Optimized Hybrid Security Model using Base 64 Algorithm in conjunction with Substitution Cipher to Enhance Text Security

Abdullah Maitlo[1], Rafaqat Hussain Arain[1], Riaz Ahmed Shaikh[1], Hidayatullah Shaikh[1], Mahmood Hussain Shah[2], Safdar Ali Shah[1], Mumtaz Hussain Mahar[1]

[1]Department of Computer Science, Shah Abdul Latif University, Khairpur, Sindh, Pakistan
[2]School of Strategy and Leadership, Coventry University, UK

Summary

Social business has improved the ability of managers and stakeholders when decision making. However, existing information security systems provide insufficient practice for information protection while transferring information; hackers access valuable information and break encryption codes applied to text messages. This paper presents the development of an Optimized Hybrid Security Model using Base 64 Algorithm and Substitution in Conjunction to enhance message security. This research is a prototype for the user input of message and security key in Hypertext Preprocessor using JQuery. The developed system needs the input of the plain text and the security key. Initially, Base 64 algorithm encrypts plain text into cypher text with the security key and then the Substitution Cipher encrypts the key into a cypher secured key. For testing, 300 text messages were input with different security keys. This research is a step forward in securing text messages; it can be used to encrypt text between sender and receiver through email, or it can be applied on instant messaging services and also can be used for stronger password encryption.

Key words:
Information Security, Network Security, Encryption, Decryption, Substitution Cypher, Cryptography

1. Introduction

Extensive usage of internet and communication technologies has increased the challenges for secure transmission of information from source to destination. It is uncertain whether any message transferred will be interrupted and intercepted by unauthorized access. Therefore, secured dissemination of information has become a major concern in communication networks as fraudsters can compromise the network by breaking security codes covering confidential information during sharing.

These days, the biggest challenge for organizations is the secure distribution of information while using various channels such as websites, email, video conferencing and messaging [1]. It is necessary for the organizations to protect valuable information and other resources from hackers [2]. Mostly the information is being accessed by illicit persons through violating information security breaches while it is in transmission. Existing systems are not capable of protecting data.

This research provides an advance in securing information from unauthorized access through dually encrypting the message or data and security key using a unique combination of Base 64 Algorithm and Substitution Cipher. The Developed Hybrid Security Model encrypts the text along with a substitute security key while transferring the message. This model is useful for secure communication between the sender and receiver through the email, or it can be applied to an instant messaging service. Furthermore, it is also used for strong password encryption.

2. Research Background

By adopting new technology in business, the environment is changing daily. Using the internet for information sharing has increased the threat of compromised data integrity. Surveys have indicated the challenges for businesses to secure their valuable information [3]. IS is about to protect the integrity, confidentiality and availability of the data and resources of existing information systems [4][5].

It is essential for organizations to set security policies for IS and the protection of electronic resources. Security policies contain the standards and guidelines for the secured use of the data and system resources within and outside the organization [6]. Security policymakers develop the rules for information security as per standards required in an organization [7]. These information security rules must be implemented and practiced inside or among other organizations [8]. The main purpose of the security policies is to inform managers and staff and to have a clear picture of the security measures [9].

Manuscript received March 5, 2018
Manuscript revised March 20, 2018

Companies set policies to protect their employees and valuable information from being compromised. The security policies must be accepted and implemented by the personnel concerned, for example, managers, technical administrators and other staff members. Furthermore, policy documents define the consequences of violating the standards by applying standard laws as per rules and regulations or the countries as well organizations. IS must be considered an important factor by the organizations. It is the responsibility of the management in an organization, particularly top management including the board of directors and the CEOs of the organization, to design and implement the security policies in the organization [10].

Information security policies are adopted by the companies to protect information usage, but information is still being stolen by unauthorized persons [11]. Hackers take over the communication channels and violate security layers. The importance of valuable information lost and the heavy costs incurred by information security breaches continually attract the attention of private companies, government organizations and researcher institutions [12].

There are numerous techniques for securing the information; information hiding is one of the familiar techniques [13] and [14]. Substitute Cipher is one, in which original data can be transformed and characterised into various letters. In 1993 Bruce Schneier developed Blowfish Algorithm that was a symmetric blocks cypher containing a 64 bits block with 32 bits to 448 bits long variable key [15]. The Korean Cryptographers created an algorithm named ARIA that included 28, 129 and 256 sized keys along with a 128-bit block, which encrypted blocks in 12, 14 or 16 rounds [16].

Ron Rivest developed an algorithm with the name of Rivest Cipher which is known as RC2 algorithm [17]. The algorithm was a block cypher that used a 64-bit block along with a key having a different length [18]. The RC2 ranged from 1 byte to 128 bytes, and existing implementations used 8 bytes. In 1987, Ron Rivest designed the RC4 algorithm, which was a later version of RC2. It creates random bytes in a stream, and XORing bytes with the text.

The National Security Agency (NSA) introduced another family of algorithms, which is known as Secure Hash Algorithms (SHA). The SHA computed a digest (hash) of the input for larger documents. The hashing was a one-way process to recover the original documents where the digest obtained could not be used in the SHA. [19] developed the SHA-2 cryptographic algorithm for hash functioning. The SHA family has three generations: SHA-1, SHA-2 and SHA-3 [20].

John Linn, in 1993, introduced the encoding algorithm named Base 64 encryption algorithm [21]. It was created for encrypting the information in the format of binary bytes streaming into 64 printable characters. [22] Designed a cryptographic method in conjunction with Bit Manipulation and MSA algorithms to encrypt and decrypt the files. To encrypt and decrypt the information, MSA used randomized key matrix.

Table 1: Literature review findings

Author & Year	Literature Findings
[3]	Use of internet to share information has increased the number of security threats, and it has become a challenge for organizations.
[8], [10] and [23]	Information security policies are essential for organizations to secure information and electronic resources. Policymakers focus on the development of rules to secure information in their organizations. These security policies must be implemented and practiced in organizations.
[11] and [12]	Unauthorised persons are compromising information. Hackers take over the communication channels and violate information security layers. The significance of valued information and heavy costs of information security systems breached incessantly attracts the attention of companies, governments and researcher institutions.
[13] and [14]	There are many techniques of securing the information; information hiding is a familiar technique.
[15], [16], [18], [19], [21] and [22]	For hiding data, various algorithms have been developed. For example Substitute Cipher, Blowfish Algorithm, ARIA, RC2, RC4, SHA-1, SHA-2, SHA-3, MSA algorithms and Base 64 algorithm. We found the use of the cryptographic method in conjunction with bit manipulation and MSA algorithm to encrypt and decrypt the files.

Table 1 describes the findings of the existing literature. Extensive use of the internet and new technology has increased the threat of unauthorized access to valuable information. It has become a major concern for companies to secure their valuable information and other resources from fraudsters. Companies set and implement their information security policies for inside and outside the company. From a technical point of view, different information security techniques have been adopted, and information hiding is one of those techniques (see Table 1).

The review of the existing literature in the related area identifies that to some extent the work is done on information hiding. The encryption algorithms are developed and used for information security. However, by reviewing the existing literature, we found that information could be secured effectively by the combined use of data security algorithms. While refining the existing literature, we did not find any examples for the combination of Base 64 algorithm and Substitution Cipher for increasing one encrypting layer to increase the security of valuable data.

This research paper presents the development of the Optimized Hybrid Security Model based on a combination of Base 64 algorithm and Substitution Cipher for improving the security level of valuable information to enhance the security of information using dual encryption of both text and security key.

3. Proposed Model

The sole purpose of the current paper was to develop an Optimized Hybrid Security Model to increase the security layer of the text message. The model is based on the combination of Base 64 algorithm and Substitution Cipher for hiding information from unauthorized access. Merging the Base 64 algorithm and Substitution Cipher enabled the researcher to encrypt and decrypt the text to enhance the security level and the security key.

For experimental purposes, this research developed the algorithm in Hypertext Preprocessor by using JQuery. A prototype was created for the user input of message and security key. It has an input of plain text and the security key. Base 64 algorithms encrypts the plain text into cypher text with the security key, and then the Substitution Cipher encrypts the security key which was initially input by the user to substitute the secured cypher key. For decoding, Substitution Cipher decrypts the substitution secured cypher key and assigns it to Base 64 along with the cipher text. Base 64 algorithm decrypts the cipher text with the security key and generates the original message.

Over 300 text messages were encrypted for experimental purposes. This research found that the developed prototype was efficient in the processing of encoding and decoding of information. The implementation of two algorithms (Base 64 and Substitution Cipher) was as per the expectations of the research objectives. Furthermore, the developed model can accept input in the numeric, alphanumeric and alphabetic form.

4. Evaluation of Optimized Hybrid Security Model

Information security is the process of protecting the valuable information and systems from any unauthorized access, via computers and other organizations [24]. The activities and techniques applied to secure the information and information resources of companies are known as information security practices. These are classified into various information security categories such as network security and data security.

Network security refers to securing organizational networks from unauthorized access. It includes the secure usage of the network, as well as the reliability and safety of both the network and the data transferred in network communication [25].

Data security refers to ensuring the security of the data that can be lost via computer damage or theft. As a result, those data losses will cause huge damage to organizations due to the violation of sensitive information [26]. Therefore, the data must be protected from unauthorized access by using various effective approaches such as steganography, cryptography, encryption and decryption.

Information hiding through cryptography is mainly the focus of this paper. Cryptography is the collection of tools and techniques related to various areas of information security [27] such as privacy, authenticity and integrity of information. Cryptography is used to convert valuable data into a form that cannot be interpreted [28].

In this research, Base 64 algorithm is used in conjunction with Substitution Cipher for the encryption of text and the security key to enhancing an extra layer of security. Fig. 1 describes the process of encrypting the security key and text to produce an encrypted key and cipher text.

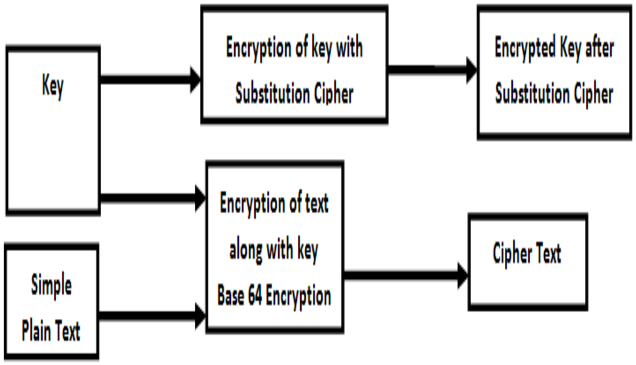

Key
Encryption of key with Substitution Cipher
Encrypted Key after Substitution Cipher
Simple Plain Text
Encryption of text along with key Base 64 Encryption
Cipher Text

Fig. 1 Text encryption process using Base 64 algorithm with the combination of Substitute Cipher

In the initial stage, the plaintext message was input along with the security key for the encryption by using an input interface. Base 64 algorithm encrypts the plain text along with the security key by user input; after which Substitution Cipher encrypts the original key into encrypted substitution cypher. After the encryption of the cypher text and substitution, the cypher key is in a more secure form.

The decryption is the reverse process of message coding. To decode the message a cypher key is assigned to the Substitution Cipher to decrypt the message. A decrypted key is then assigned to the Base 64 algorithm for the decryption of the ciphertext through the security key Base 64 algorithm, which decrypts the encrypted original message. Fig. 2 describes the process of decryption of the ciphertext and the Substitution Cipher key of text message

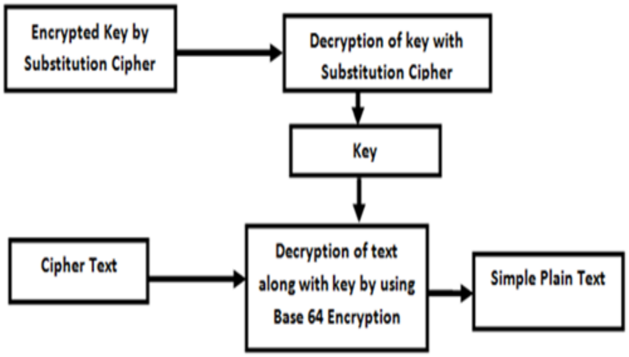
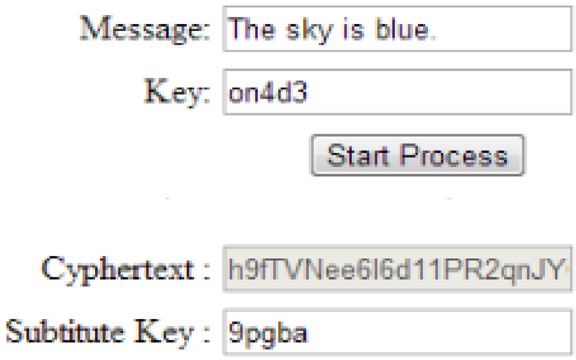

Encrypted Key by Substitution Cipher
Decryption of key with Substitution Cipher
Key
Cipher Text
Decryption of text along with key by using Base 64 Encryption
Simple Plain Text

Fig. 2 Text decryption process using Base 64 algorithm with the combination of Substitute Cipher

The purpose of using Base 64 algorithm and Substitution Cipher in conjunction was to enhance the security level of the information, as existing cryptographic algorithms encrypt the message and send it to the receiver with an encrypted key. If any unauthorized person accesses the key, then he or she can easily compromise the security level by the decryption of the encrypted message. In this developed Optimized Hybrid Security Model, the security key is encrypted twice with the Substitution Cipher, so that the receiver obtains the encrypted message (cipher text) along with the key encrypted by Substitution Cipher. Unauthorized access to the encrypted message and encrypted key would result in the user not being able to decrypt the message because the key will also be encrypted; in which case, no one will be able to decrypt the message because of the encrypted cypher key. In other words, the strength of the developed Hybrid Security Model is based on the fact that after encryption of the message or plain text with Base 64 Substitution Cipher, it is then applied to the security key. As a result, the message cannot easily be decoded as long as the originality of the key is being questioned.

For experimental purposes, the algorithm was developed in Hypertext Preprocessor by using JQuery which created the prototype for the user input of the message and the security key. The developed system is input in plain text as well as the security key. Initially, Base 64 algorithm encodes the text into the secured ciphertext using the security key; then the Substitution Cipher encrypts the key into a substitute cypher secured key. Fig. 3 describes the process of encryption of the message and the security key.


Message: The sky is blue.

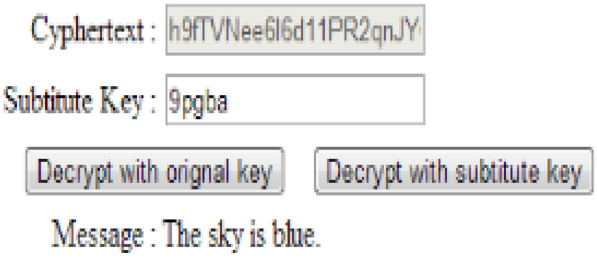
Key: on4d3

Cyphertext : h9fTVNee6l6d11PR2qnJY

Subtitute Key : 9pgba

Fig. 3 The process for encryption of text and security key

For decryption, Substitution Cipher decodes a substitute cypher key and assigns it to Base 64 along with the ciphertext, and Base 64 algorithm decrypts the ciphertext with the security key to generate the original message, as shown in Fig 4.


Cyphertext : h9fTVNee6l6d11PR2qnJY

Subtitute Key : 9pgba

Message : The sky is blue.

Fig. 4 Decryption of cypher text with substitute cypher key the in original text

Over 300 text messages were encrypted for experimental purposes. This research found that the developed prototype was efficient at processing encoding and decoding information with the implementation of two algorithms (Base 64 and Substitution Cipher) as per the expectations of the research objectives. Furthermore, the model accepts input in the numeric, alphanumeric and alphabetic form.

5. Conclusion

This research is aimed at enhancing data integrity. Two security algorithms (Base 64 and Substitution Cipher) were selected to use in conjunction to improve the encryption layer to hide the information. The combination of algorithms (Base 64 algorithm and Substitution Cipher) provided extra protection to the data message. Through Base 64 algorithm, the message was encrypted along with the security key, and then the Substitution Cipher encrypted the security key. Decryption used the reverse process, by firstly decoding the secured key with the

Substitution Cipher and then the Base 64 decrypted the coded message with the security key. If any unauthorised access decrypted the message, the user would need to decrypt the substitution key; without decryption of the security key, it is not possible to decrypt the message.

For the validation of the Optimised Hybrid Security Model, a novel prototype has been developed and tested on sample data. Use of the Base 64 algorithm in conjunction with Substitution Cipher provided enhanced security to the data. The model is reliable for information protection. This research is a step forward when securing short text messages. It can be used to encrypt text between sender and receiver through emails, or it can be integrated to an instant messaging service and used to provide stronger password encryption.

This paper provides a doorstep for the combined use of security algorithms. In this research, we have used only two algorithms for the experiment. By the procedures adopted in this paper, many more algorithms could be used in conjunction to increase the security of valuable information from unauthorised access by hackers and other persons. This Optimised Security Model can be implemented on different platforms to increase the security of information

References

[1] K. Doughty, “Implementing enterprise security: a case study *,” Inf. Syst., pp. 99–114, 2003.

[2] C.-Y. Ku, Y.-W. Chang, and D. C. Yen, “National information security policy and its implementation: A case study in Taiwan,” Telecomm. Policy, vol. 33, no. 7, pp. 371–384, Aug. 2009.

[3] H.-S. Rhee, Y. U. Ryu, and C.-T. Kim, “Unrealistic optimism on information security management,” Comput. Secur., vol. 31, no. 2, pp. 221–232, Mar. 2012.

[4] D. Dang-Pham, S. Pittayachawan, and V. Bruno, “Investigating the Formation of Information Security Climate Perceptions with Social Network Analysis: A Research Proposal,” in 19th Pacific Asia Conference on Information Systems, 2015.

[5] D. L. Nazareth and J. Choi, “A System Dynamics Model for Information Security Management,” Inf. Manag., vol. 52, no. 1, pp. 123–134, Nov. 2014.

[6] Abdullah, M. H. Shah, and W. Ahmed, “Identity theft prevention in online retail organisations: a knowledge sharing framework,” in 4th International Academic Conference in Paris (IACP), 2016, pp. 71–85.

[7] I. Alsmadi, R. Burdwell, A. Aleroud, A. Wahbeh, M. A. Al-Qudah, and A. Al-Omari, “Introduction to Information Security,” in Practical Information Security, Springer, 2018, pp. 1–16.

[8] A. Klaiü and N. Hadjina, “Methods and Tools for the Development of Information Security Policy – A Comparative Literature Review,” pp. 1532–1537, 2011.

[9] P. Eloff, “Information security policy – what do international information security standards say?,” Inf. Secur., pp. 402–409, 2002.

[10] S. Posthumus and R. von Solms, “A framework for the governance of information security,” Comput. Secur., vol. 23, no. 8, pp. 638–646, Dec. 2004.

[11] L. Karadsheh, “Applying security policies and service level agreement to IaaS service model to enhance security and transition,” Comput. Secur., vol. 31, no. 3, pp. 315–326, May 2012.

[12] A. G. Gokce, “The Public Information Systems Security Program,” in International Conference on Information Security, 2012, pp. 352–356.

[13] C. Gu and X. Cao, “Research on information hiding technology,” 2012 2nd Int. Conf. Consum. Electron. Commun. Networks, pp. 2035–2037, Apr. 2012.

[14] E. Shmueli, R. Vaisenberg, E. Gudes, and Y. Elovici, “Implementing a database encryption solution, design and implementation issues,” Comput. Secur., vol. 44, pp. 33–50, Jul. 2014.

[15] B. Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) B. Schneier Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993),” Schneier.com, 1994. [Online]. Available: http://www.schneier.com/paper-blowfish-fse.html. [Accessed: 30-Apr-2012].

[16] D. K. J. Lee, J. Kim, “A Description of the ARIA Encryption Algorithm,” IETF Trust, 2010.

[17] R. Rivest, “A Description of the RC2(r) Encryption Algorithm,” MIT Lab. Comput. Sci. RSA Data Secur. Inc., pp. 1–12, 1998.

[18] S. Kellerman, “Strongest Encryption Algorithm,” 2008. [Online]. Available: http://www.kellermansoftware.com/t-ArticleStrongestAlgo.aspx. [Accessed: 30-Apr-2012].

[19] G. Sumangala, V. R. Kulkarni, S. Sali, and S. Apte, “PERFORMANCE ANALYSIS OF SHA-2 ALGORITHM WITH AND WITHOUT,” World J. Sci. Technol., vol. 1, no. 12, pp. 12–20, 2011.

[20] L. VOCAL Technologies, “SHA-1 and SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) Encryption Algorithm,” 2012. [Online]. Available: http://www.vocal.com/cryptography/sha1.html. [Accessed: 30-Apr-2012].

[21] D. H. Yang, “Base64 Encoding Algorithm,” Data Encodings - Herong’s Tutorial, 2010. [Online]. Available: http://www.herongyang.com/encoding/Base64-Encoding-Algorithm.html. [Accessed: 09-May-2012].

[22] N. Khanna, J. Nath, J. James, S. Chakraborty, A. Chakrabarti, and A. Nath, “New Symmetric Key Cryptographic Algorithm Using Combined Bit Manipulation and MSA Encryption Algorithm: NJJSAA Symmetric Key Algorithm,” 2011 Int. Conf. Commun. Syst. Netw. Technol., pp. 125–130, Jun. 2011.

[23] Z. A. Soomro, M. H. Shah, and J. Ahmed, “Information security management needs more holistic approach: A literature review,” Int. J. Inf. Manage., vol. 36, no. 2, pp. 215–225, Apr. 2016.

[24] H. J. M. Michael E. Whitman, Principles of Information Security, 4th ed. Boston: Course Technology CENGAGE Learning, 2012.

[25] Cisco, “what is network security?,” cisco.com, 2012. [Online]. Available:

http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html. [Accessed: 10-May-2012].

[26] BBC, “BBC - GCSE Bitesize: Key threats to data security,” BBC.COM, 2012. [Online]. Available: http://www.bbc.co.uk/schools/gcsebitesize/ict/databases/6datasecurityrev1.shtml. [Accessed: 10-May-2012].

[27] G. Gürkaynak, I. Yilmaz, and N. P. Taskiran, “Protecting the communication: Data protection and security measures under telecommunications regulations in the digital age,” Comput. Law Secur. Rev., vol. 30, no. 2, pp. 179–189, Apr. 2014.

[28] S. Som and S. Ghosh, “A Simple Algebraic Model based Polyalphabetic Substitution Cipher,” Int. J. Comput. Appl., vol. 39, no. 8, pp. 53–56, Feb. 2012.

Dr. Abdullah Maitlo Assistant Professor, Department of Computer Science, Shah Abdul Latif University Pakistan has done Ph.D. from University of Central Lancashire, UK. His research interests include Cyber Security, Online Business Security, Knowledge Management, Knowledge Economy, and Social Networks Security.

Dr. Rafaqat Hussain Arain has completed his Ph.D. in Computer Science, from University of Electronic Science and Technology of China in 2017. His areas of interest include Image Processing, Machine learning, and Artificial Intelligence. He is serving as Assistant Professor in the Department of Computer Science, Shah Abdul Latif University, Pakistan.

Dr. Riaz Ahmed Shaikh has received his Ph.D. in Computer Science, from University of Electronic Science and Technology of China in 2016. Currently he is working as Assistant Professor in the Department of Computer Science, Shah Abdul Latif University, Pakistan. His research areas include Image Processing, CBIR and Computer Vision.

Dr. Hidayatullah Shaikh has obtained his Ph.D. in Computer Science, from Shah Abdul Latif University Pakistan. Currently he is working as Assistant Professor in the Department of Computer Science, Shah Abdul Latif University, Pakistan. His research areas include Natural Language Processing, Image Processing and Artificial Intelligence.

Dr Mahmood Shah is an internationally known academic in cyber security at the University of Central Lancashire, UK. He has over 15 years’ experience as a consultant to several UK and international banks and online retailers on information security and e-banking management related issues. He has published several high profile books and papers in several high quality Journals. His professional interests include cyber security e-banking, mobile computing, identity theft prevention methods and technology alignment.

Syed Safdar Ali Shah pursuing his Ph.D. in Computer Science, from Shah Abdul Latif University (SALU), Pakistan. He is serving as Computer Programmer in SALU. His area of research is Image Processing.

Dr. Mumtaz Hussain Mahar has completed his Ph.D. from England. Currently he is working as Dean, Faculty of Physical Sciences, Shah Abdul Latif University, Khairpur.