

Abstrak

Kriptografi adalah ilmu yang digunakan untuk menjaga kerahasiaan. Kriptografi menjadi suatu bagian yang tidak dapat dipisahkan dari sistem keamanan jaringan pada era informasi global. Pada kriptografi terdapat banyak algoritma yang telah berkembang diantaranya adalah algoritma TEA, XTEA dan XXTEA. Dimana ketiga algoritma ini merupakan algoritma kriptografi block cipher yang masih satu keluarga dan memiliki kesamaan pada panjang kunci yaitu 128 bit.

Pada tugas akhir ini dilakukan pengukuran dan analisa perbandingan performansi algoritma TEA, XTEA, dan XXTEA dengan menerapkan algoritma tersebut pada suatu perangkat lunak. Kemudian diukur performansinya berdasarkan Parameter *avalanche effect*, *cryptanalysis* (menggunakan *brute force attack*) dan menghitung kompleksitas waktu algoritma.

Berdasarkan hasil pengujian didapatkan dari ketiga algoritma tersebut bahwa avalanche effect pada algoritma TEA dan XTEA dengan kondisi beda bit kunci lebih baik dibandingkan dengan beda bit plainteks. Sedangkan pada algoritma XXTEA, pada beda bit kunci maupun beda bit plainteks nilai avalanche effect-nya sama-sama baik. Waktu proses enkripsi dan dekripsi yang dibutuhkan algoritma TEA lebih kecil dibandingkan dengan XTEA dan XXTEA. Dan waktu proses enkripsi dan dekripsi algoritma XXTEA lebih kecil dibandingkan dengan algoritma XTEA. Ketahanan algoritma XXTEA terhadap *brute force attack* lebih baik dibandingkan dengan TEA dan XTEA. Kompleksitas waktu algoritma TEA, XTEA dan XXTEA merupakan algoritma yang efisien terlihat pada kompleksitas waktu asimptotik yang dimiliki ketiga algoritma ini adalah sama yaitu $O(n)$.

Kata kunci: kriptografi, *cipher* blok, TEA, XTEA, XXTEA, *avalanche effect*, *cryptanalysis*, kompleksitas algoritma