Voice Mail Encryption Using International Data Encryption Algorithm (IDEA)


Abstract:

Nowadays, Electronic Voice Mail Services (EVMS) encryption is an area of a great interest due to the wide spreading of communication networks. If voice or some other analog signal must be conveyed with a high level of security then it should be digitized (A/D converted) and digitally encrypted. In the past, the digitization process was expensive so that analog scramblers found a place in the security business because of their lower cost and lower bandwidth requirements. The International Data Encryption Algorithm (IDEA) is one of the most secure block-ciphering algorithm. The key length of IDEA is 128 bits, which is hard to be broken with exhaustive search. There are no Substitution Code Boxes (S-boxes) in IDEA. Instead, there is a logical function that is especially designed in order to make the encryption algorithm itself the decryption algorithm, with another key. This means that the IDEA is asymmetric algorithm. This paper presents a study of using IDEA for speech encryption.