

Abstrak

Komunikasi merupakan hal yang sangat umum dilakukan oleh siapa saja, baik itu komunikasi dalam bentuk langsung maupun tidak langsung. Tentu saja, keamanan pada komunikasi tersebut perlu dipastikan. Pada keamanan untuk komunikasi langsung, keamanan komunikasi tersebut dapat dengan mudah dijaga dengan mudah dengan memastikan tidak ada yang mendengar pesan lisan selain penerima pesan tersebut. Di sisi lain, pada keamanan untuk komunikasi tidak langsung, keamanan dapat dijaga dengan berbagai macam bentuk. Misalnya, ketika mengirim pesan dalam bentuk *file* teks. Informasi dapat diamankan dengan teknik kriptografi dan mengubah format *file*-nya, contohnya dari *file* teks diubah formatnya ke format *file* lain, seperti file .mid. Pada perangkat lunak ini, teknik kriptografi dilakukan dengan enkripsi simetris. Kemudian, konversi antar bentuk *file* menyembunyikan pesan di *file* MIDI. Pastinya, perangkat lunak kehilangan fungsinya jika tidak bisa mengembalikan pesan tersembunyi yang ada di dalam *file* MIDI. Maka perangkat lunak dapat membalikkan pesan tersembunyi tersebut. Dari pesan tersembunyi di *file* MIDI menjadi dua *file* terpisah, *file* MIDI asli dan pesan tersembunyi. Konversi telah dilakukan, tetapi pesan masih dalam bentuk *ciphertext* yang dienkripsi sebelumnya. Oleh karena itu, pesan masih belum bisa dibaca. Dengan demikian, dekripsi diperlukan untuk mendekripsi *ciphertext* ke pesan yang dapat dibaca. Tentu saja, perangkat lunak ini mampu melakukan itu, sehingga pesan yang sebenarnya terungkap. Sebagai penutup, perangkat lunak ini ditulis dengan bahasa pemrograman C++ dan membahas tentang enkripsi dari *file* teks ke *ciphertext*, dekripsi dari *ciphertext* ke *file* teks, konversi dari *ciphertext* ke *file* MIDI, dan sebaliknya konversi dari *file* MIDI ke *ciphertext*.

Kata kunci: *file* teks, *file* MIDI, kriptografi, pesan rahasia

Abstract

Communication is a common thing for anyone to do, whether it is direct or indirect communication. Certainly, it is necessary to ensure its security of its. When the case is the security of direct communication, the communication is maintained easily by making sure no one hears the spoken message other than the recipient. On the other hand, in the case of the security of indirect communication, security comes up in many different forms. For instance, sending a message in a .txt file. The information can be secured by cryptography techniques and enhancing it by altering its forms, like from a text file and converting it into another file form, such as a .mid file. In this software, the cryptography technique is done with symmetrical encryption. Then, the conversion between file forms hides the message in the MIDI file. Certainly, the software loses its function if it cannot reveal the hidden message in the MIDI file. Thus, the software can reverse the condition. From a hidden message in the MIDI file into two separate files specifically, an original MIDI file and the hidden message. The conversion is done, but the message is still in a ciphertext form that is encrypted. Hence, it is unreadable. In such a manner, decryption is required to decrypt the ciphertext to a readable message. Certainly, the software is capable of doing that, so the true message is revealed. In closure, this software is written in C++ programming language and discusses encryption from a text file to ciphertext, decryption from ciphertext to a text file, conversion from ciphertext to MIDI file, and vice versa conversion from MIDI file to ciphertext.

Keyword: text file, MIDI file, cryptography, hidden message