Analisis Komparatif dan Implementasi dari Sandi Blok AES dalam Bahasa C = Comparative Analysis and Implementation of AES Block Ciphers in C Language

Rodriguez Breil Soenoto, author

Abstrak

Penyandian blok merupakan salah satu jenis enkripsi yang sering digunakan untuk komunikasi aman, karena dapat diimplementasikan dengan mudah dan praktis. Namun, sandi blok hanya dapat mengenkripsi satu blok data dengan ukuran tertentu. Oleh karena itu, penggunaan sandi blok disertai dengan mode-mode operasi, yang membagi data ke dalam beberapa blok dan melibatkan masukan-masukan lain. Dalam tulisan ini, beberapa mode operasi sandi blok dari skema enkripsi AES diimplementasikan dalam bahasa C dan dianalisis dari segi keamanan, performa, dan penggunaan sumber daya. Hasil perbandingan ini akan dapat digunakan sebagai pertimbangan untuk memilih metode enkripsi untuk beberapa kasus komputasi dimana sistem memiliki kemampuan terbatas dan performa lebih diutamakan.

.....Block ciphers are a type of encryption often used for secure communication, due to its ease of implementation and practicality. However, block ciphers can only encrypt one block of data at a time of a specific size. Therefore, block cipher implementations employ a mode of operation, that divides data into several blocks and involves other inputs. In this paper, several block cipher modes of operation with the AES cryptoscheme are implemented in the C programming language and analyzed from the security, performance, and resource perspectives. The results can then be used as information in determining an encryption method for a particular computation use case where system capabilities are limited and performance is an important factor.