

ABSTRAK

Sistem pengamanan dokumen administrasi di kelurahan Karanglewas Lor saat ini masih belum memadai sehingga berkas penting berisiko bocor, berubah isi, atau diakses pihak tidak berwenang. Penelitian ini bertujuan menerapkan kriptografi hibrida AES-128 dan RSA untuk mengamankan dokumen administrasi dengan pengembangan sistem menggunakan model *waterfall*. Pengujian mencakup black box testing untuk aspek fungsional, pengukuran waktu proses enkripsi dan dekripsi untuk aspek kecepatan, dan *brute force* testing untuk aspek keamanan. Aplikasi berbasis web yang dihasilkan mampu mengenkripsi berkas dalam berbagai format (*pdf, doc, docx, xls,xlsx, txt, jpg, jpeg, png, dan mp4*), dengan AES-128 menyandikan isi berkas dan RSA mengamankan kunci enkripsinya. Hasil pengujian menunjukkan seluruh fitur berjalan sesuai rancangan, waktu pemrosesan berbanding lurus dengan ukuran berkas dengan rata-rata waktu enkripsi 136,67 ms dan dekripsi 114,33 ms untuk ukuran berkas 240 KB hingga 152,33 ms dan 148,00 ms untuk ukuran berkas 6.472 KB. Pengujian *brute force* terhadap passphrase kunci privat RSA menghasilkan tingkat keberhasilan serangan 0% pada seluruh skenario uji dengan estimasi waktu tembus mencapai 236,9 hari untuk kombinasi 9 karakter alfanumerik. Temuan ini membuktikan bahwa kombinasi AES-128 dan RSA efektif menjaga kerahasiaan dan integritas dokumen administrasi kelurahan, layak digunakan secara fungsional, serta memberikan ketahanan keamanan yang baik apabila didukung passphrase dengan kompleksitas memadai.

Kata kunci: Kriptografi Hibrida, AES-128, RSA, Keamanan Data, Dokumen Administrasi

ABSTRACT

The current document security system at the Karanglewas Lor village office is still inadequate leaving important files vulnerable to leakage, content alteration, or access by unauthorized parties. This study aims to apply hybrid AES-128 and RSA with using the waterfall model. Testing covered black box testing for functional aspects, processing time measurement for speed aspects, and brute force testing for security aspects. The resulting web based application is able to encrypt files in various formats pdf, doc, docx, xls, xlsx, txt, jpg, jpeg, png and mp4, with AES-128 encoding the file content and RSA securing the encryption key. Test result show that all features functioned as designed, with processing time proportional to file size averaging 136,67 ms for encryption and 113,33 ms for decryption on a 240 KB file, up to 152,33 ms and 148,00 ms on a 6.472 KB file. Brute force testing against the RSA the private key passphrase resulted in a 0% attack success rate across all tested scenarios, with estimated crack time of 236.9 days for a 9 character alphanumeric combination. These findings confirm that the combination of AES-128 and RSA effectively maintains the confidentiality and integrity of village administrative documents, is functionally suitable for use, and provides strong security resilience when supported by a sufficiently complex passphrase.

Keyword: Hybrid Cryptography, AES-128, RSA, Data Security, Village Administration