

ABSTRACT

Currently, digital media security especially in wav sound file is very important to be kept confidential. This has to do with copyright. For that developed a method that aims to randomize wav sound file, so it can not be manipulated and falsified by others who are not interested.

The encryption method is one kind of safety data, one using the RC4 algorithm. RC4 uses a key length from 1 to 256 bits are used to initialize the table along 256 bits. RC4 has an S-Box, S0, S1,, S255, which contains a permutation of the numbers 0 to 255. Using two indices i and j in the algorithm. Index i is used to ensure that an element changed, while the index j will ensure that an element changed randomly. Essentially, the algorithm encryption method will generate pseudorandom bytes of key XOR operation will be subject to the plaintext to produce the ciphertext. And to produce the original plaintext, the ciphertext it will be subject to the pseudorandom byte XOR operation her.

From testing research on the application of the RC4 algorithm wav sound files obtained some results. First, the greater the capacity wav sound files are processed, the longer it takes. Because, the larger the file size, then the contents of pengacakkan wav sound files will also be longer. Second, the keys used in the encryption and decryption must be the same or symmetry. Third, the capacity of the file before and after the change are not encrypted.

Keywords: Cryptography, the RC4 algorithm, wav format sound files