TINJAUAN STATISTIK UJI CHI-SQUARE GOODNESS OF FIT TERHADAP KEACAKAN HASIL PENYANDIAN PADA ALGORITMA FAST DATA ENCHIPHERMENT ALGORITHM (FEAL) DENGAN MENGGUNAKAN MODE ECB DAN CFB

MARIA PUTRI HANDAYANI, ADANG SUHENDRA,SSI,SKOM,MSC

Penulisan Ilmiah, Fakultas Ilmu Komputer, 2005

Universitas Gunadarma

http://www.gunadarma.ac.id

kata kunci : statistik

Abstraksi :

Salah satu kemajuan teknologi yang nampak jelas dan nyata pengaruhnya bagi masyarakat adalah bidang komunikasi, dimana sekarang ini kebutuhan akan informasi semakin besar. Di dalam proses pertukaran informasi, terutama untuk informasi yang bersifat rahasia, terdapat bahaya penyadapan terhadap informasi tersebut, oleh karena itu diperlukan suatu sistem keamanan yang dapat menjamin keamanan informasi yang dikirim atau diterima, dimana salah satu bentuknya adalah dengan menggunakan sistem penyandian. Penyandian Blok, yang termasuk dalam sistem sandi simetrik, pada dasarnya menggunakan mode penyandian ECB. Pada mode ECB, blok teks terang yang sama selalu menghasilkan blok teks sandi yang sama pula sehingga jika kriptanalis memiliki teks terang dan teks sandi dari beberapa berita, ia dapat mencocokkan buku kode tanpa perlu mengetahui kuncinya. Penelitian yang dilakukan dalam Tugas Akhir ini adalah untuk mendapatkan kemungkinan alternatif dari algoritma Block Cipher (FEAL) dengan mode ECB dengan alternatifnya yaitu algoritma FEAL dengan mode CFB. Salah satu syarat kekuatan suatu sistem sandi adalah teks sandi yang dihasilkan harus acak. Oleh karena itu dilakukan pengujian terhadap teks sandi untuk mengukur apakah penggunaan mode CFB dapat menjadi alternatif yang lebih baik bagi algoritma standar. Pengujian keacakan teks sandi pada algoritma standar mode ECB dan alternatifnya algoritma dengan mode CFB menggunakan uji statistik Chi-Square Goodness of Fit. Dari hasil pengujian statistik Chi-Square Goodness of Fit dengan tingkat signifikansi a=0,001, 0,01,dan a=0,05 diperoleh hasil presentasi keacakan yang cenderung sama antara hasil penyandian dengan algoritma FEAL mode ECB dan CFB. Sehingga mode CFB dapat menjadi alternatif untuk penyandian blok algoritma FEAL dengan mode ECB.