

Sistem kriptografi dengan kunci publik aplikasinya pada pembuatan skema pemeriksaan keaslian password

Inu Laksito Wibowo, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=82301&lokasi=lokal>

Abstrak

Sistem kriptografi (data encryption) dengan kunci publik, mempunyai keunggulan dalam pengaturan kunci dibanding dengan sistem kriptografi yang konvensional. Pada sistem kriptografi konvensional, suatu jaringan komputer dengan n komputer dibutuhkan $n(n-1)/2$ kunci, sedangkan pada sistem kriptografi dengan kunci publik ini hanya dibutuhkan n kunci. Di samping mempunyai keunggulan pada pengaturan kunci, sistem kriptografi dengan kunci publik ini menjamin keaslian pesan yang dikirimkan oleh seorang user. Sistem kriptografi dengan kunci publik ini dapat pula diaplikasikan untuk pembuatan skema pemeriksaan keaslian password. Salah satu keunggulan skema pemeriksaan keaslian password dengan dasar sistem ini mampu mempertahankan keamanan sistem walaupun berkas yang berisi password-password user berhasil diketahui. Salah satu alasannya adalah derajat kesulitan untuk menurunkan password-password yang sebenarnya relatif tinggi.