TRIPLE DES ALGORITHM ANALYSIS FOR MESSAGE DISGUISING

Sony Hartono Wijaya, Sugi Guritman, Wisnu Ananta Kusuma

ABSTRAK

Paper ini mendiskusikan hasil analisis terhadap algoritma triple DES sebagai varian dari DES (Data Encryption Standard) yang lebih kuat dan mampu melindungi informasi dengan baik. Analisis yang dilakukan meliputi analisis algoritma, analisis keamanan dan analisis hasil implementasi (kecepatan). Analisis algoritma terbagi menjadi dua bagian yaitu analisis algoritma enkripsi dan analisis algoritma deskripsi.

Triple DES menggunakan algoritma DES sebagai algoritma utama. Triple DES dikembangkan untuk mengatasi kelemahan ukuran kunci yang digunakan pada proses enkripsi-deskripsi DES sehingga teknik kriptografi ini lebih tahan terhadap exhaustive key search yang dilakukan oleh kriptoanalis. Penggunaan triple DES dengan suatu kunci tidak akan menghasilkan pemetaan yang sama seperti yang dihasilkan oleh DES dengan kunci tertentu. Hal itu disebabkan oleh sifat DES yang tidak tertutup (not closed). Sedangkan dari hasil implementasi dengan menggunakan modus Electronic Code Book (ECB) menunjukkan bahwa walaupun memiliki kompleksitas/notasi O yang sama (O(n)), proses enkripsi-deskripsi pada DES lebih cepat dibandingkan dengan triple DES.