MIS Review Vol. 20, No. 1, September (2014), pp. 59-71
DOI: 10.6131/MISR.2014.2001.04
© 2014 Department of Management Information Systems, College of Commerce
National Chengchi University & Airiti Press Inc.

airiti

Securing E-Commerce Business Using Hybrid Combination Based on New Symmetric Key and RSA Algorithm

Prakash Kuppuswamy[1], Saeed Q. Y. Al-Khalidi[2]
[1]*Department of Computer Engineering and Networks, Jazan University, KSA*
[2]*Deanship of Libraries Affairs, King Khalid University, KSA*

ABSTRACT: *Security in e-commerce is becoming more topical as the shift from traditional shopping and transactions move away from physical stores to online. E-commerce has had a drastic effect on the global economy and has rapidly accelerated over the years into the trillions of dollars a year. Protecting payment web application users and application systems requires a combination of managerial, technical and physical controls. In this paper, we propose hybrid cryptographic system that combines both the symmetric key algorithm, and popular RSA algorithm. The symmetric key algorithm based on integer numbers and RSA algorithm widely using in all data security application. Efficiency of the security methods are dignified and such competence increases as we combined security methods with each other.*

KEYWORDS: *E-Commerce, Hybrid Security, RSA Algorithm, Simple Symmetric Key*

1. Introduction

Electronic commerce is buying and selling of goods and services across the internet. Commercial activities over the internet have been growing in an exponential manner over the last few years. When it comes to payment, one needs to establish a sense of security. Customers must be able to select a mode of payment and the software must verify their ability to pay. This can involve credit cards, electronic cash, encryption, and/or purchase orders. The more of these techniques are supported by an E-commerce package, the more secure the system can be, and therefore the more customers are benefits from E-commerce abilities (Al-Slamy, 2008; Greenberg, 2001; Olkowski, 2001).

Security issues are an important topic in e-commerce. How to protect the security of an e-commerce system and data is its core research area (Davis, 2003). There are many sensitive financial data and asset data in e-commerce databases, such as transaction records, commercial transactions, user account and market scheme and so on. The data are very important to the parties involved in e-commerce, so we must assure their security completely (Hou, 2009).

At present the security technologies used in e-commerce databases are Web access control, user authentication, authorization control, safety audit, backup and recovery,

airiti

data encryption and so on. These technologies can assure general database security, but it is difficult to assure their security for important databases. Encryption technology is one of the most effective technologies of database security. However a simple encryption technology, such as symmetrical encryption or asymmetrical encryption, is very difficult to guarantee the security of network databases. We must combine the both and through hybrid encryption we can create a safe, efficient e-commerce database system (Hou, 2009).

Secure communication is an intrinsic requirement for many popular online transactions such as e-commerce, stock trading and e-banking. E-commerce and m-commerce transactions are growing at an explosive rate. The success of these depends on how transactions are carried out in the most secured manner. The prime requirements for any e-commerce and m-commerce transactions are Privacy, Authentication, Integrity maintenance and Non-Repudiation. Cryptography helps us in achieving these prime requirements. Today, various cryptographic algorithms have been developed. These are broadly classified as symmetric key (Rasmi & Paul, 2011).

A hybrid cryptosystem is a protocol using multiple ciphers of different types together, each to its best advantage. One common approach is to generate a random secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient's public key (Rasmi & Paul, 2011).

The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient. The recipient decrypts the secret key first, using his/her own private key, and then uses that key to decrypt the message (Janakiraman, Ganesan & Gobi, 2007).

It is clear that electronic commerce will revolutionize businesses, and customers will be offered new and exciting services. As E-commerce businesses are growing, more secure technologies are being developed and improved every day. The current internet security polices and technologies fail to meet the needs of end users. The success or failure of an E-commerce operations hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Any business that wants to have a competitive edge in today's global marketplace should adopt a comprehensive security policy in consultation with partners, suppliers, and distributors that will provide safe environment for the coming proliferation of E-commerce (Chaffey, 2004; Greenberg, 2001). In Figure 1 shows the features of E-commerce security and Figure 2 shows the simple architecture of E-commerce system.

airiti

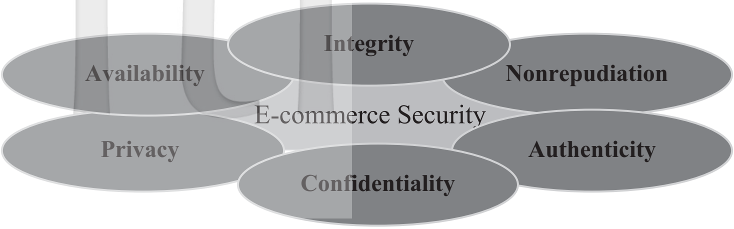

Figure 1 Dimension of E-Commerce Security

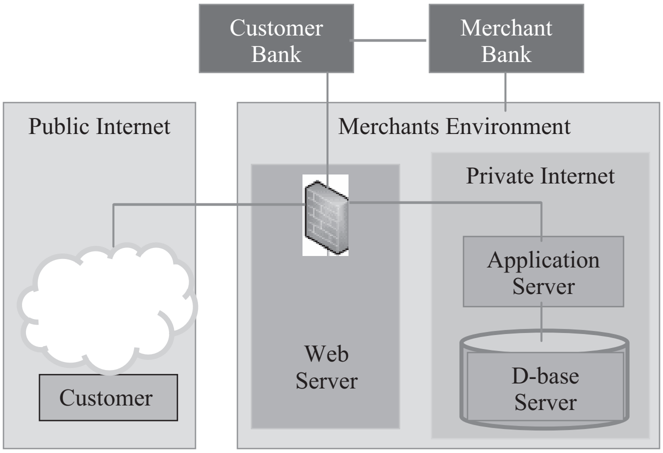

Figure 2 Simple E-Commerce Structure

2. Literature review

Kherad et al. (2010), in this research they proposed a new self-developed symmetric algorithm called FJ RC-4, which is derived from RC4. They investigated and compared the robustness of the RC4 and FJ-RC4 and shown that FJ-RC4 is stronger than RC4 against the attacks. In addition, it takes more time to find key in FJ-RC4 and requires more resources (Kherad et al., 2010).

Rasmi and Paul (2011), the circle symmetric key algorithm is based on 2-d geometry using property of circle, and circle-centered angle. It is a block cipher technique but has the advantage of producing fixed size encrypted messages all cases. The asymmetric algorithm is RSA with CRT which improves the performance of the basic RSA algorithm by four (Rasmi & Paul, 2011).

Palanisamy and Jeneba Mary (2011), the Rijndael algorithm mainly consists of a symmetric block cipher that can process data blocks of 128, 192 or 256 bits by using key lengths of 128, 196 and 256 bits. This work also generating two pairs of keys; public

airiti

and private key. Using Public key it encrypts the data key and other one is public and private key pair, which will send to other person, so that opposite person can decrypt the encrypted key using his public and private key (Palanisamy & Jeneba Mary, 2011)

Kuppuswamy and Al-Khalidi (2012), proposed new symmetric key algorithm based on integer and modular 37 and select any number and calculate inverse of the selected integer using modular 37. The symmetric key distribution should be done in the secured manner. This study's main goal is to reflect the importance of security in network and provide the better encryption technique for currently implemented encryption techniques in simple and powerful method (Kuppuswamy & Al-Khalidi, 2012).

Yasin, Haseeb and Qureshi (2012), they suggested E-commerce has presented a new way of doing transactions all over the world using internet. Organizations have changed their way of doing business from a traditional approach to embrace E-commerce processes. The purpose of this paper is to explain the importance of E-commerce security digital signature and certificate based cryptography techniques in E-commerce security (Yasin et al., 2012).

Nanehkaran (2013), electronic commerce is supporting of customers, supplying of services and commodities, portion of business information, manages business transactions and maintaining of bond between suppliers, customers and vendors by devices of telecommunication networks. In this research article paper is to review of principles, definitions, history, frameworks, steps, models, advantages, barriers and limitations of electronic commerce (Nanehkaran, 2013).

3. Problem statement

Over the years, the methods used by ecommerce or web commerce sites to process and store credit card/master card information has become much more sophisticated than the early days of online shopping business. This progress has helped online business overcome one of its greatest obstacles, customer faith. As showed by the amount of money transaction online every year, people feel much more secure in online shopping than they ever have. Regrettably for businesses, the methods used by cyber criminals trying to steal their customer's information have made it easier than ever for them to compromise a web application.

Security threats to web sites and web applications come in many ways. Data centres and other resources used for hosting web sites and their associated systems need to be protected from all type of vulnerable activity. Threats should be identified using application threat modeling and then evaluated with a vulnerability assessment. Susceptibilities can be removed or reduced and counter measures put in place to mitigate the effects of an incident should the threat be realized.

airiti

Figure 3 shows money spending for information/data security between 2009 and 2013. In the year of 2011 and 2012, 2.6 million US$ only spend for information security, but, in the year of 2013 spend more than 4 million dollar, It is the huge margin comparing to the previous years.

4. Proposed hybrid algorithm

4.1 Simple symmetric key algorithm

Symmetric key is implemented in two ways either as a block cipher or stream cipher. Block cipher transforms a fixed length block of plaintext say a fixed size of 64 data into a block of ciphertext (encrypted text) data of the same length. We know that, whatever user ID consist of Alphabets between A to Z and numbers which is between 0 ~ 9. Here, in New symmetric key algorithm, we introduce synthetic data, which is based on the user ID. Normally the synthetic data value consists of equivalent value of alphabets and numbers. Alphabet value A is assigned as integer number 1 and B = 2 ... so on. Next we consider integer value 0 assigned as 27 and 1 = 28 ... 9 = 36 also the space value considers as an integer number 37.

4.1.1 Key generation method

(1) Select any natural number say as n.

(2) Find the inverse of the number using modulo 37 (key 1) say k.

(3) Again select any negative number (for making secured key) n1.

(4) Find the inverse of negative number using modulo 37 (key 2) k1.

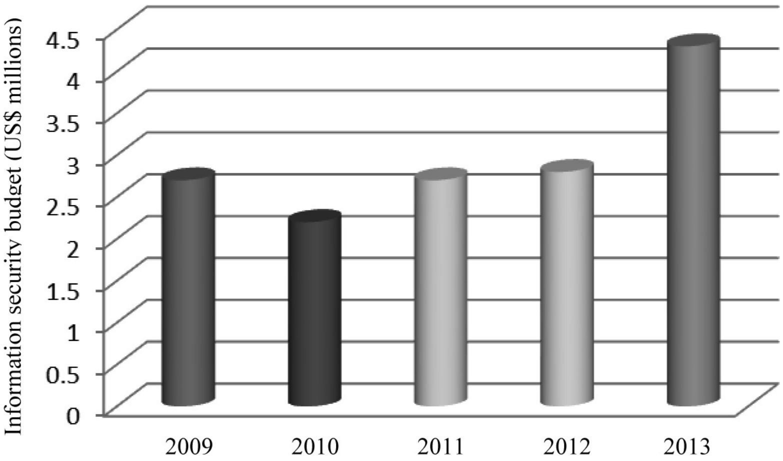

Figure 3 Budget Used for Information Security

Source: The Global Information Security Survey 2014.

airiti

4.1.2 Encryption method

(1) Assign synthetic value for user ID.

(2) Multiply synthetic value with random selected natural number.

(3) Calculate with modulo 37.

(4) Again select random negative number and multiply with it.

(5) Again calculate with modulo 37 $CT = (PT \times n \times n1) \bmod 37$.

4.1.3 Decryption method

(1) Multiply received text with key 1 & key 2.

(2) Calculate with modulo 37.

(3) Remainder is Revealed Text or Plain Text $PT = (CT \times n^{-1} \times n1^{-1}) \bmod 1$.

4.2 RSA asymmetric key algorithm

The RSA algorithm is based on the assumption that integer factorization is a difficult problem. This means that given a large value n, it is difficult to find the prime factors that make up n. It is most popular asymmetric key algorithm.

4.2.1 Key generation

(1) Choose two very large random prime integers p and q.

(2) Compute n and $\varphi(n)$: $n = pq$ and $\varphi(n) = (p-1)(q-1)$.

(3) Choose an integer e, $1 < e < \varphi(n)$ such that: $\gcd(e, \varphi(n)) = 1$(where gcd means greatest common denominator).

(4) Compute d, $1 < d < \varphi(n)$ such that: $ed \equiv 1 \pmod{\varphi(n)}$, the public key is (n, e) and the private key is (n, d).

The values of p, q and $\varphi(n)$ are private; e is the public or encryption exponent; d is the private or decryption exponent.

4.2.2 Encryption

ciphertext $CT = M^e \pmod{n}$.

4.2.3 Decryption

Message M = $CT^d \pmod{n}$.

airiti

5. Proposed hybrid architecture

The following hybrid architecture design using, symmetric cipher and familiar RSA public key algorithm. It is basis of the protocol that enables to provide security while accomplishing an important system or network security. A protocol is an agreed-on hierarchical sequence of actions that leads to desirable results. Both the encrypted secret key and the encrypted message are then sent to the Merchant. The recipient decrypts the private key first, using his own private secret key, and then uses that secret key to decrypt the message. Figure 4 shows the block diagram of a hybrid crypto system which takes the advantages of both shared secret and public key algorithms. That means it combines both the symmetric key algorithm and asymmetric-key algorithm to take the advantage of the higher speed of symmetric ciphers and the ability of asymmetric ciphers to securely exchange keys.

6. Implementation with sample message

Our E-commerce implementation test measures efficient of implementing E-commerce on real time application. Ecommerce security is responsible for identifying

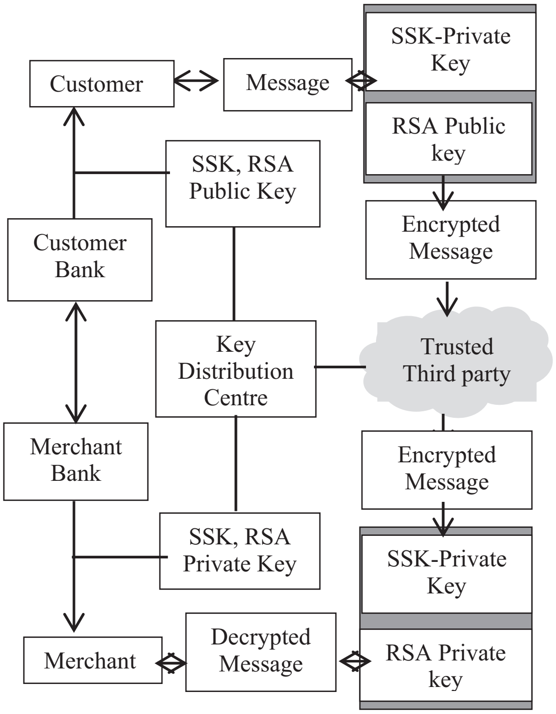

Figure 4 Proposed E-Commerce Architecture

airiti

network security threats, coordinating threat response, secure payment transaction. It will be responsible for business transaction between customer and merchant using external networks. In this implementation process the sample message “PRODUCT” mentioned in the Table 1 has taken for the experiment.

Table 1 Sample Message

P	R	O	D	U	C	T
16	18	15	4	21	3	20

6.1 SSK key generation

(1) We are selecting random integer number n = 3.

(2) Then inverse of 3 = 25 (verification 3 × 25 mod 37 = 1). So, Key 1 = 25.

(3) Again we are selecting random negative number n1 = -8.

(4) Then inverse of -8 = 23 (verify -8 × 23 = -184 mod 37 = 1). So, Key 2 = 23.

Encryption using SSK shows in the Table 2.

Table 2 Symmetric Key Encryption

Plain Text	Integer Value	CT = (M × n) mod 37 (n = 3)	CT = (CT × n1) mod 37 (n = -8)	Cipher Text
P	16	11	23	W
R	18	17	12	L
O	15	8	10	J
D	4	12	15	O
U	21	26	14	N
C	3	9	2	B
T	20	23	1	A

6.2 RSA key generation

Encryption using RSA.

We choosing here.

P = 7; q = 13; Therefore n = 91 Øn = 72.

airiti

Selecting e = 5 then inverse of e or d = 29 (verification 5 × 29 mod 72 = 1).

Public key is e, n = 5, 91.

Private key "d" = 27.

6.3 RSA encryption

Now we receive the cipher text message from above table "WLJONBA" i.e., equivalent integer value 23, 12,10, 15, 14, 2, 1. The encryption process of RSA algorithm mentioned in Table 3.

$(m)^e$ mod n i.e., $(2)^7$ mod 33 = 29.

Table 3 RSA Encryption Using Public Key

W	23	$(23)^5$ mod 91 =	4
L	12	$(12)^5$ mod 91 =	38
J	10	$(10)^5$ mod 91 =	82
O	15	$(15)^5$ mod 91 =	71
N	14	$(14)^5$ mod 91 =	14
B	2	$(2)^5$ mod 91 =	31
A	1	$(1)^5$ mod 91 =	1

6.4 Decryption using RSA & SSK

The decryption process of RSA algorithm and symmetric key algorithm mentioned in Table 4 and Table 5 respectively.

$(m)^d$ mod n

Table 4 RSA Decryption Using Private Key

4	$(4)^{29}$ mod 91 =	23	W
38	$(38)^{29}$ mod 91 =	12	L
82	$(82)^{29}$ mod 91 =	10	J
71	$(71)^{29}$ mod 91 =	15	O
14	$(14)^{29}$ mod 91 =	14	N
31	$(31)^{29}$ mod 91 =	2	B
1	$(1)^{29}$ mod 91 =	1	A

airiti

Table 5 Symmetric Key Decryption Using Private Key

Cipher Text	Integer Value	PT = (M × k1 × k2) mod 37	Plain Text
W	23	16	P
L	12	18	R
J	10	15	O
O	15	4	D
N	14	21	U
B	2	3	C
A	1	20	T

7. Result analysis

Here we have encrypted customer message “PRODUCT” into numbers using private and RSA public key and hence decrypted the keys to obtain the final character and the final message. Here we analyzed with existing DES, 3DES and AES algorithm to find out our new hybrid combination performance. The algorithm executes on PC computer of CPU Intel Pentium 4, 2.2 MHz Dual Core. The programs implemented using MATLAB and messages are stored in 3 different arrays for Key generation, Encryption and Decryption scheme. It is tested with the length of 100 bits.

Here we are examining two types of facts for consideration of performance. First one is computational performance and second one is communication performance. Computational performance refers to the speed of computation required to perform cryptographic operations. Communication performance indicates the total security required for transmission of data between two parties.

DES is the old “data encryption standard” from the seventies. Its key size is too short for proper security. 3DES is believed to be secure up to at least “2^{112}” security. But it is slow, especially in software. AES is the successor of DES, and it accepts keys of 128, 192 or 256 bits. Our proposed Hybrid combination of algorithm based on Simple symmetric key and RSA algorithm, which has been using in many application. The key size of RSA algorithm is standard and compatible for all application also encryption/decryption time of the Hybrid is less than comparing to the other algorithms. It is more secure than others using by the combination of two different algorithm. Table 6 and Figure 5 show the performance of DES, 3-DES, AES and our proposed hybrid algorithm.

airiti

Table 6 Performance Comparison

Algorithm	Key Size	Encryption/Decryption Timing (100 bits)
DES	64 bits	10 Sec
3-DES	2^{112}	20 Sec
AES	256 bits	15 Sec
SSK+RSA	2,048	10 Sec

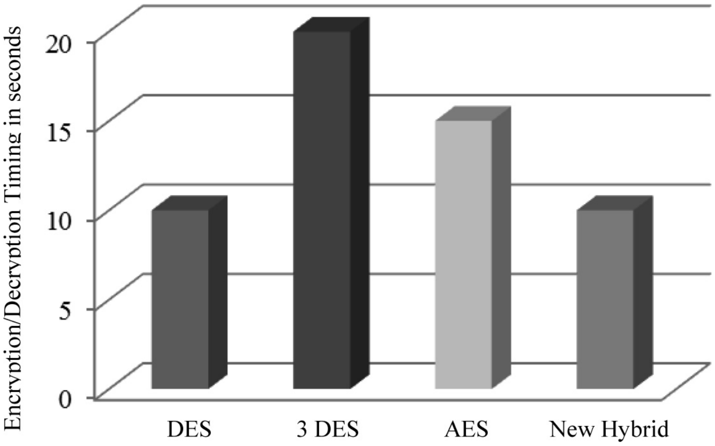

Figure 5 Performance Analysis of Various Algorithms

8. Conclusion

The proposed hybrid encryption algorithm used in this paper can also be used to enhance the security of other network. This work using simple symmetric key algorithm based and natural numbers and modular 37 cryptography used to data encryption/decryption and RSA cryptography asymmetric algorithm. On implementation of this combination of hybrid algorithm, we concluded several points. The encryption and decryption of any data has a secret or private key, which is used for data encryption. For this purpose asymmetric key or public key system is used. We introduced here the version of RSA which was resistant against security attack. Finally we illustrated the new directions for the future research.

References

Al-Slamy, N.M.A. (2008), 'E-commerce security', *International Journal of Computer Science and Network Security*, Vol. 8, No. 5, pp. 340-344.

airiti

Chaffey, D. (2004), *E-Business and E-Commerce Management*, 2nd ed., Prentice Hall, Harlow, UK.

Davis, Z. (2003), 'E-commerce', *Software World*, Vol. 30, pp. 207-212.

Greenberg, P.A. (2001), 'In E-commerce we trust … not', available at http://www.ecommercetimes.com (accessed 12 February 2014).

Hou, J. (2009), 'Research on database security of E-commerce based on hybrid encryption', *Proceedings of the 2009 International Symposium on Web Information Systems and Applications*, Nanchang, China, pp. 363-366.

Janakiraman, V.S., Ganesan, R. and Gobi, M. (2007), 'Hybrid cryptographic algorithm for robust network security', *ICGST-CNIR*, Vol. 7, No. I, pp. 1141-1146.

Kherad, F.J., Naji, H.R., Malakooti, M.V. and Haghighat, P. (2010), 'A new symmetric cryptography algorithm to secure e-commerce transactions', *Proceedings of the International Conference of Financial Theory and Engineering*, Dubai, United Arab Emirates, pp. 234-237.

Kuppuswamy, P. and Al-Khalidi, S.Q.Y. (2012), 'Implementation of security through simple symmetric key algorithm based on Modulo 37', *Council for Innovative Research International Journal of Computers & Technology*, Vol. 3, No. 2, pp. 335-338.

Nanehkaran, Y.A. (2013), 'An introduction to electronic commerce', *International Journal of Scientific & Technology Research*, Vol. 2, No. 4, pp. 190-193.

Olkowski, D.J. (2001), 'Information security issues in E-commerce', available at http://www.sans.org/reading-room/whitepapers/ecommerce/information-security-issues-e-commerce-37 (accessed 10 March 2015).

Palanisamy, V. and Jeneba Mary, A. (2011), 'Hybrid cryptography by the implementation of RSA and AES', *International Journal of Current Research*, Vol. 33, No. 4, pp. 241-244.

Rasmi, P.S. and Paul, V. (2011), 'A hybrid crypto system based on a new circle-symmetric key algorithm and RSA with CRT asymmetric key algorithm for E-commerce applications', *Proceedings of International Conference on VLSI, Communication & Instrumentation*, Kerala, India, pp. 14-18.

Yasin, S., Haseeb, K. and Qureshi, R.J. (2012), 'Cryptography based E-commerce security: a review', *International Journal of Computer Science Issues*, Vol. 9, No. 2, pp. 132-137.

airiti

About the authors

Prakash Kuppuswamy, Lecturer, Department of Computer Engineering & Networks in Jazan University, KSA. He is research Scholar-Doctorate Degree yet to be awarded by Dravidian University. He has published 25 International Research journals/Technical papers and participated in many international Conferences in Maldives, Libya and Ethiopia. His research area includes Cryptography, Bio-informatics and E-commerce security etc. Corresponding author. College of Computer Science & Information system, Jazan University, KSA. Sathuvachary, Vellore, Tamil Nadu, India. Tel: +966 532883941. E-mail address: prakashcnet@gmail.com

Saeed Q. Y. Al-Khalidi, Dean, Deanship of Libraries Affairs at King Khalid University, Abha. KSA. He published many National & International papers, Journals. Also, he participated as a Reviewer in many international conferences worldwide. He completed Master Degree and Doctor of Philosophy in University of East Anglia. His research interests include: Information System development, approaches to systems analysis and the early stages of systems development process, IT/IS evaluation practices, E-readiness assessment. E-mail address: prakashcnet@gmail.com, salkhalidi@yahoo.com