Hybrid Algorithm for E-commerce Applications

Jothina Mazarire[1]

Medlog Zimbabwe Pvt Ltd,

27 Natal road Avondale, Harare

Clopas Kwenda[2]

Department of Accounting and Information Systems,

Great Zimbabwe University, Masvingo, Zimbabwe

ABSTRACT

Encryption is the processes of converting plaintext message (human readable form of message) to cipher text (scrambled form of message) while decryption is the reverse process of encryption. There are specialized algorithms used to handle the encryption/decryption process in e-commerce applications such as CRYPTON, DES, CAST and others. The chief algorithm used in the E-commerce applications for decoding and encoding large volumes of data is the RSA algorithm because of its level of security. Despite its use its major drawback is that of speed. The algorithm is slow in both encryption and decryption process and therefore could not cope up with large volumes of data. With that that problem in mind a hybrid algorithm was designed by harmonizing AES and RSA with the hope that the weaknesses of RSA will be offset by AES and vice versa.

Key words: Encryption, Decryption, RSA, AES

INTRODUCTION

Electronic Commerce usually referred to as e-commerce can be defined as a process of buying and selling of goods and services as well as business communication and transactions over computer networks and through individual computer linked to the World Wide Web(1). The most common form of E-Commerce technologies which has been used by banks is that of Electronic Funds transfer (EFT) which are electronic transmissions of account exchange information over private communication network and theElectronic data interchange (EDI) which is the exchange of data between computer systems by standardized message formatting, and the whole process is automated(2). Therefore e-commerce involves using the internet to conduct various forms of business. Business transactions involve sensitive data which should be kept secure while in transit between communication networks. Data encryption is part and parcel of the components of e-commerce and there are various encryption algorithms. Some of the algorithms used for the encryption and decryption data process include DES, CAST, IDEA and CRYPTON among others but the R.S.A algorithm is the most popular algorithm used by e-commerce applications for decryption

and encryption of blocks of data though it has got its own drawbacks of being slow and with the advancement of technology and people acquiring new knowledge it can now easily be attacked (1)(3).A Survey on Performance Analysis of DES, AESand RSA Algorithm carried out proved that RSA is slow in both encryption and decryption processes [10]. This is shown by the table below:

S.NO	*Algor*	*Pack Size (KB)*	*Encrypt Time (Sec)*	*Decrypt Time (Sec)*	*Buff Size*
1	DES	153	3.0	1	157
	AES		1.6	1.1	152
	RSA		7.3	4.9	222
2	DES	118	3.2	1.2	121
	AES		1.7	1.2	110
	RSA		10.0	5.0	188
3	DES	196	2.0	1.4	201
	AES		1.7	1.24	200
	RSA		8.5	5.9	257
4	DES	868	4.0	1.8	888
	AES		2.0	1.2	889
	RSA		8.2	5.1	934
5	DES	312	3.0	1.6	319
	AES		1.8	1.3	300
	RSA		7.8	5.1	416

Table 1 Encryption and Decryption times for RSA DES AES

Since Advanced Encryption Standard (AES) is a symmetric algorithm it implies that the key that is used to encrypt is also the same key that is used to decrypt. So if the attacker gets hold of the key he/she can simply decode the cipher text.
The motive behind this project paper is to build a hybrid algorithm that harmonizes R.S.A and A.E.S with assumption that the weaknesses of R.S.A will be offset by A.E.S and vice versa.

R.S.A algorithm

R.S.A named after Ron Rivest, Adi Shamir, and Leonard Adelman in 1978. This algorithm is based known as the asymmetric cryptosystem for key exchange. It is a block cipher system based on number theory (4). The concept behind the algorithm is that it uses very large prime numbers to generate the public and private keys which are then used for encryption and decryption processes. The algorithm is such that the sender encrypts the message using receiver public key and when then message gets to the receiver can then decrypt it using his or her private key(5)(6). R.S.A is based on 3 key operations that are key generation, encryption and decryption.

Key Generation Procedure (7)

a) Choose two distinct large random prime numbers p & q such that $p \neq q$.
b) Compute $n = p \times q$.
c) Calculate: phi (n) = (p-1) (q-1).
d) Choose an integer e such that 1<e<phi(n)

e) Compute d to satisfy the congruence relation d × e = 1 mod phi (n); d is kept as private key exponent.
f) The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

Encryption

Plaintext: P < n

Ciphertext: C= P^e mod n.

Decryption

Ciphertext: C

Plaintext: P=Cd mod n.

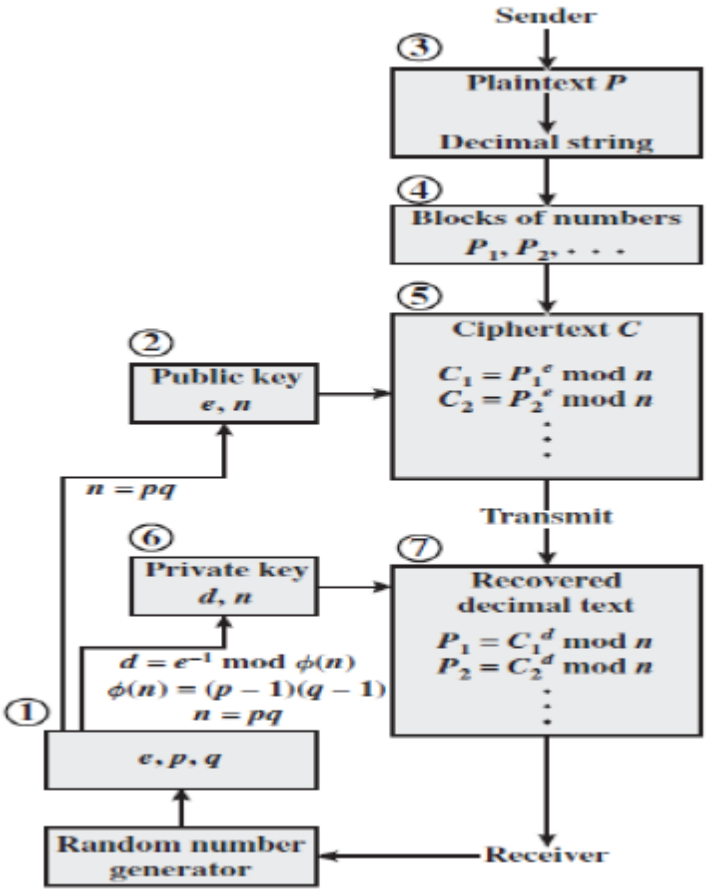

Figure 1 Workflow of RSA algorithm

D.E.S Algorithm

History of DES adapted from (2)

National Bureau of Standards (NBS) later renamed to National Institute of Standards and Technology or NIST recognize the need of general public for a secure cryptographic standard. This need emerged because existing US government cryptographic system that was in use at the time by agencies such as the department of defense, FBI, CIA, etc. were not meant for public use and because problems were beginning to arise with a proliferation of commercial encryption devices.

Not only were such commercial encryption devices were not compatible with each other but the algorithms upon which they relied on had not been extensively tested by independent reviewers. In 1972, the NBS requested proposals for a public cryptosystem. The criteria specified by the NBS for the system were that it be:

- Highly secure
- Easy to understand
- Publishable
- Available to all at no cost
- Adaptable to a diverse of applications
- Economical
- Efficient to use
- Able to be validated
- Suitable for export

In 1974, IBM proposed their Lucifer encryption systems which ultimately become the basis of the DES. Theproposed algorithm was tested privately by the National Security Agency (NSA) and by the general public. In1976, DES was adopted as the US standard for encrypting sensitive but unclassified data and for encryptedcommunication. The standard was later adopted by International Standards Organization (ISO) and becomewidely used by government and companies throughout the world

The D.E.S algorithm is the foundation that later gave birth to the A.E.S algorithm. Below is a detailed algorithm of D.E.S (5)(8)

1) 64 bit plain text is passed to the Initial Permutation (IP) function
2) The initial permutation is performed on the text
3) The IP produces two halves of permuted block: Each half will consist of 32 bit because initially input plain text was of 64 bit. The other will be called left plain text (LPT) while the other will be called right plain text(RPT)
4) Each LPT and RPT goes through 16 permutations orrounds of the encryption process, each with its own key.
a) From the 56 bit key, a different 48 bit sub-key isgenerated using Key Transformation
b) Using the expansion permutation, the RPT isexpanded from 32 bits to 48 bits
c) Now the 48 bit key is XORed with 48 bit RPT and theresulting output is passed on to the next step
d) Using the S- Box substitution this will produce the 32bit from 48 bit input
e) These 32 bit are permuted using the P- Boxpermutation
f) The P- Box outputs 32 bits are XORed with 32 bitLPT
g) The result of the XORed 32 bits becomes the RPT andold RPT becomes the LPT. This process is calledswapping
h) Now the RPT again given to the next round andperformed the 15 more rounds
5) After completion of 16 rounds the final permutation is performed

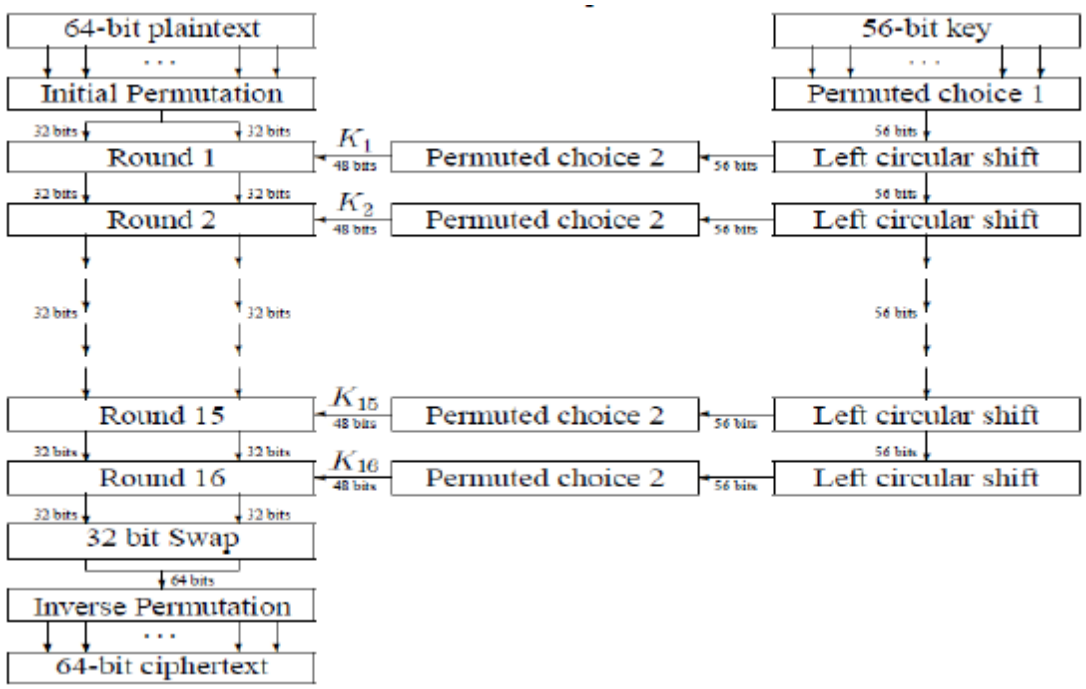

Figure 2 Workflow of DES algorithm

The initiative of choosing D.E.S for e-commerce purposes is strongly disagreed by DrSoper who outlined the following weaknesses of DES(9):

D.E.S uses a fixed key length [56 bits] and this implies that it has got 2^{56} total possible keys which is approximately 10^{15} keys. This key structure is becoming is short for modern computers, therefore as a result

- In 1997, D.E.S was cracked by a group of 3 500 computers in 4 months
- In 1998, D.E.S was cracked by specially designed hardware in 4 days
- In 2008, D.E.S was cracked with inexpensive commercially available hardware in less than one day

A BRIEF HISTORY OF AES

Background by DrSoper(9) suggest that in 1997 the national institute of standard and technology NIST requested proposal for a new encryption standard. Criteria for the new standard had to stipulate that the code of the algorithm must be unclassified and publicly disclosed and the algorithm had to be royalty-free world wide. The algorithm itself had to implement symmetric block cipher that would operate on 128 bits blocks of data and had to be usable with keys that were128, 192 and 256 bits in length. The response to the request proposal was robust and in 1998 15 algorithms were selected as semi-finalists. After further analysis of the semi-finalists 5 finalists were selected in 1999 including the MARS algorithm, RC6™ algorithm, the Rijndael algorithm, Serpent algorithm and the Twofish algorithm. The 5 finalists were subjected to extensive evaluation and scrutiny in both private and public arenas. The three key criteria by which the finalists algorithms were evaluated included security, efficiency of operation and the easy with which the

algorithm could be implemented. Following 2 years of analysis the Rijndael algorithm of Belgian cryptographers Joan Daemon and Vincent Rijmen was selected as a winner in 2001. Rijndael was adapted by the US Government as federal information processing standard 197 or FPS 197 and was thereafter known as Advanced Encryption Standard(A.E.S). It was extensively used worldwide since 2002.

Each round of AES is governed by the following transformations(10)(11):
Substitute Byte transformation
The step consists of using the 16 x 16 lookup table to find a replacement byte for a given byte in the input state array. Entries in the lookup table are created by using the notions of multiplicative GF(2^8) and bit scrambling to destroy the bit level correlations inside each byte.

Shift Rows transformation

It is called ShiftRows for shifting the rows of the state array during the forward process. The corresponding transformation during decryption is denoted InvShiftRows for Inverse Shift-Row Transformation. The goal of this transformation is to scramble the byte orderinside each 128-bit block.

Mixcolumns transformation

It is calledMixColumns for mixing up of the bytes in eachcolumn separately during the forward process. The corresponding transformation during decryption is denoted InvMixcolumns and stands for inverse mix column transformation. The goal is here is to further scramble up the 128-bit input block.

Addroundkey transformation

It is called AddRoundKey for adding the round key to the output of the previous step during the forward process. The corresponding step during decryption is denoted InvAddRound-Key for inverse add round key transformation.

The block diagram for A.E.S algorithmon the assumption of 128 bit key length is as follows(4)

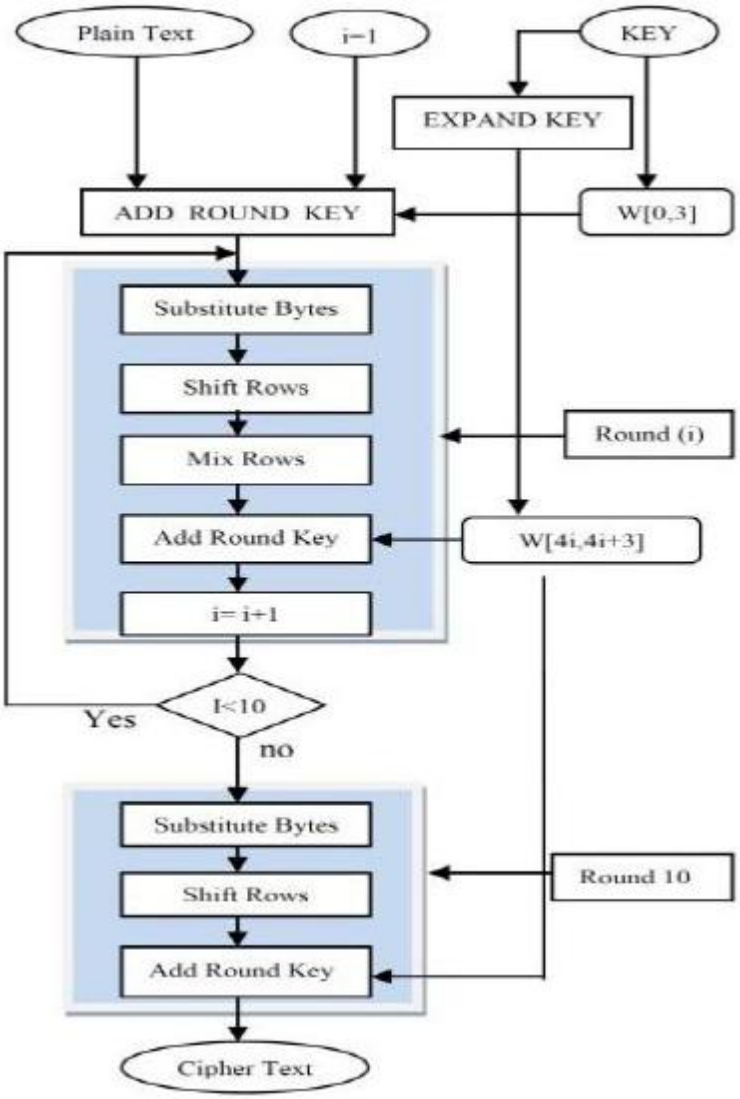

Figure 3 Workflow of AES algorithm

Hybrid Algorithm Design

The conceptual being in mind for the design an algorithm that will be as a result of harmonizing the R.S.A and A.E.S is that the algorithm has to be fast and the same time secure. Another assumption that is made is that the key size required for Asymmetric A.E.S algorithm is that the key size is 128 bits which is suitable for 10 rounds that includes the 4 components of byte substitution, row shift, column mix and add round key for each round. Since the R.S.A is slow in both encryption and decryption, it willnot be involved in those process therefore as such the A.E.S has to take over for both encryption and decryption. R.S.A will be involved in two processes, in the first process it will encrypt the symmetric key used by A.E.S when encrypting plaintext. The stage is important for the enhancement of security of the data itself and the key that are in transit. On the second stage the

R.S.A will decrypt the encrypted symmetric key that would be used by the A.E.S to decrypt cipher text back to plain text.

Design Objectives of the Hybrid Approach

The two key conceptual objectives of the hybrid approach are as follows:

- To enhance the security
- To reduce decryption and decryption times

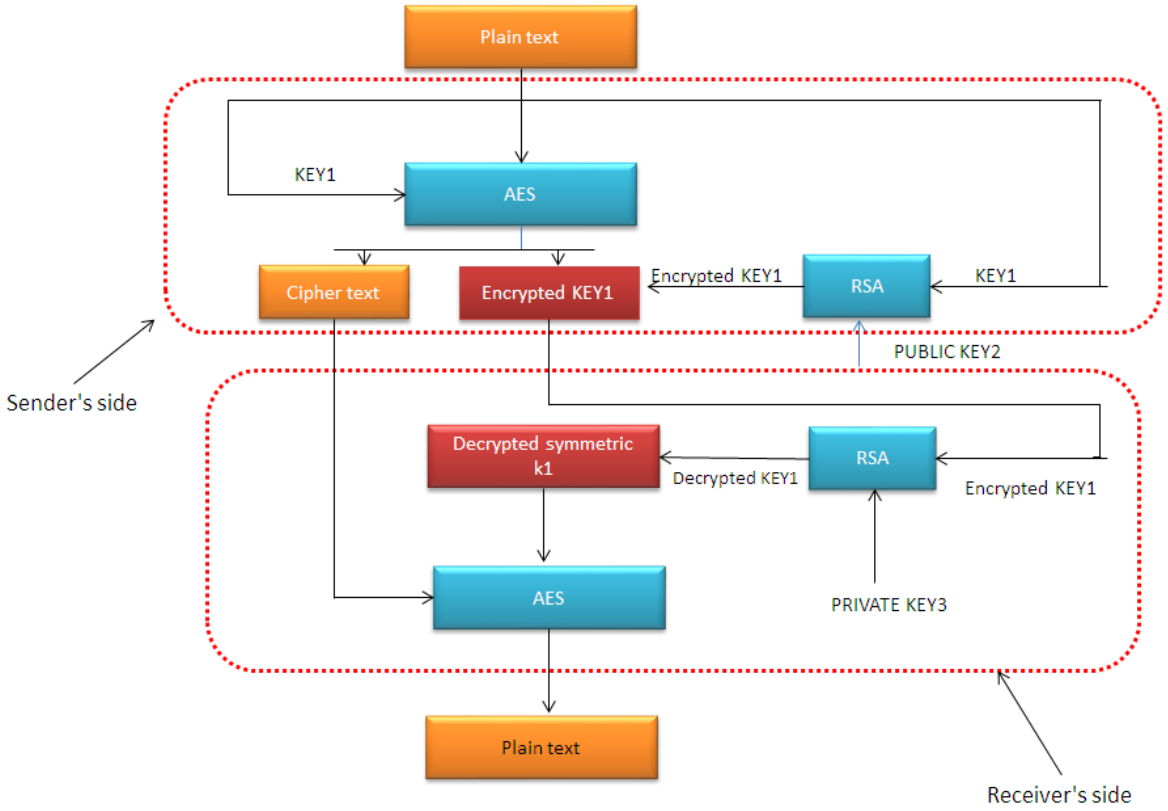

Figure 4 Workflow of the Hybrid Algorithm

Stages of the Hybrid Algorithm

a) Sender uses A.E.S algorithm to encode plain text message using A.E.S symmetric key1 to form cipher text
b) R.S.A algorithm is used to encrypt A.E.S symmetric key1 using Receiver's public key2
c) The cipher text and encrypted asymmetric key1 are then send to the receiver
d) Receiver uses own private key3 to decode A.E.S symmetric key1
e) Finally receiver uses the decoded A.E.S symmetric key1 to convert the cipher text back to plain text.

REFERENCE

1. E-Commerce. [Online]. [cited 2015 october 15. Available from: http://www.keyitsolutions.com/e-commerce_ecommerce.htm.

2. Kwenda C. Effective Data Security for E-Commerce Applications. International Journal of Advanced Research in Computer and Computer Engineering. 2015 October; 4(10).

3. Sengupa A, Mazumdar C, Barik M. E-Commerce Security - A life Cycle Approach. Sadhana. 2005 June; 30.

4. Singh S, Supriya. A Study Of Encryption Algorithms(RSA,DES,3DES and AES) for information security. International Journal For Computer Applications. 2013 April; 67(9).

5. Aman K, Sudesh J, Sunil M. Comparative Analysis Between DES and RSA Algorithm. International Journal Of Advanced Research in Computer Science and Software Engineering. 2012 July; 2(7).

6. Zhou X, Tang X. Research and Implementation of RSA algorithm for Encryption and Decryption. In The 6th International Forum on Strategic Technology; 2011. p. 1118-1121.

7. Somani U, Lakhani K, Mundra M. Implementing Digital Signatures with RSA Algorithm to Enhance the Data Security of Cloud in Cloud Computing. In 1st International Conference; 2010; Solani. p. 211-216.

8. Singh S, Maakar S, Kumar S. A Perfomance Analysis of DES and RSA Cryptography. International Journal of Emerging Trends and Technology in Computer Science. 2013 June; 2(3).

9. Soper D. Encryption Concepts - Information Security lecture #6 of 12. [Online].; 2013 [cited 2015 September 21. Available from: https://www.youtube.com/watch?v=qcai6ZY6sVs&list=PLwNJunAkF44LaPBlwiQIAsRNb2Nkiq3uD&index=6.

10. Padmavathi B, Ranjika Kumari s. A Survey on Perfomance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique. International Journal of Science and Research. 2013 April; 2(4).

11. Avik K. Lecture Notes on Computer and Network Security. Avinash Kak Purdue University. 2013 May.