A New Data Communication Method Using RSA and Steganography

Varun Shukla, Manoj Kumar Misra, Shivani Dixit, and Himanshu Dhumras

1 Introduction

Information exchange is an inseparable part in modern life. The security of information is a key term. Cryptography is all about keeping data secure. Cryptography provides various security categories such as confidentiality, authentication, data integrity and non-repudiation, and they are called as goals of information security or classic goals of cryptography as shown below in Fig. 1 [1–5].

On the other hand, steganography is used to hide the presence of message. Steganography hides the text message in a carrier file. The carrier file can be an image, sound file or a video file. The aim of steganography is also to safeguard information and hence steganography is always seen as a supporting tool of cryptography [6, 7]. A basic comparison between steganography and cryptography is shown in Fig. 2.

The remaining part of this paper is organized as follows: The proposed method is given in Sect. 2. Security analysis and advantages are discussed in Sect. 3. Conclusion and future scope are given in Sect. 4.

V. Shukla · S. Dixit
Department of ECE, Pranveer Singh Institute of Technology, Kanpur, India

M. K. Misra (✉)
Department of CSE, Pranveer Singh Institute of Technology, Kanpur, India
e-mail: manojmisra12@gmail.com

H. Dhumras
Department of Mathematics, Jaypee University of Information Technology, Waknaghat, India

B. K. Roy et al. (eds.), *Cryptology and Network Security with Machine Learning*,
Algorithms for Intelligent Systems, https://doi.org/10.1007/978-981-99-2229-1_19

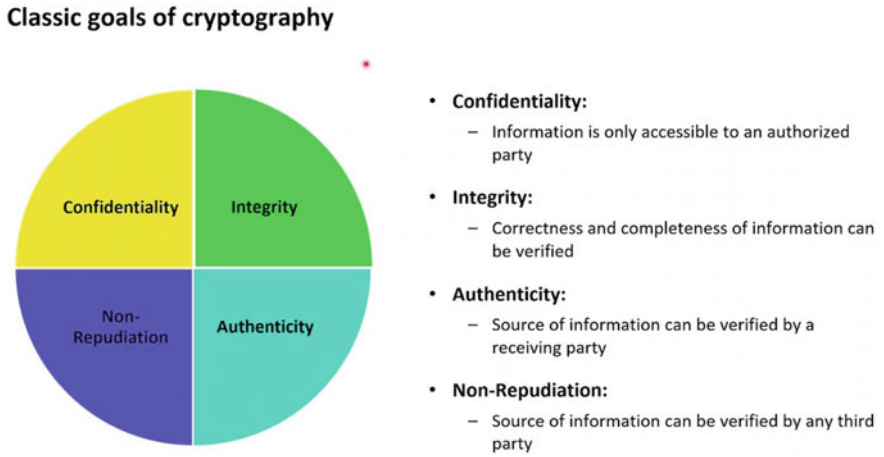

Fig. 1 Goals of information security

	Cryptography	Steganography
Application	Secret communication using scrambled information	Secret communication using hidden information
Supported data	Text	Digital medium (e.g., Text, audio, image, video)
Secret key type	Single (private) Double keys (public)	Single (private)
Key size importance	Critical	Moderate
Processing time	Part of the roundtrip delay	Add processing time to the roundtrip delay
Usage	All communications types	Dependent on payload capacity
Human perception	Visible but unreadable	Invisible/Inaudible
Machine based attack	Cryptanalysis	Steganalysis
Attack result	Secret information recovered	Secret communication detected

Fig. 2 Basic comparison between cryptography and steganography

2 Proposed Method

Step 1: In the first step of the proposed method, RSA is used to generate the cipher text [8, 9]. For RSA, we need two prime numbers p and q and $n = pq$. We calculate

$$\varphi(n) = (p-1) \times (q-1).$$

The public key is $\{e, n\}$ and the private key is $\{d, n\}$ where $ed\ mod \varphi(n) = 1$. If the plain text is represented by m and cipher text is given as c then $c = m^e mod\ n$ and $m = c^d mod\ n$. We show the readings in Table 1. These readings are only for illustration point of view but user can extend the values of p and q and then the corresponding parameters will also be changed. The security of RSA algorithm is based on the selection of p and q, and these prime numbers must be large enough for security. So the proposed method provides this flexibility that user can select the large prime numbers also.

Step 2: In the second step, the generated cipher text is kept inside the carrier image (the process of steganography). The selected cipher text and carrier image are shown in Figs. 3 and 4, respectively.

Now the cipher text is kept inside the carrier image so that intruder never knows the presence of cipher text. Since only receiver knows it, he or she will be able to extract the data from the embedded output [10–12]. The comparison of carrier image and embedded output is shown in Fig. 5, and the histogram comparison is also shown in Fig. 6 to prove that both the images look exactly the same.

3 Security Analysis and Advantages

- **Security of RSA**: The proposed method utilizes RSA algorithm for the generation of cipher text. RSA is the most trusted Public Key Cryptosystem (PKC) and its security is still trusted [13, 14]. The large values of prime numbers p and q will make sure that the generated cipher text remains secure from intruders.
- **Usage of steganography**: The use of steganography makes sure that intruders will have no idea about the cipher text. RSA secures the plain text but steganography makes the cipher text invisible. So steganography acts as a second layer of security for the proposed method. User can select any image of his choice as carrier image and generate the corresponding embedded output.
- **Hybrid method**: The proposed method is a combination of cryptography and steganography [15, 16]. Suppose the level of security provided by RSA is A and steganography is B then the overall level of security of the proposed method will be $A + B$. The benefit of using steganography is that the presence of cipher text remains unknown to intruders.

Table 1 Showing readings of the proposed method

Plain text	S.N	p	q	$n = p \times q$	$\varphi(n) = (p-1) \times (q-1)$	e	d	Cipher text
Hello Alice let us share a secret number	1	11	13	143	120	7	103	91 62 4 4 45 98 59 4 118 44 62 98 4 62 129 98 39 80 98 80 91 59 49 62 98 59 98 80 62 44 49 62 129 98 33 39 21 32 62 49
	2	17	19	323	288	5	173	168 271 109 109 42 223 241 109 22 131 271 223 109 271 165 223 53 115 223 115 168 241 190 271 223 241 223 115 271 131 190 271 165 223 230 53 181 319 271 190
	3	23	29	667	616	3	411	302 453 416 416 281 85 217 416 380 481 453 85 416 453 116 85 146 115 85 115 302 217 137 453 85 217 85 115 453 481 137 453 116 85 335 146 382 55 453 137

302 453 416 416 281 85 217 416 380 481 453 85 416 453 116 85 146 115 85 115
302 217 137 453 85 217 85 115 453 481 137 453 116 85 335 146 382 55 453 137

Fig. 3 Showing the selected cipher text

- **Innovative method**: Many security methods have been presented till now using PKCs but the proposed method is a combination of PKC with steganography which is quite unique. This unique combination will show the new direction of research, and it will provide safe and reliable data communication in various applications.
- **Customized method**: The proposed method is customized from user's perspective. User can select prime numbers of his own choice. User can also select the carrier image. Any plain text message can be encrypted and kept inside the carrier image which will produce embedded output. User can select any prime numbers based on the required level of security.

Fig. 4 Showing the carrier image

Fig. 5 Showing comparison of carrier image (left) and embedded output (right)

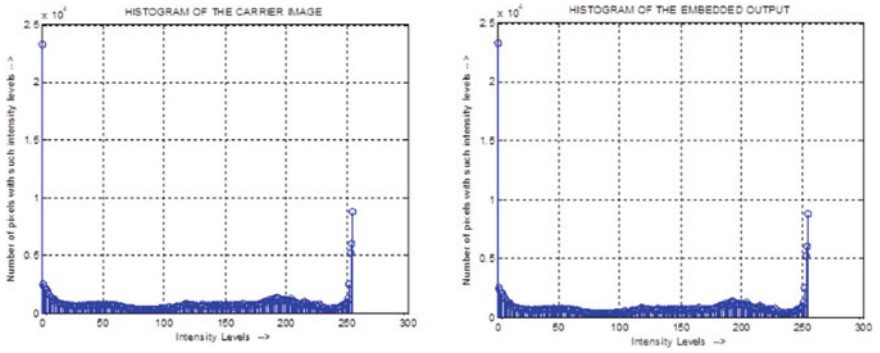

Fig. 6 Showing histogram comparison of carrier image (left) and embedded output (right)

- **Useful in various applications**: The proposed method is a general method that provides strong encryption and then hides the presence of the cipher text using steganography. The proposed method can be used in all those applications where data communication security is vital. The examples can be financial transactions, passing military messages, Electronic Health Records (EHR), e-commerce application, etc. [17–19]. Various password strategies can also be implemented to make the proposed method more secure [20, 21].
- **Resistive against brute force**: The proposed method uses RSA encryption which is resistive against brute force attack. Proper selection of key size makes sure that intruders will not be able to search all the possible combinations in feasible time duration. As an additional security measurement, the presence of cipher text is also hidden which enhances the insurance that intruders will not launch brute force because they don't know about the existence of cipher text.
- **Resistive against DoS**: In Denial of Service (DoS) attack, the intruder intentionally disrupts the ongoing services because they know that communication is going on in an encrypted fashion but in the proposed method, the presence of cipher text is hidden. So intruders will never think of launching DoS [22, 23].
- **Resistive against MITM**: Man in the Middle Attack (MITM) is very dangerous for communication protocols but it is not applicable in the proposed method. RSA itself is resistive against MITM and even if any possibility of MITM is there, it will be nullified by the generated embedded output which hides the cipher text. Since only transmitter and receiver know about the hidden cipher text, there is no question about MITM [24–28].
- **Easily implementable**: The proposed method is easily implementable in various platforms. Mobile apps can also be developed where user needs to select prime numbers and carrier image of his choice and the hidden encrypted message will be transmitted. No additional memory or hardware requirements are needed for the implementation of proposed method. Various hash mechanisms can also be incorporated specifically when the proposed method is used for financial transactions [29–31] or any other-related applications [32–41].

4 Conclusion and Future Scope

An innovative data communication method using RSA and steganography is presented in this paper. The proposed method generates the cipher text using RSA and the cipher text is kept inside the carrier image and embedded output is produced. The carrier image and embedded output look exactly the same, and intruder will not be able to find any difference. The method is an innovative hybrid method and resistive against various well-known security attacks such as brute force, DoS, MITM, etc. The method is easily implementable and can be used in a variety of applications. The future extension of the proposed method is also possible as other encryption algorithms instead of RSA can be used. Similarly, other innovative steganographic procedures can also be applied in order to increase difficulty for intruders.

Acknowledgements The authors thank the editor and the anonymous reviewers for reviewing this article and providing valuable and kind suggestions.

Conflict of Interest The authors declare no competing interests.

References

1. Menezes AJ, Oorschot PCV, Vanstone SA (2001) Handbook of applied cryptography, 5th edn. CRC Press Inc, USA, ISBN: 9780849385230
2. Stallings W (2005) Cryptography and network security, principles and practices, 7th edn. Prentice Hall, ISBN-13:978-0134444284, ISBN-10:0134444280
3. Shukla V, Chaturvedi A, Srivastava N (2019) Nanotechnology and cryptographic protocols: issues and possible solutions. Nanomater Energy 8(1):1–6. https://doi.org/10.1680/jnaen.18.00006
4. Shukla V, Chaturvedi A, Srivastava N (2019) A secure stop and wait communication protocol for disturbed networks. Wirel Pers Commun 110:861–872. https://doi.org/10.1007/s11277-019-06760-w
5. Shukla V, Srivastava N, Chaturvedi A (2016) A bit commitment signcryption protocol for wireless transport layer security (wtls). In: IEEE international conference on electrical, computer and electronics engineering, pp 83–86. https://doi.org/10.1109/UPCON.2016.7894629
6. Subramanian N, Elharrouss O, Maadeed SA, Bouridane A (2021) Image steganography: a review of the recent advances. IEEE Access 9:23409–23423. https://doi.org/10.1109/ACCESS.2021.3053998
7. Shukla V, Mishra A (2020) A new sequential coding method for secure data communication. In: IEEE international conference on computing, power and communication technologies, pp 529–533. https://doi.org/10.1109/GUCON48875.2020.9231252
8. Zhou X, Tang X (2011) Research and implementation of RSA algorithm for encryption and decryption. In: Proceedings of 6th international forum on strategic technology, pp 1118–1121. https://doi.org/10.1109/IFOST.2011.6021216
9. Kaabi SSA, Belhaouari SB (2019) Methods toward enhancing RSA algorithm: a survey. Int J Netw Secur Appl 11(3):53–70. https://doi.org/10.5121/ijnsa.2019.11305
10. Maniriho P, Ahmad T (2019) Information hiding scheme for digital images using difference expansion and modulus function. J King Saud Univ Comput Inf Sci 31(3):335–347. https://doi.org/10.1016/j.jksuci.2018.01.011
11. Attaby AA, Ahmed MFMM, Alsammak AK (2018) Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3. Ain Shams Eng J 9(4):1965–1974. https://doi.org/10.1016/j.asej.2017.02.003
12. Chaturvedi A, Shukla V, Misra MK (2021) A random encoding method for secure data communication: an extension of sequential coding. J Discr Math Sci Cryptogr 24(5):1189–1204. https://doi.org/10.1080/09720529.2021.1932902
13. Kaur J, Ramkumar KR (2021) The recent trends in cyber security: a review. J King Saud Univ Comput Inf Sci. https://doi.org/10.1016/j.jksuci.2021.01.018
14. Hassan MA, Shukur Z, Hasan MK (2020) An efficient secure electronic payment system for e-commerce. Computers 9(3):1–13. https://doi.org/10.3390/computers9030066
15. Taha MS, Rahim MSM, Lafta SA, Hashim MM, Alzuabidi HM (2019) Combination of steganography and cryptography: a short survey. IOP Conf Ser Mater Sci Eng 518(5):1–13. https://doi.org/10.1088/1757-899X/518/5/052003
16. Jan A, Parah SA, Hussan M, Malik BA (2021) Double layer security using crypto-stego techniques: a comprehensive review. Health Technol 1–23. https://doi.org/10.1007/s12553-021-00602-1

17. Shukla V, Chaturvedi A, Srivastava N (2015) A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography. Commun Appl Electron 3(3):16–21. https://doi.org/10.5120/cae2015651903
18. Misra MK, Chaturvedi A, Tripathi SP, Shukla V (2019) A unique key sharing protocol among three users using non-commutative group for electronic health record system. J Discr Math Sci Cryptogr 22(8):1435–1451. https://doi.org/10.1080/09720529.2019.1692450
19. Chaturvedi A, Srivastava N, Shukla V, Tripathi SP, Misra MK (2015) A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks. Int J Comput Appl 128(2):36–39. https://doi.org/10.5120/ijca2015906437
20. Shukla V, Chaturvedi A, Srivastava N (2019) A new one time password mechanism for client-server applications. J Discr Math Sci Cryptogr 22:1393–1406. https://doi.org/10.1080/09720529.2019.1692447
21. Zviran M, Haga WJ (1999) Password security: an empirical study. J Manage Inf Syst 15(4):161–185. https://www.jstor.org/stable/40398409
22. Yang ZC (2011) DOS attack analysis and study of new measures to prevent. In: International conference on intelligence science and information engineering, pp 426–429. https://doi.org/10.1109/ISIE.2011.66
23. Mahjabin T, Xiao Y, Sun G, Jiang W (2017) A survey of distributed denial-of-service attack, prevention, and mitigation techniques. Int J Distrib Sens Netw 13(12):1–34. https://doi.org/10.1177/1550147717741463
24. Aliyu F, Sheltami T, Shakshuki EM (2018) A detection and prevention technique for man in the middle attack in fog computing. Proc Comput Sci 141:24–31. https://doi.org/10.1016/j.procs.2018.10.125
25. Conti M, Dragoni N, Lesyk V (2016) A survey of man in the middle attacks. IEEE Commun Surv Tutor 18(3):2027–2051. https://doi.org/10.1109/COMST.2016.2548426
26. Chaturvedi A, Srivastava N, Shukla V (2015) A secure wireless communication protocol using Diffie-Hellman key exchange. Int J Comput Appl 126(5):35–38. https://doi.org/10.5120/ijca2015906060
27. Shukla V, Chaturvedi A, Misra MK (2021) On authentication schemes using polynomials over non commutative rings. Wirel Pers Commun 118(1):1–9. https://doi.org/10.1007/s11277-020-08008-4
28. Mallik A, Ahsan A, Shahadat MMZ, Tsou JC (2019) Man-in-the-middle-attack: understanding in simple words. Int J Data Netw Sci 3(2):77–92. https://doi.org/10.5267/j.ijdns.2019.1.001
29. Shukla V, Misra MK, Chaturvedi A (2021) A new authentication procedure for client-server applications using HMAC. J Discr Math Sci Cryptogr 24(5):1241–1256. https://doi.org/10.1080/09720529.2021.1932908
30. Shukla V, Chaturvedi A, Srivastava N (2019) Authentication aspects of dynamic routing protocols: associated problem & proposed solution. Int J Recent Technol Eng 8(2):412–419. https://doi.org/10.35940/ijrte.B1503.078219
31. Shukla V, Mishra A, Agarwal S (2020) A new one time password generation method for financial transactions with randomness analysis. Innovations in electrical and electronic engineering (Part of the lecture notes in electrical engineering book series (LNEE, vol 661)), pp 713–720. https://doi.org/10.1007/978-981-15-4692-1_54
32. Shukla V, Mishra A, Yadav A (2019) An authenticated and secure electronic health record system. In: IEEE international conference on information and communication technology, pp 1–5. https://doi.org/10.1109/CICT48419.2019.9066168
33. Chaturvedi A, Shukla V, Misra MK (2018) Three party key sharing protocol using polynomial rings. In: 5th IEEE Uttar Pradesh section international conference on electrical, electronics and computer engineering (UPCON), pp 1–5. https://doi.org/10.1109/UPCON.2018.8596905
34. Shukla V, Chaturvedi A, Srivastava N (2017) Secure wireless communication protocol: to avoid vulnerabilities in shared authentication. Commun Appl Electron 7(6):4–7. https://doi.org/10.5120/cae2017652680
35. Shukla V, Misra MK, Chaturvedi A (2022) Journey of cryptocurrency in India in view of financial budget 2022–23. Cornell university arxiv, pp 1–6. https://doi.org/10.48550/arXiv.2203.12606

36. Chaturvedi A, Shukla V (2020) Miracle of number theory. Everyman's Sci 50(3–4):131–134. http://www.sciencecongress.nic.in/pdf/e-book/august_nov_2020.pdf
37. Shukla V, Chaturvedi A (2018) Cryptocurrency: characteristics and future perspectives, vol 53, number 2, pp 77–80. http://164.100.161.164/pdf/e-book/june-july-18.pdf#page=14
38. Shukla V, Kushwaha A, Parihar SS, Srivastava S, Singh VP (2016) Authenticated wireless information display system using GSM module. Commun Appl Electron 5(3):7–11. https://doi.org/10.5120/cae2016652251
39. Shukla V, Chaturvedi A, Srivastava N (2017) Double layer cryptographic protocol for mobile ad-hoc networks (MANETs) by commitment scheme. Commun Appl Electron 7(9):32–36. https://doi.org/10.5120/cae2017652716
40. Shukla V, Dixit S, Dixit P (2022) An IoT based user authenticated soil monitoring system. Adhoc Sensor Wirel Netw 53(3–4):269–283. https://doi.org/10.32908/ahswn.v53.9453
41. Chaturvedi A, Shukla V, Srivastava N (2017) A secure wireless peer to peer authentication protocol using triple decomposition problem. Asian J Math Comput Res 22(2):63–69. https://archives.biciconference.co.in/index.php/AJOMCOR/article/view/1167