

ANALISA PERBANDINGAN VARIASI UKURAN FRAME DENGAN VARIASI KUNCI AES PADA KOMBINASI TEKNIK KRIPTOGRAFI AES - TURBO CODE

Anissa Rachmawati

(13.04.111.00004)

Pembimbing 1 : Dwi Kuswanto, S.Pd., M.T.

Pembimbing 2 : Mula'ab, S.Si., M.Kom.

ABSTRAK

Untuk menghindari pesan yang dikirim tidak disalah gunakan oleh pihak yang tidak berkepentingan, maka perlu dilakukan proses enkripsi dan dekripsi pesan asli. Salah satu bidang ilmu untuk menjaga keamanan informasi adalah kriptografi AES. Namun dibutuhkan juga pendeteksi dan pengoreksi kesalahan, salah satu metodenya adalah *Turbo Code*. Dengan melakukan kombinasi antara enkripsi AES dan teknik pengkodean *Turbo Code* pada satu langkah diharapkan dapat menghasilkan keputusan yang efektif. Hasil penelitian yang dilakukan kinerja BER (*Bit Error Rate*) terhadap kanal ideal berupa garis lurus dengan nilai BER 0, yang artinya tidak ada *noise* pada informasi yang dikirimkan. Sedangkan kinerja BER (*Bit Error Rate*) terhadap kanal AWGN semakin membaik saat SNR 13 sampai 15 dB dengan persentase data yang kembali rata-rata sebesar 99,9 %. Dengan demikian AES-Turbo dapat bekerja secara efektif meskipun persentase data yang kembali tidak mencapai 100%. Nilai rata-rata pengujian *avalanche effect* sebesar 50%. Dikarenakan nilai maksimal dari *avalanche effect* sebesar 50%, dapat membuktikan metode AES-Turbo lebih efektif.

Kata kunci: AES, *Turbo Code*, AES-Turbo.

COMPARISON OF FRAME SIZE VARIATIONS WITH AES KEY VARIATIONS ON AES-TURBO CODE CRYPTOGRAPHIC ENGINEERING COMBINATION

Anissa Rachmawati

(13.04.111.00004)

Pembimbing 1 : Dwi Kuswanto, S.Pd., M.T.

Pembimbing 2 : Mula'ab, S.Si., M.Kom.

ABSTRACT

In order to avoid messages sent by unauthorized parties, encryption and decryption of the original message is required. One of the areas of science to keep information secure is AES cryptography. However, there is also a detector and error correction, one of the methods is Turbo Code. By doing a combination of AES encryption and Turbo Code coding techniques In one step is expected to make effective decisions. The results of the study conducted a Bit Error Rate against the ideal channel in the form of a straight line with a value of a 0, which means there is no noise in the information transmitted. While the performance of BER (Bit Error Rate) of the AWGN channel is getting better when SNR 13 to 15 dB with a percentage of data that returns an average of 99.9%. Thus AES-Turbo can work effectively even though the percentage of returning data does not reach 100%. The average value of an avalanche effect test is 50%. Due to the maximum value of the avalanche effect of 50%, it can prove the AES-Turbo method more effective.

Keywords : AES, Turbo Code, AES-Turbo.