World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:17, No:01, 2023

The Effectiveness of a Hybrid Diffie-Hellman-RSA-Advanced Encryption Standard Model

Authors : Abdellahi Cheikh

Abstract : With the emergence of quantum computers with very powerful capabilities, the security of the exchange of shared keys between two interlocutors poses a big problem in terms of the rapid development of technologies such as computing power and computing speed. Therefore, the Diffie-Hellmann (DH) algorithm is more vulnerable than ever. No mechanism guarantees the security of the key exchange, so if an intermediary manages to intercept it, it is easy to intercept. In this regard, several studies have been conducted to improve the security of key exchange between two interlocutors, which has led to interesting results. The modification made on our model Diffie-Hellman-RSA-AES (DRA), which encrypts the information exchanged between two users using the three-encryption algorithms DH, RSA and AES, by using stenographic photos to hide the contents of the p, g and ClesAES values that are sent in an unencrypted state at the level of DRA model to calculate each user's public key. This work includes a comparative study between the DRA model and all existing solutions, as well as the modification made to this model, with an emphasis on the aspect of reliability in terms of security. This study presents a simulation to demonstrate the effectiveness of the modification made to the DRA model. The obtained results show that our model has a security advantage over the existing solution, so we made these changes to reinforce the security of the DRA model.

Keywords : Diffie-Hellmann, DRA, RSA, advanced encryption standard
Conference Title : ICCNM 2023 : International Conference on Calculus and Numerical Methods
Conference Location : New York, United States
Conference Dates : January 30-31, 2023