IMPLEMENTATION OF THE MERKLE HELLMAN ALGORITHM FOR TEXT DATA SECURITY

DODI SETIAWAN
Informatics Study Program, Faculty of Science & Technology
University of Technology Yogyakarta
Jl. Ringroad Utara Jombor Sleman Yoyakarta
E-mai : dodisetiawan062@gmail.com

ABSTRACT

The development of information technology today has a very large impact and problems in the form of data security and confidentiality. One solution that can be used to ensure the confidentiality and security of information is cryptography. By using cryptography, data can be secured through encryption and description processes. The issue of data security and confidentiality is the most important aspect of an information system. One mechanism to improve security is to use asymmetric algorithms such as the Merkle Hellmen algorithm. Merkle Hellman is a crypto system that uses an asymmetric key type. In the Merkle Hellman system, the keys used are 2 different keys, namely the public key and the secret key. Encryption produces ciphertext and description produces plain text to secure data that you want to keep secret. The advantage of the Merkle Hellman algorithm is that there is no need for confidentiality in the key distribution process. From the results of experiments that have been carried out with this application, the encrypted data is in the form of an incomprehensible message (ciphertext), but after the description process is carried out, the data is successfully returned to its original form (plaintext) that can be understood.

Keywords: Cryptography, Data, Merkle Hellman