A Hybridized Honey Encryption for Data Security using Residue Number System

Tawakalitu Afoluwaso GIWA[1], Oludare Isaac ABIODUN[1], Abiodun Esther OMOLARA[1], Rafiu Mope ISIAKA[2]
[1] Department of Computer Science, University of Abuja, Gwagwalada, Nigeria
tawakalitu.giwa@uniabuja.edu.ng, oludare.abiodun@uniabuja.edu.ng, esther@uniabuja.edu.ng
[2] Department of Computer Science, Kwara State University, Malete, Nigeria
rafiu.isiaka@kwasu.edu.ng

Abstract

Different encryption algorithms such as Advanced Encryption Standard (AES), Rivest, Shamir, Adleman (RSA) were proposed to protect the privacy of the data. However, most of these existing methods are vulnerable to a brute-force attack because the cipher text remains unintelligible until the original data is found. Consequently, this problem prompted researchers to introduce honey encryption (HE). HE helps to withstand the vulnerability of the encryption algorithms in brute force attacks making transmitted data more secure and efficient. Hence to reduce processing time we proposed a hybridized HE with Residue Number System. Traditional Moduli Set {2n-1, 2n, 2n+1} was used to generate the Key while Chinese Remainder Theorem (CRT), and HE technique were used for decrypting the data, based on the Distribution Transformation Decoder. Thus, anytime an attacker tries to access the data, so long the length of the guessed key is the same as the original key, the HE algorithm will generate meaningful but fake data, this helps to deter an attacker from further threat. The result showed that the proposed system was able to withstand brute force attacks with less processing time compared to other systems. N-values for the moduli set used were varied against encryption and decryption time. Comparing the obtained results with the existing system, the proposed system processing time was faster and more secure.

Index terms: security and privacy, data protection, honey encryption, distribution transformation encoder, residue number system, moduli set, Chinese remainder theorem

References

[1]. A. N. Babatunde, G. R. Jimoh and K. A. Gbolagade, "An algorithm of residue Number System Based Video Encryption System," Anale.seria Informatica Vol. XIV Fasc.2-2016. Annals. computer Science 14th Tome @nd fasc - 2016, p. 1, 2016.

[2]. S. Ansari and R. Sahu, "A Secure Framework for Messaging on Android Devices with Honey Encryption," International Journal Of Engineering And Computer Science, ISSN:2319-7242, Volume 6, Issue 9, September 2017, Page No. 22480, Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i9.1522485, p. 34, 2017.

[3]. E. Mok, A. Samsudin and S.-F. Tan, "Implementing the Honey Encryption for Securing," School of Computer Sciences, Universiti Sains Malaysia, Penang, 11800, Malaysia, Malaysia, 2017.

[4]. S. Murty and P. M. Mulchandani, "Improving Security of Honey Encryption in Database: Implementation," International Conference on Science and Engineering for Sustainable Development (ICSESD-2017) (www.jit.org.in) International Journal of Advanced Engineering, Management and Science (IJAEMS) Special Issue-3, ISSN: 2454-1311, p. 34, 2017.

[5]. A. Juels and T. Ristenpart, "Honey Encryption: Security Beyond the Brute-Force Bound," University of Wisconsin February 28, 2014, Version 1.2, p. 36, 2014.

[6]. I. A. Aremu and K. A. Gbolagade, "An Overview of Residue Number System," International Journal of Advanced research in omputer Engineering and Technology (IJARCET), Volume 6, Isssue 10, October 2017, ISSN: 2278 - 1323, p. 26, 2017.

[7]. S. Alhassan and K. Gbolagade, "Enhancement of the Security of a Digital Image using the Moduli Set {2n -1, 2n, 2n + 1}," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 7, July 2013, ISSN: 2278 – 1323, p. 36, 2013.

[8]. B. A. Weyori, S. A. Akobre and G. K. Armah, "Application of RNS to Huffman's method of Secured data Encryption Algorithm," International Journal of Soft computing 4(5): 197 - 200, 2009, ISSN: 1816 - 9503, p. 38, 2009.

[9]. T. Giwa, "XYZ of computing," AB journal of info tech, pp. 1-8, 2020.

[10]. N. Babatunde, "An algorithm for a Residue Number System Based Video Encryption System," 2018.

[11]. A. J. A. T. Ristenpart, "Honey Encryption: Security beyond the Brute-Force Bound," 2014.

[12]. T. Win and K. S. M. Moe, "Protecting Private Data using Improved Honey Encryption and Honeywords Generation Algorithm," Advances in Science, Technology and Engineering Systems Journal, Vol. 3, No. 5, 311-320 (2018), ASTESJ, ISSN: 2415 - 6698, p. 33, 2018.

[13]. R. Sahu and M. S. Ansari, "Securing Messages from Brute Force Attack by Combined Approach of Honey Encryption and Blowfish," International Research Journal of Engineering and Technology (IRJET), Volume: 04, Issue: 09 | Sep -2017 e-ISSN: 2395-0056v, p. 35, 2017.

[14]. V. Hema and M. G. Durga, "Data Integrity Checking Based On Residue Number System and Chinese Remainder Theorem In Cloud," International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014, 2014 International Conference on Innovations in Engineering and Technology (ICIET'14) ISSN (Online): 2319 - 8753, p. 36, 2014.

[15]. A. Azizifard, M. Qermezkon and R. Farshidi, "Information Steganography within 3D Images Using Residue Number System," Postgraduate, Department of agriculture on agronomy, Dezfoul Branch, Islamic Azad university, Dezfoul, Iran, Dezfoul, 2013.

[16]. E. A. Omolara and A. Janlan, "Modified Honey Encryption Scheme for Encoding Language.," International Journal of Electrical and Computer Engineering Volume 9(3). Doi: 10:11501/ijece. vp13.pp 1871-1878, 2018.

[17]. H. A. B. A. N. R. M. Seddeq E. Ghrare, "New Text Encryption Method Based on Hidden Encrypted System," Department of Electrical and Computer Engineering, Faculty of Engineering, University of Gharyan, P.O Box 64418 Gharyan-Libya, p. 15, 2018.

[18]. S. E. Ghrare, H. A. Barghi and N. R. Madi, "New Text Encryption method Based on Hidden Encryption System," Department of Electrical and Computer Engineering, Faculty of Engineering, University of Gharyan, P.O Box 64418 Gharyan-Libya, p. 15, 2018.

[19]. H. K. Bello and K. A. Gbolagade, "An Efficient CRT Based Reverse Converter for {2^2n+1 - 1, 2^n-1,2^2n -1} Moduli set," Journal of Advanced mathematics and Computer Science 26(6: 1-9, 2017; Article no. JAMCS>38517 ISSN:2456-9968), p. 27, 2017.

[20]. D. D. Popoola, "Data Integrity using Ceaser Cipher and Residue Number System," ProQuest, Kwara state university (Nigeria), Proquest Dissertations Publishing, 2019 13897657, p. 48, 2019.

[21]. P. Dharshini, R. J. Arokia and K. Mohan, "Screening the covert key using honey encryption to rule out the brute force attack of AES," published online 3 February 2017 in Wiley online library (wileyonlinelibrary.com) DOI: 10.1002/sec.1753, 2017.

[22]. S. Geric and Z. Hutinsk, "Information System Security threats classifications," University of Zagreb, Faculty of organization and informatics, Varazdin, Croatia, 2007.

[23]. J. Kent and k. Steiner, "Ten Ways to Improve the Security," US-CERT, United states computer emergency readinesss team, 2015.

[24]. R. Lindholm and A. Costin, "Honey Encryption: Implementation Challenges and Solution," Master's Thesis in Information Technology, University of Jyvaskgla, Faculty of Information Technology, Jyvaskgla, 2019.

[25]. K. H. Bello and A. K. Gbolagade, "An Efficient CRT Based Reverse Converter for," Journal of Advances in Mathematics and Computer Science,25(6): 1-9, 2017; Article no. JAMCS.38517, (Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851), p. 26, 2017.

[26]. N. Stamenkovie, B. Jovanovie and V. Stojanovie, "An Improved Residue Number to Binary Converter Based on Mixed Radix Conversion for the Moduli Set," 2010.

[27]. W. Yin, J. Indulska and H. Zhou, "Protecting Private data by Honey Encryption," Hindawi Security and Communication Networks Volume 2017, Article ID 6760532, 9 pages | https://doi.org/10.1155/2017/6760532.North China Institute of Computing Technology, Beijing, China2School of ITEE, University of Queensland, Brisbane, QLD, Australia, 2017.

[28]. C. Adams, G. V. Jourdan, J.-P. L. Levac, and F. Prevost, "Lightweight protection against brute force login," in DOI: 10.1109/PST. 2010 559324/ Source: IEEE Xplore, 2010 Eighth Annual International Conference on Privacy, Security and Trust, Ottawa, 2010.

[29]. A. E. Omolara, A. Jantan and O. I. Abiodun, "A comprehensive review of Honey Encryption Scheme," Indonesian Journal of Electrical Engineering and Computer

Science. Volume 13, Issue 2, page 649-656. ISSN: 2502, DOI: 10.1159/ijeecs.viz.12, pp. 649, 656, p. 33, 2019.

[30]. S. M. Ansari and R. Sahu, "Securing messages from Brute force attack by combined approach of Honey Encryption and blowfish," International Research Journal of Engineering and Technology (IRJET), Volume: 04, Issue: 09/sep-2017, e-ISSN: 2395-0056, p-ISSN: 2395-0072, p. 21, 2017.

[31]. R. Vaidya, "Cyber Security Breaches Survey," 2019.

[32]. E. A. Omolara and A. Janlan, "Modified Honey Encryption Scheme for Encoding Language.," International Journal of Electrical and Computer Engineering Volume 9(3). DOI: 10:11501/ijece. Vol. 13. pp.1871-1878, 2018.

[33]. Breithaupt and M. S. Merkow, Information Security: Principles and Practices, 2nd Edition, USA: PEARSON, 800 East 96th Street, Indianapolis, Indiana 46240 USA, 2014.

[34]. Y. Parwej, Q. Abbas, J.P.D. Dixit, N. Akhtar, and A.K. Jaiswal, "A Systematic Literature Review on the Cyber Security," International Journal of Scientific Research and Management, Volume 9 (Issue 12), ISSN: 2321-3418, 2021.

[35]. O.I Abiodun, M. Alawida, E.S. Omolara, A. Abdulatif, "Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey," Journal of King Saud University - Department of Computer and Information Science, Volume 34, Issue 10, part B, 2022.

[36]. Ayushi, "A Symmetric Key Cryptographic Algorithm," International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15, 2010.

[37]. K.L. Panchal, "Differential Privacy and Natural Language Processing to Generate Contextually Similar Decoy Messages in Honey Encryption Scheme," University of Massachusetts, 2020.

[38]. T. Soofun, A. Samsudin, "Enhanced Security of Internet Banking Authentication with EXtended Honey Encryption (XHE) Scheme," Innovative Computing, Optimization and Its Applications, 2018.