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

Inu Laksito Wibowo, author

Abstrak

Sistem kripto (data encryption) dengan kunci publik, mempunyai keunggulan dalam pengaturan kunci dibanding dengan sistem kripto yang konvensional. Pada sistem kripto konvensional, suatu jaringan komputer dengan n riser dibutuhkan n(n-1)2 kunci, sedangkan pada sistem kripto dengan kunci publik ini hanya dibutuhkan n kunci. Di samping mempunyai keunggulan pada pengaturan kunci, sistem kripto dengan kunci publik ini menjamin keaslian pesan yang dikirimkan oleh seorang user. Sistem kripto 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.