JOURNAL OF SOUTHERN COMMUNICATION ENGINEERING
ISLAMIC AZAD UNIVERSITY BUSHEHR BRANCH
E-ISSN: 2980-9231
https://jce.bushehr.iau.ir
https://doi.org/...

Vol. x/ No. x/Spring 2024

Research Article

A New DNA Cryptosystem for Encrypting Persian Texts and Images with Key Exchange based on Hyper Elliptic Curve

Fatemeh Alidadi Shamsabadi, MSc[1] | Shaghayegh Bakhtiari Chehelcheshmeh, Assistant Professor[2*] | Narges Farhadi, MSc[3]

[1]MSc., Department of Computer, Faculty of Engineering, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran, fatemehalidadi53@yahoo.com

[2]Assistant Professor, Department of Computer, Faculty of Engineering, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran, sh.bakhtiari@iaushk.ac.ir

[3]MSc., Department of Computer, Faculty of Engineering, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran, n.farhadi705@gmail.com

Correspondence
Shaghayegh Bakhtiari Chehelcheshmeh, Assistant Professor, Department of Computer, Faculty of Engineering, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran, sh.bakhtiari@iaushk.ac.ir

Received: 16 December 2023
Revised: 28 January 2024
Accepted: 31 January 2024

Abstract

With the emergence of quantum computers, traditional cryptography methods will be broken and lose their efficiency. Fortunately, DNA-based cryptography methods have high resistance against quantum attacks. However, these methods have not yet been used to secure Persian texts. On the other hand, DNA encryption methods require a secure communication channel for sharing the secret key. Therefore, in this paper, a new cryptosystem is presented to provide confidentiality of Persian texts based on DNA cryptography. Also, considering the widespread use of images in public media, the ability to encrypt images is also embedded in this scheme. In the proposed method, the hyper-elliptic curve cryptography (HECC) system is used to generate a shared secret key on both sides of communication so that there is no longer a need for a secure channel. Also, DNA hybridization technology is used to perform encryption and decryption of the message to minimize the time complexity of the cryptography algorithm. According to the results of the performance evaluation, the proposed scheme reduces the computational overhead and has lower energy consumption compared to previous schemes.

Keywords: Security, HEC Key Agreement, DNA Cryptography, Persian Plaintexts, DNA Hybridization.

Highlights

- Encryption of Persian texts using a DNA cryptography system for the first time.
- Providing a large key space to increase resistance against external factors.
- Minimizing time complexity using DNA hybridization technology.
- No need for a secure channel for key sharing.
- Highly secure and efficient key agreement using encryption based on hyper-elliptic curve.

Citation: [in Persian].