Kamies: optimalisasi keamanan algoritma kasumi dengan meningkatkan tingkat difusi = Kamies security optimization of kasumi algorithm by increasing diffusion level

Rizki Yugitama, author

Abstrak

Tesis ini membahas mengenai pengembangan Algoritma KASUMI dengan Penerapan fungsi F MISTY1 dan S-box AES. Algoritma hasil pengembangan diberi nama KAMIES. Untuk membandingkan tingkat keamanan KASUMI dan KAMIES dilakukan beberapa pengujian pada masing-masing komponen. Komponen yang dilakukan pengujian diantaranya adalah fungsi F yang terdiri dari FI, FL dan FO, kemudian S-box yang terdiri dari S7, S8, dan S9 yang terdapat pada masing-masing algortima. Metode pengujian yang digunakan diantaranya Bit Independence Criterion BIC dan Strict Avalanche Criterion SAC pada fungsi F sedangkan pada S-box digunakan metode pengujian Avalanche Criterion AC , SAC, BIC, XOR Table, LAT dan Nonlinearity.

Hasil yang didapat dari penelitian ini membuktikan bahwa penerapan F MISTY1 dan S-box AES memiliki pengararuh terhadap tingkat keamanan algoritma KASUMI. Hal ini berdasarkan hasil pengujian Strict Avalanche Criterion SAC dan Avalanche Weight Distribution AWD pada algoritma keseluruhan KASUMI dan KAMIES yang menunjukkan bahwa KAMIES memiliki nilai difusi yang lebih baik dibandingkan KASUMI.

.....This thesis discusses the development of KASUMI Algorithm with Application of F Function MISTY1 and S box AES. The result of development algorithm is named KAMIES. To compare the level of security KASUMI and KAMIES performed some testing on each component. Components that are tested are F functions consisting of FI, FL and FO, then S boxes consisting of S7, S8, and S9 are present in each algortima. Test methods which used include Bit Independence Criterion BIC and Strict Avalanche Criterion SAC on F function while in S box used Avalanche Criterion AC , SAC, BIC, XOR Table, LAT and Nonlinearity testing methods.

The results obtained from this study prove that the application of F MISTY1 and S box AES have influence to the security level of KASUMI algorithm. This is based on the results of Strict Avalanche Criterion SAC and Avalanche Weight Distribution AWD testing on the overall algorithm of KASUMI and KAMIES which shows that KAMIES have better value than KASUMI.