Suggesting a System to Decipher Cipher Text using Cryptography and Information Security for Sri Lankan Military

A Wickramasinghe, IA Wijethunga

Department of Computer Science, Faculty of Computing, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka

The motive to illegally decrypt encrypted messages could be for economic, security, or political reasons. Finding a secured way of protecting ciphertexts from being stolen and revealed, has been very challenging for existing cryptographic researchers. Data security guarantees that only the intended recipient can view our data and prohibits any change or alteration of the data. Various algorithms and methods have been developed to achieve this level of safety. Data Encryption is one current protocol for securing information, particularly during end-to-end communication through computer networks. This paper mainly discusses the methods of converting cipher text into plain text and the period of key validation. One of the latest technologies in this area is Homomorphic Encryption conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form.

Keywords: *Military, Decipher, Cryptography*