IMPLEMENTASI ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) DAN RSA (RIVEST SHAMIR ADLEMAN) UNTUK PENGAMANAN SURAT DI HUMANIKA

[1] *Binar Putri Pratiwi* (14 1065 1060)
[2] *Mudafiq Riyan Pratama, S.Kom., M.Kom* [3] *Triawan Adi Cahyanto, M. Kom.*

Program Studi Teknik Informatika, Fakultas Teknik
Universitas Muhammadiyah Jember

Email: binarpratiwi@gmail.com

ABSTRAK

Tandatangan tradisional dalam sistem persuratan di Humanika masih menjadi penentu keaslian dari sebuah surat, sehingga sering kali menjadi faktor penghambat implementasi dari sebuah sistem persuratan tersebut. Diperlukan sebuah sistem yang dapat menjadi pelengkap sekaligus dapat mempercepat secara signifikan pemrosesan dokumen digital yaitu dengan *E-Signature* atau biasa disebut juga *Digital Signature*. *Digital signature* bukanlah sebuah tandatangan fisik yang di scan lalu ditambahkan kedalam dokumen. Lebih dari itu sebuah tandatangan digital menggunakan teknik kriptografi yang dapat memastikan keaslian dan transparansi dari sebuah surat sehingga surat tersebut dapat dipertanggungjawabkan. Pengamanan tanda tangan digital surat ini menerapkan kombinasi algoritma *AES* dan *RSA*. Uji coba dilakukan berdasarkan skenario pengujian sistem terhadap pengaruh penggunaan algoritma AES dan RSA pada tanda tangan digital dengan 5 kali uji coba surat dan pada keamanan jaringan sistem. Skenario pengujian ini menghasilkan sistem informasi manajemen persuratan dengan algoritma AES dan RSA yang dapat menjamin dari pemalsuan surat karena pada proses validasi surat membutuhkan kode verifikasi, sedangkan tanpa algoritma AES dan RSA tidak membutuhkan kode verifikasi sehingga dapat memanipulasi keaslian surat tersebut. Sedangkan pengujian keamanan jaringan dengan SSL dapat terbaca semua proses login, pembuatan surat dan id surat yang akan disetujui, tetapi jika menggunakan Open SSL tidak ada data yang terbaca saat proses sistem informasi manajemen persuratan dijalankan. Qrcode dapat berfungsi sebagai autentikasi tanda tangan Ketua Humanika dan memverifikasi surat yang sah.

Kata Kunci : *Digital Signature, Advanced Encryption Standar, Rivest Shamir Adleman, QRCode.*

IMPLEMENTASI ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) DAN RSA (RIVEST SHAMIR ADLEMAN) UNTUK PENGAMANAN SURAT DI HUMANIKA

[1] *Binar Putri Pratiwi* (14 1065 1060)
[2] *Mudafiq Riyan Pratama, S.Kom., M.Kom* [3] *Triawan Adi Cahyanto, M. Kom.*

Informatics Engineering Study Program Engineering Faculty
Muhammadiyah University of Jember

Email: binarpratiwi@gmail.com

ABSTRACT

Traditional signatures in the humanitarian systems are still the determinants of the authenticity of a letter, which is often a factor inhibiting the implementation of such a system. Required a system that can be a complement as well as can accelerate significantly processing of digital documents that is with E-Signature or commonly called Digital Signature. Digital signature is not a physical signature that is scanned and then added to the document. Moreover a digital signature uses cryptographic techniques that can ensure the authenticity and transparency of a letter so that the letter can be accounted for. This digital signature security letter implements a combination of AES and RSA algorithms. Trials are based on system testing scenarios against the effect of AES and RSA algorithms on digital signatures with 5 times mail trials and on system network security. This test scenario produces a management information system with AES and RSA algorithms that can guarantee from letter faking because the validation process requires a verification code, while no AES and RSA algorithms do not require verification codes to manipulate the authenticity of the letter. While testing the network security with SSL can be read all the login process, making a letter and letter id to be approved, but if using Open SSL no data is read when the process of management information system management is executed. Qrcode can serve as the Humanika Chairman's signature authentication and verify valid mailings.

Keywords : *Digital Signature, Advanced Encryption Standar, Rivest Shamir Adleman, QRCode.*