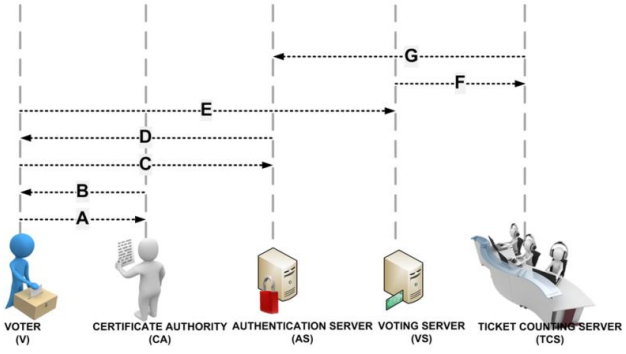

Figure 14. DeMillo and Merritt's protocol

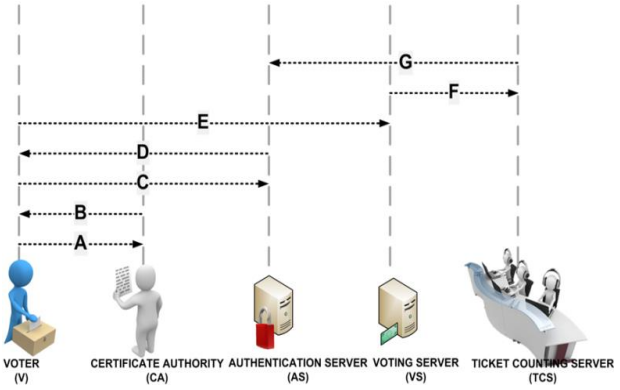

Figure 15. Mu and Vardharajan's Secure Anonymous Voting Protocol

XI. Assessment and Evaluation of Student Outcomes

Student progress towards attaining each Student Outcome described in section 1 of this paper is measured in stages. For each stage, students complete a pre-defined set of activities in the course. Data collection processes to assess and evaluate each student outcome include exam questions, group activities, project presentations, focus groups, industrial advisory committee meetings, and other processes that are relevant and appropriate to the program. Student performance is evaluated in the course by the assessment data collection, data analysis, review and recommendations, and course outcomes. Student and Exit surveys are also used to collect data. Data collection processes for each outcome include quizzes, tests, final exams, homework, lab reports, oral presentations, and project work. The undergraduate committee and the program Chair analyze the data. The program faculty make recommendations thereafter. The undergraduate committee approves the recommendations. The program faculty and the Chair implement those recommendations. The faculty retreat and department meeting times are used to discuss these changes.

XII. Conclusion

This paper described a task based active learning module developed to help students understand secure protocols, algorithms and modeling web applications to prevent attacks. It presented UML sequence diagrams and mathematical representations used in security. It also described the transformation of cryptographic algorithms to spatial circuits. It also provided examples related to confidentiality and integrity and their combinations. The active learning modules developed were easily adapted and effectively used in a classroom with senior undergraduate or graduate students in computing, engineering IT and businesses. These modules helped to teach other symmetric key algorithms. Both reading and interpreting equations are important in e-Commerce and Security classes. We continuously improve the student outcomes while collecting assessment data, evaluating them and taking actions.

References

[1] http://csrc.nist.gov/publications/fips/fips197/fips -197.pdf ES Announcement, last accessed April 6, 2013

[2] R.L.Rivest, A. Shamir; L. Adleman "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 1978.

[3] http://csrc.nist.gov/groups/ST/hash/sha-3/winner_sha-3.html last accessed April, 6, 2013

[4] D. Chaum., "Blind signature for untraceable payments", Advances in Cryptology – Crypto - 82, Springer Verlag, p.p. 199-203

[5] T. Okamoto,. "An Efficient Divisible Electronic Cash Scheme", Third IEEE Symposium on Computers & Communications. Jun 1998.

[6] DeMillo, R.; and M. Merritt, Protocols for Data Security, IEEE Computer, Feb. 1983

[7] Mu Y., Varadharajan V., "Anonymous Secure E-Voting Over a Network," 14th Annual Computer Security Applications Conference, 1998

[8] 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, Dubai May 2011

[9] Y. Albastaki, A. Herath, "Secure Digital Cashless Transactions with Sequence Diagrams and Spatial Circuits to Enhance theInformation Assurance and Security Education", International Journal of Advanced Computer Science and Applications,Vol. 3, No.4, 2012.

[10] D.Otway, O.Rees,"Efficient and timely mutual authentication". Operating Systems Review, 1987, 21 8 - 10.

[11] Neuman B. C.; T'so T. Y., "Kerberos: An Authentication Service for Computer Networks", IEEE Communications Magazine, September, 1994.

[12] W.Stallings, "Cryptography and Network Security Principles and Practice" , Prentice Hall, 2012

[13] J. Wu, D. Irwin, "Computer Networks and Cybersecurity", CRC Press, 2013

[14] http://csrc.nist.gov/groups/ST/hash/sha-3/index.html NIST's SHA-3 Contest: last accessed April, 6, 2013

[15] F. Niels, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T.Kohno, J.Callas,at.el . "The Skein Hash Function Family", http://www.skeinhash.info/sites/default/files /skein1.1.pdf

[16] P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechbergeret al. "Grøstl – a SHA-3 candidate" http://www.groestl.info/Groestl.pdf

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

[18] B. Giampaolo; Massacci, F;. and Paulson, L. "Verifying the SET Registration Protocols." Proceedings of IEEE Journal of Selected Areas inCommunications 2003.http://www.cl.cam.ac.uk/~lp15/papers/Bella/registration.pdf, last accessed April, 6, 2013

[19] https://www.schneier.com/paper-blowfish-fse.html last accessed April, 6, 2013