Pembentukkan skema secret sharing berdasarkan fungsi hash = Secret sharing scheme construction based on a hash function

Septyadi Prabowo, author

Abstrak

Tugas akhir ini membahas Pembentukkan Skema Secret Sharing berdasarkan Fungsi Hash. Metode ini menggambarkan bagaimana proses pengamanan suatu pesan/informasi rahasia dengan membaginya kepada beberapa peserta berupa share. Aturan untuk memperoleh pesan rahasia adalah untuk sembarang himpunan bagian yang terdiri dari paling sedikit k peserta tertentu dapat merekonstruksi kembali pesan, sebaliknya jika kurang dari k peserta tertentu maka pesan tidak dapat direkonstruksi kembali. Dengan menggunakan fungsi hash (hash function) dalam proses perhitungan pada skema ini yang mana sulit secara matematis untuk menemukan preimagenya, serta penggunaan operasi XOR membuat skema ini aman dan effisien dalam hal waktu proses perhitungan. Selain itu, dalam tugas akhir ini juga diberikan ilustrasi bagaimana subbagian pesan/ informasi didistribusikan ke masing-masing peserta, dan proses penemuan kembali pesan/ informasi dalam Skema Secret Sharing berdasarkan Fungsi Hash.

.....This final task discusses on this skripsi is on the construction of secret sharing schemes based on hash function. This method illustrates how the process of securing secret message/ information by distribute share to several participant. The rule to reconstruct the secret message is as follow: any subset which consists of at least k certain participant can reconstruct the message, otherwise if less than k certain participant then the message cannot be reconstructed. By using hash function in the calculation process for this scheme which mathematically difficult to find preimage, and by using XOR operation made this scheme is safe and efficient in terms of processing time calculation. Moreover, in this skripsi also provided an illustration on how to subsections of message/ information is distributed to each participant, and recovery process of the message/ information of the secret sharing schemes based on hash function.