

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis, pengujian, dan pembahasan terhadap algoritma kriptografi RC4, RC5, dan RC6 pada sistem berbasis web, maka diperoleh beberapa kesimpulan sebagai berikut:

1. RC6 memiliki keamanan tertinggi, dengan waktu rata-rata 0.000097 detik dan konsumsi memori 240 KB. Cocok untuk aplikasi web dengan kebutuhan keamanan tinggi, meskipun implementasinya paling kompleks.
2. RC4 paling efisien dengan waktu tercepat 0.000034 detik dan implementasi termudah. Namun, keamanannya rendah sehingga hanya cocok untuk sistem non-kritis.
3. RC5 berada di tengah, dengan waktu rata-rata 0.000006 detik, performa stabil, dan keamanan sedang. Ideal untuk sistem web dengan kebutuhan seimbang.

Secara umum, pemilihan algoritma tergantung pada prioritas sistem: RC6 untuk keamanan, RC5 untuk keseimbangan, dan RC4 untuk efisiensi.

5.2 Saran

Berikut adalah saran dari penulis untuk penelitian selanjutnya:

1. Penelitian lanjutan sebaiknya melibatkan algoritma modern seperti AES, Twofish, atau ChaCha20 untuk pembandingan performa dan keamanan.

2. Diperlukan pengujian pada lingkungan berbeda seperti *mobile apps*, *cloud-based system*, dan IoT untuk melihat adaptabilitas algoritma.
3. Tambahan pengujian resiliensi terhadap serangan nyata menggunakan *tool* seperti *CryptoMiniSat* atau *Differential Attack Simulator* juga disarankan.

