

DESAIN ENKRIPSI DATA MENGGUNAKAN ALGORITMA AES 128 DAN BASE 64

1. Cahyo Susilanto, 09112072, cahyosusianto@gmail.com
2. S. Supatman, 0509057202, keliksupatman@gmail.com

ABSTRAK

Teknologi pada jaman sekarang banyak dilingkupi oleh kriptografi. Mulai dari percakapan telepon genggam, akses *internet*, sampai aktivitas transaksi di ATM telah menggunakan kriptografi.

Kriptografi adalah bidang ilmu untuk menjaga keamanan pesan (*message*). Cara kerjanya adalah dengan mengubah pesan asli yang dapat dimengerti/dibaca manusia (*plaintext*) ke bentuk lain yang tidak dapat dimengerti/dibaca oleh manusia (*ciphertext*). Proses transformasi *plaintext* menjadi *chipertext* diistilahkan dengan enkripsi.

Ada banyak algoritma kriptografi, *Advanced Encryption Standard* (AES) merupakan standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat. Standar ini terdiri atas 3 blok *cipher*, yaitu AES-128, AES-192 and AES-256. Base64 adalah metode pengkodean yang mewakili data *biner* dalam format *string* ascii dengan menerjemahkannya kedalam representasi base64

Pada penelitian ini algoritma kriptografi AES (*Advanced Encryption Strandard*) digunakan untuk enkripsi data dan Base64 yang diimplementasikan untuk melindungi data yang dikirim melalui pesan *email*.

Kata Kunci :kriptografi, *plainteks*, *chiperteks*, *Advance Encryption Standard* (AES), Base 64.