Research Journal of Applied Sciences, Engineering and Technology 5(9): 2692-2700, 2013
DOI:10.19026/rjaset.5.4793
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: September 16, 2012 Accepted: October 09, 2012 Published: March 20, 2013

Research Article

A Generic Hybrid Encryption System (HES)

[1, 2]Ijaz Ali Shoukat, [1]Kamalrulnizam Abu Bakar and [1]Subariah Ibrahim
[1]Department of Computer Systems and Communication, Faculty of Computer Science and Information System, University Teknologi Malaysia, 81310, Johor Bahru, Malaysia
[2]Department of Computer Science, College of Computer and Information Sciences, King Saud University, P. O. Box. 51178, Riyadh 11543, Saudi Arabia

Abstract: This study proposes a Generic Hybrid Encryption System (HES) under mutual committee of symmetric and asymmetric cryptosystems. Asymmetric (public key) Cryptosystems associates several performance issues like computational incompetence, memory wastages, energy consumptions and employment limitations on bulky data sets but they are quite secure and reliable in key exchange over insecure remote communication channels. Symmetric (private key) cryptosystems are 100 times out performed, having no such issues but they cannot fulfill non-repudiation, false modifications in secret key, fake modifications in cipher text and origin authentication of both parties while exchanging information. These contradictory issues can be omitted by utilizing hybrid encryption mechanisms (symmetric+asymmetric) to get optimal benefits of both schemes. Several hybrid mechanisms are available with different logics but our logic differs in infrastructural design, simplicity, computational efficiency and security as compared to prior hybrid encryption schemes. Some prior schemes are either diversified in performance aspects, customer satisfaction, memory utilization or energy consumptions and some are vulnerable against forgery and password guessing (session key recovery) attacks. We have done some functional and design related changes in existing Public Key Infrastructure (PKI) to achieve simplicity, optimal privacy and more customer satisfaction by providing Hybrid Encryption System (HES) that is able to fulfill all set of standardized security constraints. No such PKI based generic hybrid encryption scheme persists as we have provided in order to manage all these kinds of discussed issues.

Keywords: Asymmetric encryption, hybrid encryption system, key exchange, symmetric encryption

INTRODUCTION

Encryption mechanisms are the backbone of exchanging secure transactions over insecure remote channels. Encrypting of data mostly concerns with the robustness of encryption methods, achieving of security constraints and processing speed related issues. But the actual problem occurs at the time of exchanging encrypted data and key(s) via insecure remote communication channels. The exchange of key is said to be secure if it fulfills the all set of security goals like confidentiality, integrity (false modification, authenticity) and availability (Melia and Elbirt, 2010). Confidentiality concerns with secrecy and privacy which means message should be visible to whom person for which it has been sent. Integrity assures that message is free from fake modifications (false addition or deletion) and it can be further classified into two terms:

- **Authenticity:** Which means the identity of sender should be verified on delivering the message whether the information is coming from authentic sender to whom we are expecting.
- **Non-repudiation:** It means both sender and receiver cannot deny about the information that they have sent. Availability means information (message, key, Certificate Verification) and medium (Certification Authority Server, online services) should be timely available when needed.

Traditional cryptosystems (Public and Private) follow robust design and operative distinctions between them as depicted in Fig. 1 and 2. Private Cryptosystems require that both parties have to share and agreed on same secret or private key before starting encryption procedure but in case of asymmetric algorithms public key is publically available to initiate encryption any time when needed without having agreement of other party and private key remains secret in both sides (Canniere, 2007). Public key cryptography operates under third trusted party to get complete set of security objectives. Conventional cryptosystems have their own

Corresponding Author: Ijaz Ali Shoukat, Department of Computer Systems and Communication, Faculty of Computer Science and Information System, University Teknologi Malaysia, 81310, Johor Bahru, Malaysia

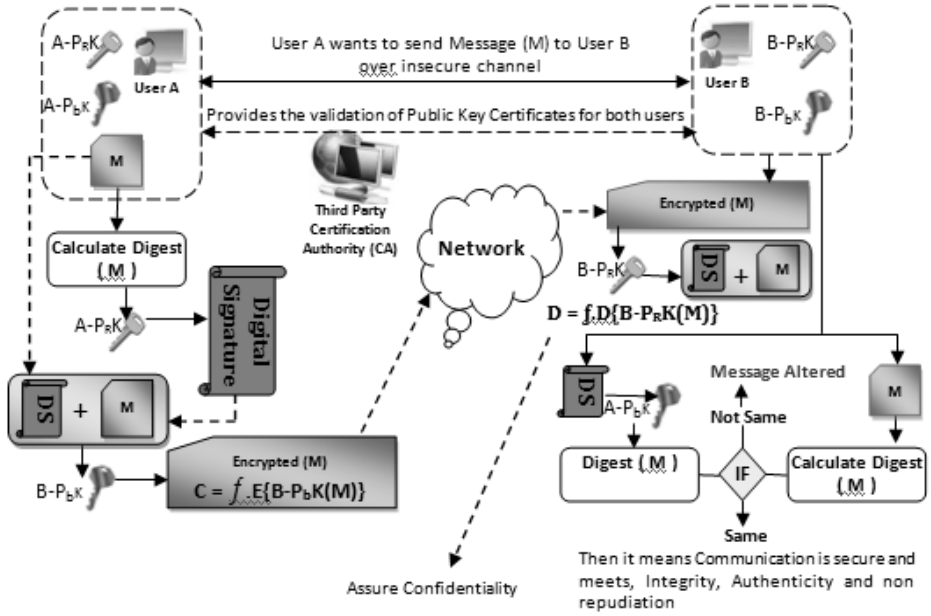

Fig. 1: Prior design and transaction flow of PKI model

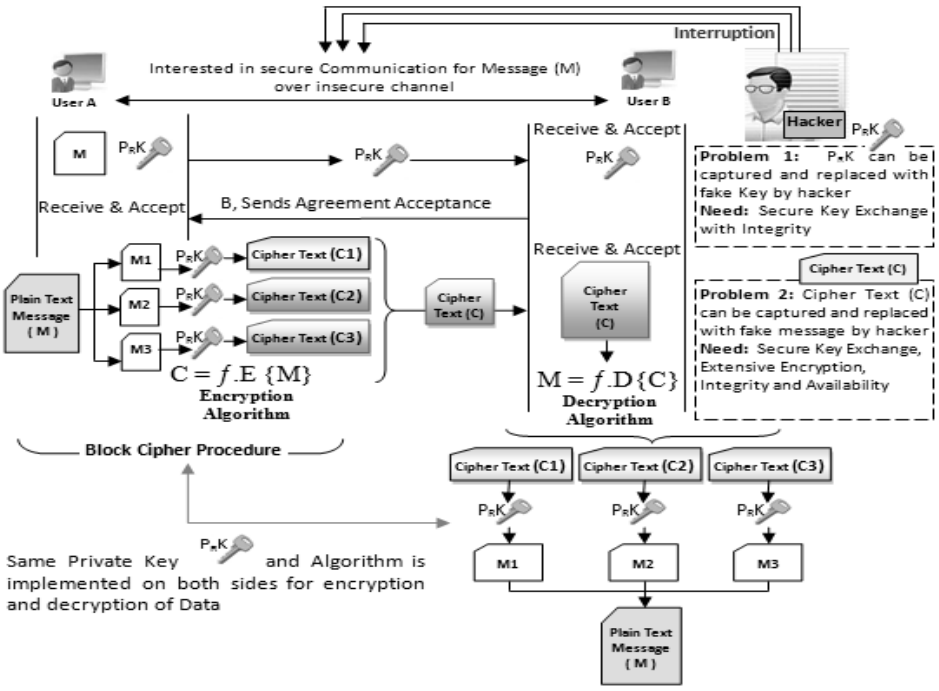

Fig. 2: Working logic of private key (Symmetric) cryptosystems

affirmative and feeble characteristics as reported by the authors of study (Shoukat *et al*., 2011).

Asymmetric schemes have applicability and feasibility related limitations in case of video, audio or any kind of bulky data because these schemes are 100 times slower rather to symmetric schemes. The other reasons of sluggish processing behind asymmetric schemes are their utilization of complex modular functions, nontrivial calculations and huge integers (512-2048) for key selections. Therefore, asymmetric schemes consume more memory, electric power and processing effort as compared to symmetric ones. As regard with symmetric schemes, the sharing of selected secret key with other party minimizes the life of a key in future due to security point of view. However, symmetric schemes are 100 times faster in processing, having no feasibility or applicability issues on bulky

data. Moreover, symmetric schemes do not associate the share of any other public information but in case of asymmetric it is necessary to share public information associated with public key with other parties that may be misused under any unwanted circumstances.

order to tackle these issues for getting of optimal performance and enhanced security while encrypting and exchanging the confidential information.

LETERATURE REVIEW

Hybrid encryption approach is an optimal way to utilize the worth full features of both symmetric and

The ultimate objective of this study is to acquire hybrid encryption systems without having forgery and password guessing attacks in addition to merge the benefits of both symmetric and asymmetric schemes. By following hybrid strategy of symmetric and asymmetric cryptosystems, all discussed issues can be escaped properly. Presented idea is timely significant in asymmetric cryptosystems. Prior Public Key Infrastructure (PKI) is a well known and widely implemented infrastructure that provides all security objectives. But when PKI is used with Public Key Cryptography then its performance degraded in encryption phase because asymmetric cryptosystems are 100 times slower than symmetric algorithms in encryption and decryption phases (Schneier, 1996).

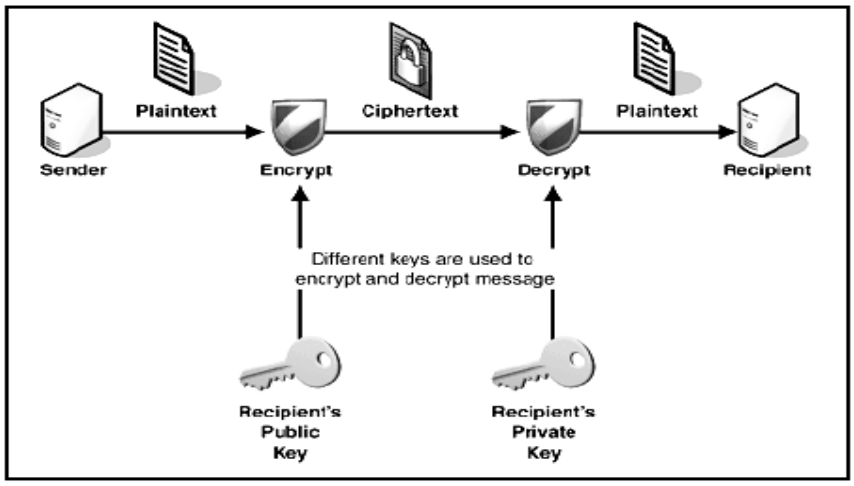

Fig. 3: Prior PKI based basic encryption strategy

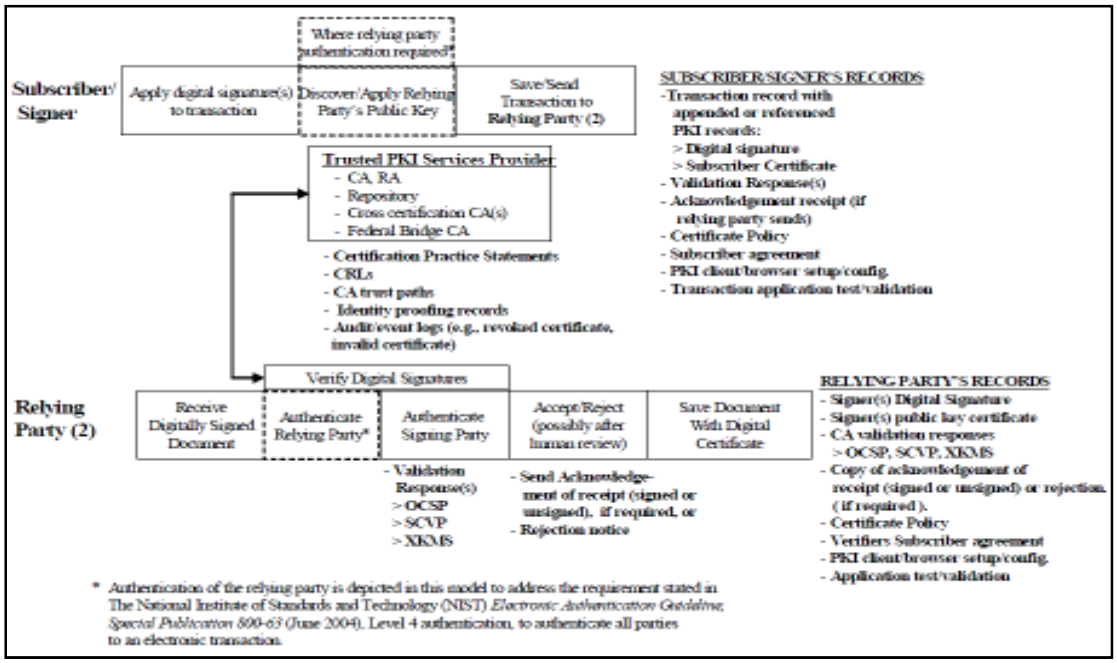

Fig. 4: Working flow of PKI based encryption scheme

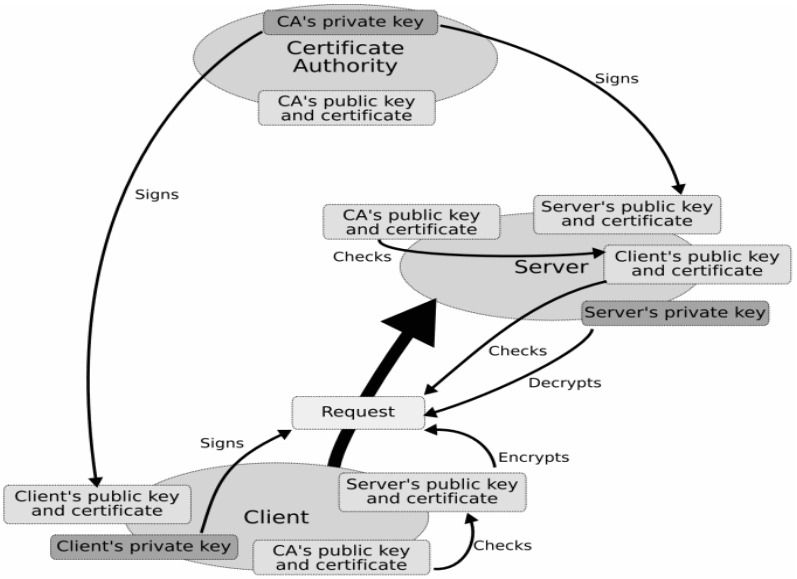

Fig. 5: Prior PKI base transaction flow

Symmetric block ciphers are good for encryption but key exchange is a problem with them especially to predict false modification, non-repudiation and origin authentication. In 2012, author of study (Ijaz, 2012) reported the basic Public Key infrastructure for encryption purposes as represented in Fig. 3. The NARA-National Archives and Records Administration (NARA, 2005) described the transaction work flow of PKI as discussed in Fig. 4. Furthermore, another transaction based PKI infrastructure is discussed by University of Southampton IT Innovation Centre in 2009 as represented in Fig. 5. All these prior reported PKI architectures and working flow is jointly depicted Fig. 1 by us.

The prior design of PKI doesn't have a specific hybrid infrastructure (symmetric + asymmetric) with generic kind of hybrid encryption scheme as we have provided. However, several hybrid encryption schemes persist under different kinds of infrastructures or their logic for hybrid encryption differs with the proposed work (Dubal *et al*., 2011; Kessler, 1999; Subasree and Sakthivel, 2010). PKI is most secure and widely used infrastructure (Vatra, 2011) that's why we selected PKI to propose hybrid encryption scheme.

We have done some design and functional modifications in traditional PKI infrastructure while proposing our HES that can provide computationally effective services as compare to most of prior hybrid encryption schemes that utilize asymmetric algorithms in encryption phase. Our proposed HES uses symmetric encryption algorithm for encrypting the confidential data because symmetric encryption algorithms are many time out performed to asymmetric ones (Schneier, 1996). This thing clearly invokes that HES is better in encryption phase rather to asymmetric base prior hybrid encryption schemes. Furthermore, HES don't have applicability issues on large data sets and it can facilitate more customer satisfaction. Private Key Cryptosystems cannot handle non-repudiation, false modification and origin authenticity against the communicated parties as discussed in Fig. 2. However, these systems are efficient and fully applicable on all type of data contents. On the other hand Public Key Cryptosystems are 100 times slower rather to Private Key Cryptosystems (Schneier, 1996) but they can fulfill all set of security objectives like non-repudiation, false modification and origin authentication. To overcome these kinds of issues several hybrid encryption schemes persist. The authors of study (Dubal *et al*., 2011) gave the idea of Elliptic Curve Digital Signature Algorithm (ECDSA) plus the utilization of Dual RSA as a hybrid scheme to achieve the task of false modification and origin authenticity. The problem with this scheme is that it utilizes public key algorithm for encrypting the plain text and ECDSA for signature verification through Elliptic Curve parameters but Elliptic Curve technique is slower in signature verification (Kessler, 1999) and RSA is slower in encrypting process rather to symmetric algorithms. Furthermore, in case of large data set like audio, video data some issues like applicability, more power and memory consuming are associated with this hybrid encryption scheme.

In 2010, the author's study (Subasree and Sakthivel, 2010) proposed a hybrid encryption protocol that utilizes Elliptic Curve Cryptography (ECC) to encrypt the plain text and dual RSA to encrypt the hash value of plaintext. The problem with this scheme is that, ECC is slower in encryption phase as compared to

symmetric encryption algorithms (Kessler, 1999). Furthermore, in this scheme both utilized algorithms are based on public key cryptography and ECC is not feasible in case large data set (audio, video) and requires more power of processing. Therefore, in prior hybrid encryption schemes (Symmetric + Asymmetric), some are diversified in computational efficiency, applicability on large data set and some are vulnerable against forgery and password attacks. This situation clearly justifies the need of our proposed hybrid encryption scheme. Our core motive is to merge processing speed, lesser energy and minimum memory requirement related benefits of symmetric algorithms with the security related objectives of asymmetric algorithms. The security objectives include:

- False modification in secret key while exchanging
- False modification in cipher text
- Non-repudiation
- Origin authentication of sender through the utilization of asymmetric schemes

For this purpose, we have proposed Hybrid Encryption System (HES) in order to meet the applicability and security related issues with optimal privacy.

The authors of study (Ramaraj *et al*., 2009) introduced a key management server with remote password base authentication protocol and applied a committee of Advanced Encryption Standard and RSA encryption algorithm to merge the benefits of both public and private key cryptosystems. This scheme utilizes nonce base remote password authentication schemes like: Lamport scheme (Lamport, 1981) and Wu scheme (Wu and Chieu, 2003) to generate a session key for Advanced Encryption Standard (AES). The problem with Lamport's scheme is that it requires to maintain additional password table in order to verify the user credentials. Later on Wu enhanced remote password authentication scheme to get rid of password table through the concept of smart card. Wu's remote authentication scheme is insecure because user is able to login on the server without knowing his/her password therefore, this scheme did not resist the forgery and password guessing (session key recovery) attacks (Yang and Wang, 2004).

Forgery Attack on Wu's Hybrid Encryption Scheme: According to Wu's scheme in login phase before authentication, user inserts the smart card that computes two steps as follows:

Step 1: Compute $B_i^* = g^{Ai,hi,(PWi)} |\text{mod}| P$ and $C_1 = h(T \oplus B^*_i)$ where A and B are the value against users stored on the smart card and P is the huge prime number, g is a function of $GF(P)$, T is the current system time with date, Pw denotes the password and $h(.)$ is a hash function.

Step 2: In 2nd step of login phase, Message (m) is computed as $m = \{ID_i, B^*_i, C_1, T\}$ where ID is the identity of user.

Let suppose, attacker intercepts message: $m = \{ID_i, B^*_i, C_1, T\}$ and computes $C_{1(Attacker)} = h(T^*_{Attacker} \oplus B^*_i)$ and pass the message : $m^*_{Attacker} = \{ID_i, B^*_i, C_{1(Attacker)}, T^*_{Attacker}\}$ to the remote server. The server will examine ID_i *and* $T^*_{Attacker}$ in order to verify the identity and login time against the transaction. When the server will verify the format of ID and T, off course it will find it valid and then attacker can calculate $C_{1(Attacker)} = h(T^*_{Attacker} \oplus B^*_i)$ very easily as this function satisfies the condition $C_{1(Attacker)} = C_1$. In this way the server can accept forged login request successfully. On the other, attacker can also suppose any random number (K) to calculate $C_{1(Attacker)} = h(T^*_{Attacker} \oplus K_i)$ and then he can submit $m^*_{Attacker} = \{ID_i, K_i, C_{1(Attacker)}, T^*_{Attacker}\}$ to the system. In this way system will also accept this request.

Password Guessing Attack on Wu's Hybrid Encryption Scheme: In case of user lost the smart card and attacker find it. There is a secret information: $\{ID_i, Ai, B_i, h(.), p, g\}$ on smart card and secret password can easily be remembered due to short length. In this way attacker can recover actual password ($PW^*_{attacker}$) by computing $B^*_{attacker} = g^{Ai,hi,(PW^*attaker)} |\text{mod}| P$ that will satisfy the condition $PW^*_{attacker} = PW_i$ successfully. In this way the attacker can get actual password. Hence, $PW^*_{attacker} = PW_i = Session\_Key(KS)$ in Ramaraj's hybrid encryption scheme (Ramaraj *et al*., 2009) that utilizes Wu's remote password authentication logic which is fully vulnerable against forgery and password guessing (session key recovery) attacks. Therefore, to handle these problems this study proposes Hybrid Encryption System (HES) through some design modifications in traditional PKI.

DESIGN OF PROPOSED HYBRID ENCRYPTION SYSTEM (HES)

The design of proposed Hybrid Encryption System (HES) requires some operational and design modifications in the existing Public Key Infrastructure (PKI). The hybrid infrastructure used by the author of study (Ramaraj *et al*., 2009) is other than the Public Key Infrastructure that is fully vulnerable against forgery and session key recovery attacks as discussed earlier. Proposed PKI negate the philosophy of utilization of nonce base concept in order to avoid these kinds to attacks. On the other hand propose hybrid scheme also negate the philosophy of using asymmetric encryption algorithms in encryption phase due to

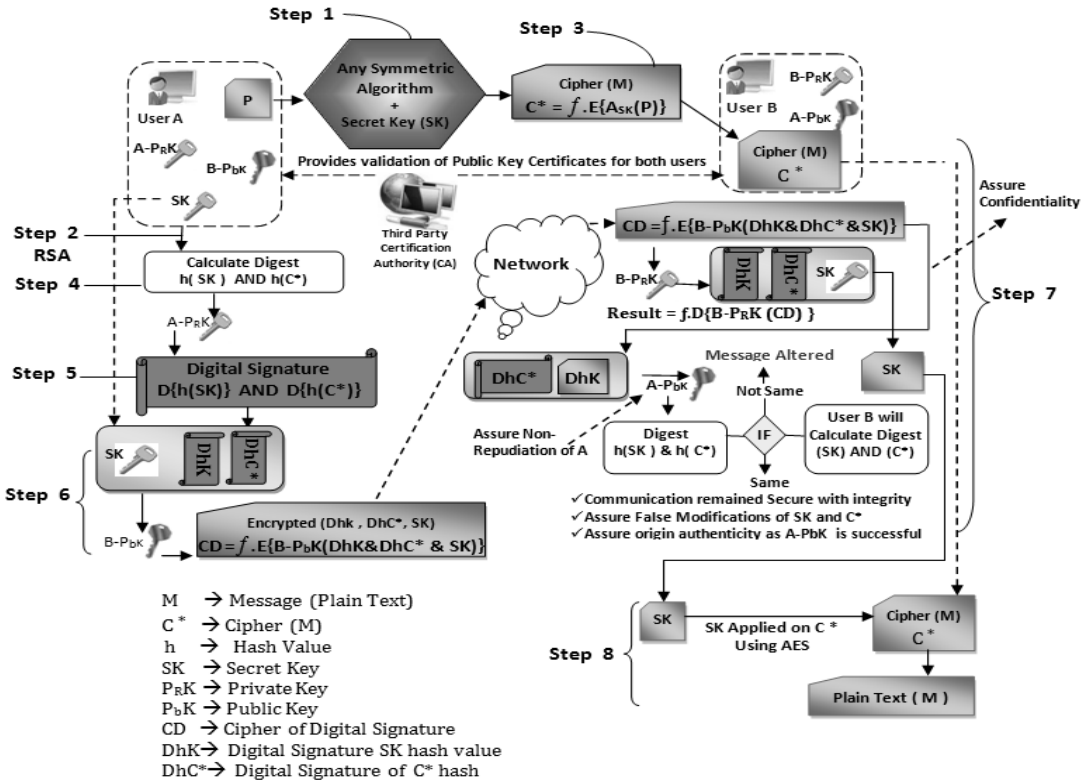

Fig. 6: Proposed design of Hybrid Encryption System (HES)

Table 1: Working steps of HES

Working steps of HES	Security issues solved
Step 1: Select a Secret Key (SK) and symmetric algorithm for enciphering procedure. We prefer AES for this step.	• Computational efficiency • Feasibility issues for large data sets
Step 2: Select MD5 or Sha-1 or any hashing algorithm for computing the hash values of SK and Cipher Text (C*). We prefer Sha-1.	• To meet the following objectives later on other side. • False modification • Authenticity • Confidentiality
Step 3: Generate the cipher text by applying AES and SK. After that Transfer the cipher text (*C**) directly to user B (Receiver).	• *Cipher text* will not be shared with third party • It minimizes the *spy based hidden* attacks • It achieves *customer satisfaction* upon third party.
Step 4: Calculate the hash (digest) of SK and Cipher Text *(C*). Hash of secret Key= h(SK)* Hash of cipher text = *h(C*)*	• Confidentiality
Step 5: Compute the digital signature of *h(SK + C*)* by applying User A's Private Key through RSA. *DhK = RSA {h(SK)}, D hC*= RSA {h(C*)}*	• Authentication of Message origin
Step 6: Apply User B's Public Key on SK, *DhK* and *Dh C** to compute cipher text of signatures *(CD)*. *CD =ƒ.E{B-PbK(DhK&DhC*& SK)}*	• User A can verify User B's *identity* by analyzing his/her Public Key (B-PbK) information. • Confidentiality
Step 7: How Non-repudiation, false modifications and origin authentications will be verified (a) Now user B has *C, CD =ƒ.E{B-PbK(DhK&DhC*& SK)}* User B will apply his/her B-PrK to decrypt the CD and will find digest values of *DhC** , *DhK and original SK* (b) After that, *DhC**and *DhK* will be deciphered by applying user A's *A-PbK* to get *h(SK)* and *h(C*)*. (c) The digest of *SK* and *C** will be recomputed by user B in order to compare the results of step (a) and (c).	• Step (a) will assure *origin authentication* of User B towards user A with *confidentiality*. • Step (b) will assure *origin authentication* and *non-repudiation* of User A towards User B with *confidentiality*. • The comparison of Step (a) and Step (c) will assure *False modification of SK and C** to assure integrity in such a way if both values are same; it means no alteration otherwise alteration persists.
Step 8: User B will get original SK from step 7 to apply SK and AES on C* for getting of Plain Text.	• Confidentiality

computational incompetency. According to HES the plain text should be encrypted through any symmetric algorithm and encrypted data should be sent directly to the other party. However, the secret key(s), digest (hash values) of secret key and hash of cipher text should be exchanged through PKI philosophy by using asymmetric algorithm like RSA for generating signature and SHA-1 for generating hash values. For encryption phase we preferably recommend Advanced Encryption Standard (AES). These resulted design and operative changes are more effective in fulfilling of performance, applicability and security related issues like non-repudiation, false modification, origin authentication and customer satisfaction. The design of Proposed HES is illustrated in Fig. 6.

Working methodology of HES: The proposed Hybrid Encryption System (*HES*) can utilize any symmetric cipher for producing cipher text in order to cover computational and applicability issues on large data sets and it can use asymmetric cipher for exchanging the secret key, hash of key and hash of cipher text etc. All this information will be exchanged through PKI strategy as described in Table 1. How confidentiality, non-repudiation, origin authentication, customer satisfaction upon third party and false modifications of keys and cipher text is achieved in our proposed scheme is discussed in Table 1 with logical justifications.

DISCUSSION AND ANALYSIS

Our proposed Hybrid Encryption System (HES) is generic that can be used with any combination of symmetric and asymmetric encryption algorithms according to the customer's preferences. However, we preferably recommend to use HES with AES and RSA for getting optimal outcomes. HES is effectively secured in fulfilling of all set of standardized security constraints (confidentiality, non-repudiation, origin authentication, false modification in secret key and cipher text) with hybrid encryption support as evidenced by Table 1. Any exchange of information through a system that can fulfill these security constraints is said to be potentially secured according to the 44 United States Codes, Section 3502. Furthermore, proposed HES is free fromforgery and password guessing (session key recovery) attacks as compared to the previously reported hybrid encryption scheme (Ramaraj *et al*., 2009) because HES relies upon secure socket layer PKI strategy (GmbH, 2007) for which no such attacks are reported yet. Prior Hybrid Encryption Schemes are diversified in many aspects as compared to our proposed Hybrid Encryption scheme. We summarized the comparison of HES with prior encryption schemes in Table 2.

The resultant analysis of Table 2 clearly invokes that our HES is computationally effective rather to prior hybrid encryption schemes as discussed earlier because these schemes used either Elliptic Curve Cryptography (ECC) or RSA algorithm for encryption phase. The ECC is slower in encryption phase (Muyinda, 2009) rather to symmetric encryption algorithms and ECDSA is slower in signature verification (Dubal *et al*., 2011). The discrepancy associated with the utilization of RSA in *encryption phase* is that it is 2000 times slower in encryption and decryption of data rather to symmetric algorithm like AES because RSA uses complex computations through non-retrieval mathematics with huge wastage of memory and electric power too (Fontaine and Galand, 2007). Our proposed HES

Table 2: Comparison of proposed HES with prior hybrid encryption schemes

	Prior Hybrid Encryption Schemes Vs Proposed HES			
Evaluation parameters	Dubal *et al*. (2011)	Subasree and Sakthivel (2010)	Ramaraj *et al*. (2009)	Our "*Proposed"* Hybrid Encryption Scheme 2012
Symmetric + Asymmetric	×	×	✓	✓
Computationally efficient	×	×	✓	✓
Feasibility for large data sets (Audio, Video)	×	×	✓	✓
Non-repudiation and False modifications	✓	✓	✓	✓
Origin authentication of both parties	✓	✓	✓	✓
Applicability of forgery attack	×	×	Yes	No
Applicability password (session key) guessing attack	×	×	Yes	No
Access of third party over	Keys Digest (Hash values)	Keys Digest (Hash values)	Keys Digest (Hash values)	Keys Digest (Hash Values)
Customer satisfaction	×	×	×	✓
Memory requirement	High	High	low	Low
Electric power (energy) consumption	High	High	Low	Low

negates the philosophy to utilize asymmetric algorithm in *encryption phase* and it recommends to use symmetric algorithm for encryption phase because symmetric algorithms are 100 times faster rather to asymmetric ones (Schneier, 1996). Due to the utilization of symmetric encryption algorithm in encryption HES does not have feasibility issues over large data sets (audio, video) because any DVD takes around a minute to generate cipher through any fast symmetric cipher in contrast with generating the same DVD with asymmetric algorithms may takes hours or days (Fontaine and Galand, 2007). Therefore, proposed HES is computationally effective and it does not have feasibility issues upon large data sets and these traits maximize the customer satisfaction too. Furthermore, by utilizing symmetric algorithms in encryption phase also minimize the memory requirements and energy consumptions because asymmetric encryption algorithms require more electric power (energy) due to large key size in encryption phase but the energy consumption of symmetric algorithms do not depend on bulky data nor on bulky key (Potlapally and Raghunathan, 2006). Symmetric ciphers are less memory waster rather to asymmetric ciphers (Agrawal and Mishra, 2012).

CONCLUSION

The joint committee of symmetric and asymmetric algorithms is more effective in case of computational efficiency, feasibility issues to process large data sets and fulfilling of all standardized set of security constraints like Confidentiality, non-repudiation, False Modification in Secret Key, False Modification in Cipher Text, Origin Authentication in addition with customer satisfaction while exchanging information over insecure remote communication channels. To achieve these objectives it is worth full decision: if cipher of plaintext is generated with symmetric algorithm like AES and all other information (*Keys*, *Digest (hash) values,* etc.) are computed with RSA and Sha-1 algorithm before enchantment through PKI strategy. The discussion and analysis with Table 2 evidenced that our Hybrid Encryption System is also significant in memory requirements and energy consumptions. Our proposed HES under the utilization of PKI is free from *forgery* and *password (session key) guessing* attacks as well as it is also capable to provide *optimal privacy* with sufficient customer's satisfaction and computational efficiency as compared to prior hybrid encryption schemes. Proposed HES facilitates generic support to use any combination of symmetric and asymmetric algorithm. No such kind of generic hybrid encryption scheme under PKI strategy is conveyed yet.

ACKNOWLEDGEMENT

This research study has been supported by "Deanship of Scientific Research", King Saud University, Riyadh, Kingdom of Saudi Arabia (KSA). We are grateful to them for this support.

REFERENCES

Agrawal, M. and P. Mishra, 2012. A comparative survey on symmetric key encryption techniques. Int. J. Comput. Sci. Eng., 4(5): 877-882.

Canniere, D.C. 2007. Analysis and Design of Symmetric Encryption Algorithms. Katholieke Universiteit Leuven, Faculty of Applied Sciences, Department of Electrical Engineering, Castle Arenberg 10, B-3001Leuven- Heverlee (Dutch), Belgium.

Dubal M.J., T.R. Mahesh and P.A. Ghosh, 2011. Design of new security algorithm: Using hybrid cryptography architecture. 3rd International Conference on Electronics Computer Technology (ICECT), Kanyakumari, April 8-10, 5: 99-101.

Fontaine, C. and F. Galand, 2007. A Survey of Homomorphic Encryption for Non-specialists, EURASIP J. Inform. Security, Hindawi Publishing Corporation, Study ID 13801, pp: 10, Doi:10.1155/2007/13801.

GmbH, T.C., 2007. Why PKI? Determining the Business Value of Deploying Digital Certificates. A TC Trust Center Whitestudy, Sonninstrasse, 20097 Hamburg, pp: 24-28.

Ijaz, I., 2012. Design and implementation of PKI (for multi domain environment). Int. J. Comput. Theory Eng., 4(4): 505-509.

Kessler, G.C., 1999. An Overview of Cryptography. In: Sloan, J. (Ed.), Handbook on Local Area Networks. Auerbach, Boston.

Lamport, L., 1981. Password authentication with insecure communication. Commun. ACM, 24: 770-772.

Melia, S.O. and A.J. Elbirt, 2010. Enhancing the performance of symmetric-key cryptography via instruction set extensions. IEEE T. VLSI Syst., 18(11): 1505-1518.

Muyinda, N., 2009. Elliptic Curve Cryptography. African Institute for Mathematical Sciences (AIMS).

NARA, 2005. Records Management Guidance for PKI Digital Signature Authenticated and Secured Transaction Records. Federal Public Key Infrastructure Steering Committee Legal/Policy Working Group and National Archives and Records Administration.

Potlapally, N.R. and A. Raghunathan, 2006. Study of the energy consumption characteristics of cryptographic algorithms and security protocols. IEEE T. Mobile Comput. IEEE, 5(2): 128-143.

Ramaraj, E., S. Karthikeyan and M. Hemalatha, 2009. A design of security protocol using hybrid encryption technique (AES- Rijndael and RSA). Int. J. Comp. Intern. Mgnt., 17(1): 78-86.

Schneier, B., 1996. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd Edn., John Wiley and Sons, New York.

Shoukat, I.A., K. Abu Bakar and M. Iftikhar, 2011. A survey about the latest trends and research issues of cryptographic elements. Int. J. of Comp. Sc. Issues (IJCSI), 8(3-2): 1694-0814.

Subasree, S. and N.K. Sakthivel, 2010. Design of a new security protocol using hybrid cryptography algorithms. IJRRAS, 2(2): 95-103.

Title 44, United States Code, Chapter 35 -Coordination of Federal Information Policy, Subchapter I - Federal Information Policy, Sec. 3502 - Definitions.

Vatra, N., 2011. A PKI architecture using open source software for E-government services in Romania. Indian J. Comput. Sci. Eng., 2(4): 532-538.

Wu, S.T. and B.C. Chieu, 2003. A user friendly remote authentication scheme with smart cards. Comput. Secur. ELS., 22(6): 547-550.

Yang, C.C. and R.C. Wang, 2004. Cryptanalysis of a user friendly remote authentication scheme with smart cards. Comput. Secur. ELS., 23: 425-427.