Pertanika J. Sci. & Technol. 26 (3): 1443 - 1452 (2018)

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Analysis of Attacks on Mail Disposition Systems Secured by Digital Signatures Equipped with AES and RSA Algorithms

Herbert Siregar, Enjun Junaeti* and Try Hayatno

Departemen Pendidikan Ilmu Komputer, Universitas Pendidikan Indonesia, Jl. Dr. Setiabudi, Bandung 40154, Indonesia

ABSTRACT

Implementation of Information and Communication Technology (ICT) to assist document management in the mail distribution will be useful in improving document management performance effectively and efficiently. Securing information in mail disposition using electronic media should be made in such an order to prevent unwanted things. Cryprography or digital signature are some of the techniques that ensures security. The purpose of this study is to see the effect of digital signatures to maintain data security using Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) algorithms to the disposition system of letter based on cryptographic purposes, namely Secrecy, Data Integrity, Authentication and Non-repudiation. Several tests of various attacks to the system were conducted. The study concluded the additions of AES algorithm can maintain secrecy and integrity of the letters, while RSA algorithm can maintain authentication and non-repudation of the letters.

Keywords: AES and RSA algorithms, cryptography attacks, digital signature, mail disposition

INTRODUCTION

From time to time the volume of documents - one of which is the mail archives - in an institution or a company will increase, so there is need to have a good document management, so the information contained in the archive can support the performance of the organisation. Implementation of Information and Communication Technology (ICT) to assist document management will be useful in improving document management performance effectively and efficiently, even by utilising internet technology will make it easier for users of information to access information which is loaded on document simultaneously without any obstacle either time or space (Buhalis & Law, 2008). However, it does not have any obstacles,

ARTICLE INFO

Article history:
Received: 20 October 2017
Accepted: 20 June 2018

E-mail addresses:
herbert@upi.edu (Herbert Siregar)
enjun@upi.edu; enjunaeti@gmail.com (Enjun Junaeti)
trybio123@gmail.com (Try Hayatno)
*Corresponding Author

ISSN: 0128-7680

because information from the documents cannot be guaranteed if not properly maintained. In order to prevent unwanted things such as changes or leaks of the letter contents, the mail security should be safeguarded. This paper discusses the performance of one of the document management systems which is assisted by ICT, a mail disposition system, when facing various cryptographic attacks.

Juju and Cowhand (2015) stated that digital signature can maintain the safety of electronic mails, while Nemavarka and Chakrawarti (2015) used cryptography to do so. Digital signature is a mark in a digital document that offered protection against an attack when a sender or a receiver is trying to have modifications of their messages either when they send them or receive them (Bernstein, Buchmann, & Dahmen, 2009). Schneier (1996) said that cryptography was a science and art to maintain the confidentiality of the message by encoding it into a form that no longer understands its meaning. But cryptography is more than to ensure just privacy; it also ensures data integrity, autentication, and nonrepudiation (Katz, Menezes, Van Oorschot, & Vanstone, 1996).

According to Kumar and Hanok (2015), digital signature was a good solution to maintain document security because it could withstand active attacks, such as forgery attack and choosing cipher text attack (Kumar & Hanok, 2015). They provided timestamped signature scheme which could be verified universally using signer's public parameters in message recovery which is implemented in E-Cash System.

The purpose of this study is to discover the effect of digital signatures to maintain data security using Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) algorithms to evaluate performance of the mail disposition system based on cryptographic purposes, namely Secrecy (Devi, 2013), Data Integrity (Katagishi, Asami, Ebihara, Sugiyama, & Toraichi, 1999), Authentication (Dhagat & Joshi, 2016) and Non-repudiation (Al-Hammadi & Shahsavari, 1999). The RSA algorithm is an asymmetric cryptographic algorithm that has a key length in bits that can be set. Thus, the longer the bit gets, the more difficult it is to solve because of the difficulty of factoring the very large two numbers and it takes a long time for the decryption process. In the meantime, AES algorithm is a symmetric algorithm that uses a block cipher (Daemen & Rijmen, 2013). During the encryption and decryption process, AES-128 algorithm does 10 cycles of transformation functions, i.e. Add Round Key, Sub Byte, Shift Rows and Mix Column (Schneier, 2007). The addition of asymmetric and symmetric algorithms, i.e. RSA and AES-128, on the digital signature had been carried out in this study for security data maintenance. Several test of various attacks to the system is conducted to evaluate the performance of the system. In conclusion, based on the research outcome, using AES algorithm can maintain secrecy and integrity of the mails, while RSA algorithm can maintain authentication and non-repudation of the mails again those attacks.

RESEARCH METHOD

The application used in this study was a mail disposition system equipped with digital signature using AES and RSA algorithms. This study used files or images with jpg format because they were easily opened using standard platforms and application in the computer operating system. The software used is described in the Figure 1.

Based on Figure 1, an admin can write a mail and view a mail. The AES and RSA algorithms will be including in email communications or viewing an incoming mail. Securing key in the process of digital signature is to sign that the messages sent with ad legality is done by RSA algorithm. The RSA algorithm is used to reach the purposes of cryptographic i.e. authentication and non-repudiation (Nandhakumar, Binu, & Paul, 2013). The AES algorithm is used to ensure security especially within the message encoding process. The AES algorithm is also used in this study to meet the objectives of cryptography i.e. secrecy and data integrity (Mewada, Sharma, & Gautam, 2016), so the content of the messages are protected from actions like tapping data.

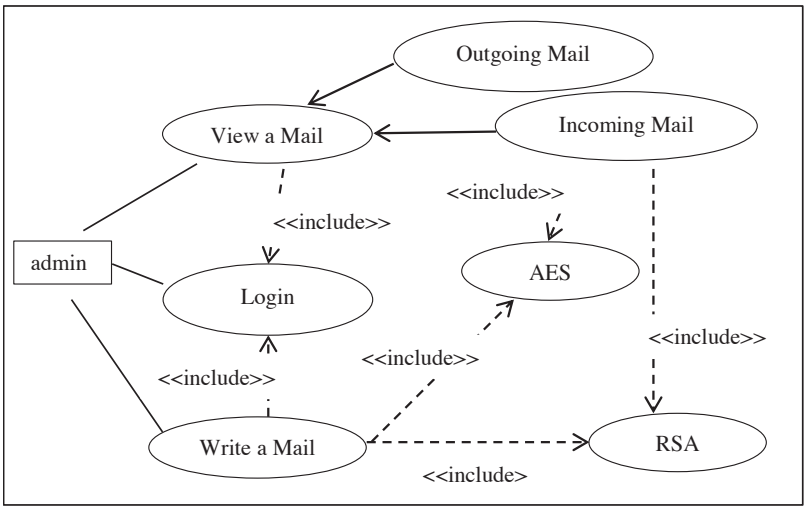

Figure 1. Use case diagram of disposition system of letter

Digital Signature Scheme

A Hash function – modified digital signature scheme (Bao & Deng, 1998) is carried out in this study. Modification is made by adding the encryption process of the mail therein. The AES algorithm serves to encript the message contents that would be delivered to the receiver while RSA algorithm will conceal the signature which is delivered along with the mail. The signature in the system is a key used to encrypt message by AES algorithm. The way RSA algorithm works is slower than that of symmetric cryptography such as DES or AES (Saxena & Kapoor, 2014). Therefore, a symmetric key algorithm, namely AES algorithm would be used to encrypt the message, while an asymmetric algorithm like RSA algorithm, is used to encrypt the key. Figure 2 shows the modification of digital signature scheme in this study.

Figure 2 shows that messages encrypted by AES algorithm would be delivered to the receivers and stored in the database of the system. The AES key used in the system is a combination of an eight-digit number of the sender identity and an eight-digit number of the date of letter sent. Then RSA algorithm would encrypt the key used in the encryption algorithm AES to generate cipher key as well as signature that would be stored in the database.

The RSA algorithms consist of namely public key and private key (Aswathy & Resmi, 2014). In this research, two keys contain prime numbers ranging from 2 to 2000 are randomly selected. The recipients would then decrypt the signature so that the key used to decrypt the messages can be generated.

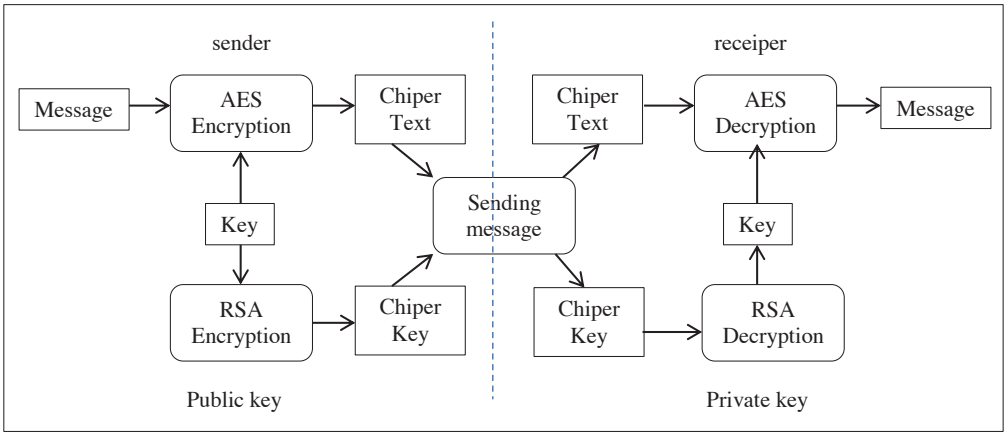

Figure 2. Modification of digital signature scheme

Experiment Testing

Several tests of various attacks had been conducted to achieve the aims of this study. Tests on digital signature schemes had been designed in accordance with the modification of the attacks (Batten, 2013), i.e. addition, reduction, and changing of single character on signature, using different key, and turning aroun time process.

The messege used in this test is shown in the figure 3(a). The keys and signature used in the experiment testing are:

- AES key (plain text) : 1957122620160621
- Public key for RSA : (7, 1728239)
- Private key for RSA : (739543, 1728239)

The ASCII Code of AES key will be encrypted using RSA algorithm to obtain signature of the message. ASCII Code of plain text (AES key) is:

49 7 53 55 49 50 50 54 50 48 49 54 48 54 49 53

So, the signature (RSA chiper text) used in this experiment testing is:

117649 185193 148877 166375 117649 125000
125000 157464 125000 110592 117649 157464
110592 157464 125000 117649

RESULTS AND DISCUSSION

Figure 3 shows an example of a file (mail) which would be encrypted and encryption as well as decryption results if the receiver uses the correct key to decrypt the message in process of the digital signature of the system.

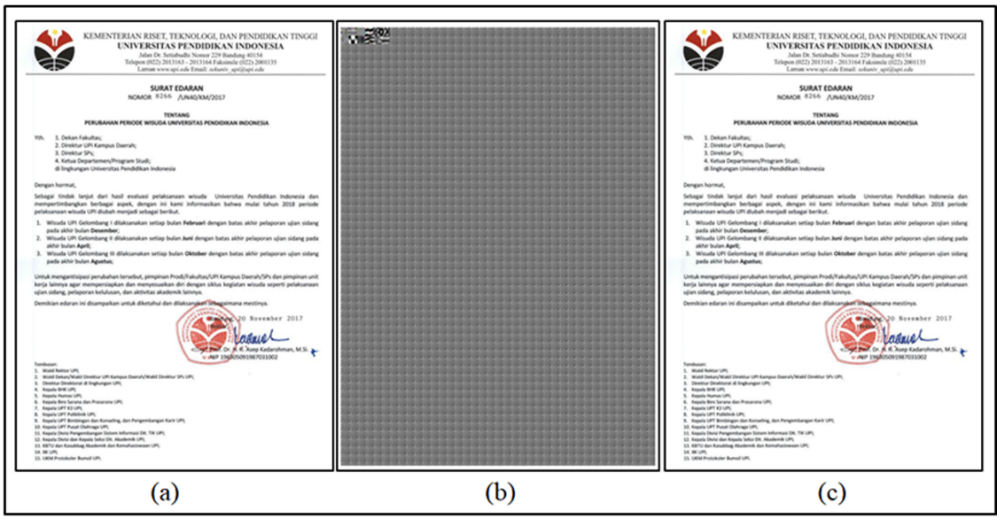

Figure 3. Sample of letter encryption using the AES algorithm

Figure 3(a) shows an example of a mail (image) with jpg format to be sent during the encryption process that used AES algorithm, only the image data will be encoded so the results are also images with jpg format, as shown in Figure 3(b). After the encryption process wis completed, the image is stored on the database system in the form of image cipher text. Figure 3(c) shows the result of decryption of message.

In order to evalutae the performance of the system fofr cryptography purposes, various tests of attack are executed in the system. The addition, reduction, and changing of one character of the signature are run in order to assess the influence of a change in the value of the AES key toward the result of the image decryption. In addition, there is a test to evaluate system resistant toward changing key and turnaround time testing.

Character Changing in the Signature

Various tests of attack character changing in the signature and decrypted results by RSA algorithms is shown in Table 1.

Table 1
Various tests of attack and the results of RSA algorithms decryption

Attack	Signature changes by the Attack	Result of RSA algorithm decryption
Addition of Single Character on Signature	117649 185193 148877 166375 117649 1215000 125000 157464 125000 110592 117649 157464 110592 157464 125000 117649	19571 2620160621
Reduction of One Character	117649 85193 148877 166375 117649 125000 125000 157464 125000 110592 117649 157464 110592 157464 125000 117649	1 57122620160621
Changing of One Character	117649 185193 148877 166375 117649 125000 125000 158464 1215000 110592 117649 157464 110592 175616 110592 148877	1957(22620160621

Based on Table 1, addition of single character on signature attack is done by adding character "1" at the 33rd place of the character sequence on the signature. Then character "1" at the 7th place of the character sequence on the signature is omitted to perform reduction of one character attack. The last at the 45th place of the character sequence on the signature, character "7" replaced by "8" to evaluated changing of one character in the signature towards the result of AES algorithm decryption. Figure 4(a), 4(b), and 4(c) show the results of AES algorithm to decrypt the message using a key which is an outcome using by RSA algorithm decryption process.

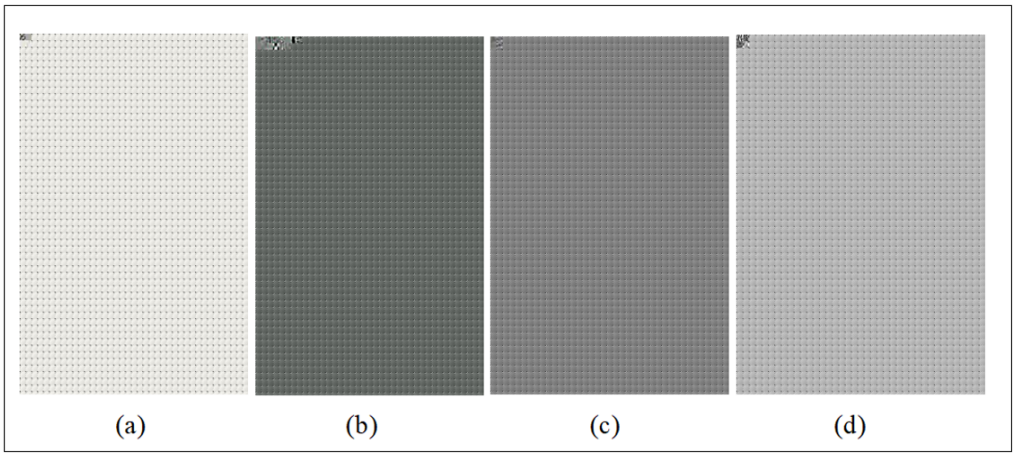

Figure 4. The result of decryption from the various tests

Secrecy of data will secure if no unauthorised parties know the meaning of it (Devi, 2013). Based on the result of AES encryption process, the message has been encrypted without any meaning, whitout AES decryption process, the purpose of the message could not be known, so that confidentiality of the data is maintained. The result of decryption of message in the Figure 3(c) shows that there is no change in the content and purpose massage. But based on Figure 4(a), Figure 4(b), and Figure 4(c), process decryption generates random message, it shows that the accuracy of the message could be guaranteed because the digital signature is very sensitive to a change in data toward the result of decryption of image, so data integrity of the massage can be maintained. It means the AES encryption and decryption process in this digital signature meet the cryptography purposes, i.e. secrecy (Sibert, 2006) and data integrity (Katagish et al., 1999).

Using Different Key

In addition to attacks in the Table, the system is tested to try to deal with "using different key" attacks, i.e. the key is used by receiver to decrypt the signature in the RSA algorithm decryption process is different with right key. This test is administered as an attempt in a case where the receiver uses a different private key which is not the spouse of the public key used to create the signature. Suppose that the key used is:

n = 1685287
public key = 3
private key = 1241787

The results of decryption with the RSA algorithm is:

□□9□□□#□□□#□□9

If this key is used to decrypt the message with the AES algorithm, the decryption result is shown by Figure 4(d). It can be seen that the result does not match the original image in Figure 3(a). This shows that the sensitivity of the digital signature scheme to the keys is good.

Using the right private key to decrypt signature will generate the correct signature, which contains the identity of the sender. This results in the authentication of the sender, and the sender cannot deny that the message is sent by them. The right private key can only be used by the right receiver, this results inauthentication of the receiver. It means that the RSA encryption and decryption process in this digital signature meet the cryptography purposes, i.e. authentication and non-repudiation (Chen, Horng, & Liu, 2013).

Turn Around Time

Turn Around Time test is done to excute the time needed for encryption of plaintext into cipher text and dectyption of cipher text back to plaintext. The image used in the test is 5 .jpg with a size of 1.96 KB to 58 KB. The results of the test is shown in Table 2.

Table 2
Table testing turnaround time

No	File Name	Size (KB)		Time (second)		
		Before	After	Encryption	Decryption	Sum
1	surat_edaran.png	513,00	513,00	36,53	86,51	131,58
2	sample1.jpg	185,00	185,00	13,17	31,20	47,45
3	sample2.jpg	163,00	163,00	11,61	27,49	41,81
4	sample3.jpg	856,00	856,00	60,96	144,35	219,56
5	surat_edaran.jpg	114,00	114,00	8,12	19,22	29,24
6	sample3.jpg	31,00	31,00	3,48	14,06	17,55
7	sample3.jpg	36,00	36,00	4,15	0,72	0,89
8	sample3.jpg	58,00	58,00	0,30	1,14	33.97

Table 2 shows the file size remains the same before encryption and after decryption using the AES algorithm. Hence, AES algorithm does not change the file size \used, so the digital signature maintained the integrity of the message. Therefore, it can be said that the larger the size of the file, the longer the time needed for encryption and decryption processes. It is shown that the time required for process of encryption or decryption is different, depending on the length of plaintext.

Digital signature scheme modification by adding encryption key along with the message and the encryption process when sending messages and adding the decryption process and the decryption key when receiving message is done correctly. The time required for the execution of the system increased because the system would make the process of AES and RSA encryption algorithm when sending messages and make decryption algorithm AES and RSA algorithms when receiving messages.

Implementation of digital signatures using algorithms AES and RSA algorithms on mail disposition system meet the four cryptographic purposes, namely secrecy, data integrity, authentication and non-repudiation. The validity of the sender and receiver are ensured by digital signatures, so the message authentication can be assured (Fu & Wei, 2011). The precise signature could ensure that the sender can not refute that the message was sent by them; it means the signature meets non-repudiation purpose (Belhadj & Akrouf, 2015). The accuracy of the message can be guaranteed by AES algorithm, so it could preserve the secrecy and integrity of data messages in the message delivery process.

CONCLUSION

Based on the research, it can be concluded that the additions of AES and RSA algorithms on the digital signature made the mail disposition system resistant to cryptographic attacks. The protection given to the system meets four objectives of cryptography, namely Secrecy, Data Integrity, Authentication and Non-repudiation.

ACKNOWLEDGEMENT

The authors thank the network security lab at the Computer Science Education Department who supported the experiment along the way.

REFERENCES

Al-Hammadi, B., & Shahsavari, M. (1999). Certified exchange of electronic mail (CEEM). In *Proceedings of the IEEE Southeastcon '99* (pp. 40-43). Lexington, Kentucky: Institute of Electrical and Electronics Engineers Inc.

Aswathy, B. G., & Resmi, R. (2014). Modified RSA public key algorithm. In *Proceedings of the First International Conference on Computational Systems and Communications* (pp. 252-255). Trivandrum, Kerala, India: Institute of Electrical and Electronics Engineers Inc.

Bao, F., & Deng, R. H. (1998). A signcryption scheme with signature directly verifiable by public key. In H. Imai, & Y. Zheng (Eds.), *Proceedings of the International Workshop on Public Key Cryptography* (pp. 55-59). Yokohama, Japan: Springer International Publishing.

Batten, L. M. (2013). *Public key cryptography: applications and attacks.* Hoboken, New Jersey: John Wiley & Sons.

Belhadj, F., & Akrouf, S. (2015). Secure fingerprint-based authentication and non-repudiation services for mobile learning systems. In *Proceedings of the International Conference on Interactive Mobile Communication Technologies and Learning* (pp. 200-204). Thessaloniki, Greece: Institute of Electrical and Electronics Engineers Inc.

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). *Post-quantum cryptography.* Boston, MA: Springer Science & Business Media.

Buhalis, D., & Law, R. (2008). Progress in information technology and tourism management: 20 years on and 10 years after the Internet—The state of eTourism research. *Tourism Management, 29*(4), 609-623.

Chen, Y. C., Horng, G., & Liu, C. L. (2013). Strong non-repudiation based on certificateless short signatures. *IET Information Security, 7*(3), 253-263.

Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard.* Heidelberg, NY: Springer Science & Business Media.

Devi, T. R. (2013). Importance of cryptography in network security. In G. S. Tomar, M. Dixit, & F. Z. Wang (Eds.), *Proceedings of the Communication Systems and Network Technologies* (pp. 462-467). Gwalior, India: Institute of Electrical and Electronics Engineers Inc.

Dhagat, R., & Joshi, P. (2016). New approach of user authentication using digital signature. In *Proceedings of the Symposium on Colossal Data Analysis and Networking* (pp. 1-3). Indore, India: Institute of Electrical and Electronics Engineers Inc.

Fu, D., & Wei, Z. (2011). Research and implementation of a digital signature scheme based on middleware. In *Proceedings of the International Conference on Electrical and Control Engineering* (pp. 2468-2471). Yichang, China: Institute of Electrical and Electronics Engineers Inc.

Jaju, S. A., & Chowhan, S. S. (2015). A modified RSA algorithm to enhance security for digital signature. In *Proceedings of the International Conference and Workshop on Computing and Communication* (pp. 1-5). Vancouver, Canada: Institute of Electrical and Electronics Engineers Inc.

Katagishi, K., Asami, T., Ebihara, Y., Sugiyama, T., & Toraichi, K. (1999). A public key cryptography-based security enhanced mail gateway with the mailing list function. In *Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing* (pp. 262-265). Victoria, Canada: Institute of Electrical and Electronics Engineers Inc.

Katz, J., Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography.* Boca Raton, USA: CRC press.

Kumar, P. B. S. P., & Hanok, K. (2015). *Time stamped digital signature scheme with message recovery and its application in E-Cash system* (Unpublished doctoral thesis). National Institute Of Technology Rourkela, India.

Mewada, S., Sharma, P., & Gautam, S. S. (2016). Exploration of efficient symmetric AES algorithm. In *Proceedings of the Symposium on Colossal Data Analysis and Networking* (pp. 1-5). Indore, India: Institute of Electrical and Electronics Engineers Inc.

Nandhakumar, N. K., Binu, A., & Paul, V. (2013). Non repudiation for internet access by using browser based user authentication mechanism. In *Proceedings of the Third International Conference on Advances in Computing and Communications* (pp. 296-299). Kochi, Kerala, India: Institute of Electrical and Electronics Engineers Inc.

Nemavarkar, A., & Chakrawarti, R. K. (2015). A uniform approach for multilevel email security using image authentication, compression, OTP and cryptography. In *Proceedings of the International Conference on Computer, Communication and Control* (pp. 1-5). Indore, India: Institute of Electrical and Electronics Engineers Inc.

Saxena, S., & Kapoor, B. (2014). An efficient parallel algorithm for secured data communications using RSA public key cryptography method. In U. Batra, S. Sujata, & A. Arpita (Eds.), *Proceedings of the IEEE International Advance Computing Conference* (pp. 850-854). Gurgaon, India: Institute of Electrical and Electronics Engineers Inc.

Schneier, B. (1996). *Foundations: Applied cryptography* (2nd Ed.). USA: John Wiley & Sons.

Schneier, B. (2007). *Applied cryptography: Protocols, algorithms, and source code in C.* USA: John Wiley & Sons.

Sibert, W. O. (2006). *U.S. Patent No. 7,058,805.* Washington, DC: U.S. Patent and Trademark Office.