Kajian skema e-voting dalam aplikasi skema secret sharing berbasis Chinese remainder theorem (crt) dengan menggunakan barisan mignotte = Study of e voting scheme in application of secret sharing scheme based on the chinese remainder theorem crt using the mignotte sequence

Widuri Lisu, author

Abstrak

Sepanjang satu tahun sebelum pelaksanaan pemilu presiden 2014, banyak wacana yang menyebutkan bahwa sudah saatnya Indonesia beralih dari pemungutan suara dengan menggunakan media kertas (paper voting) pemungutan suara dengan menggunakan media elektronik (e-voting). Dalam skripsi ini dikaji mengenai skema e-voting dalam aplikasi skema secret sharing berbasis Chinese Remainder Theorem (CRT) dengan menggunakan barisan Mignotte. Skema ini hanya difokuskan pada kasus pemungutan suara dengan pilihan “ya” atau “tidak”. Skema e-voting tersebut terdiri dari lima tahap yaitu setup, ballot construction, ballot tallying, vote casting, dan vote counting. Pada tahapan tersebut dikonstruksi barisan Mignotte berdasarkan struktur akses yang telah ditentukan. Hasil akhir dari pemungutan suara diperoleh dengan menggunakan CRT bentuk umum. Kerahasiaan identitas pemilih dan pilihannya dijamin oleh transformasi dari pilihan setiap pemilih.

.....During a year before the president election 2014 was held, there are some articles suggesting Indonesia to switched from paper voting to e-voting. In this undergraduate thesis is discussed about e-voting scheme in application of secret sharing scheme based on the Chinese remainder theorem (CRT) using the Mignotte sequence. In particular, the scheme will be focused only on the case of yes/no voting. The e-voting scheme consists of five steps i.e. setup, ballot construction, ballot tallying, vote casting, and vote counting. Those steps will be constructed the Mignotte sequence by the access structure which been specified. The final result of the voting is obtained by using general CRT. Secrecy of the voter’s identity and his vote is guaranteed by the transformation of the vote from each voter.