Bab VI
Penutup

Dari hasil pengujian enkripsi dan dekripsi dengan inputan text (kombinasi huruf, angka dan spesial karakter), image dan pdf menggunakan kombinasi *AES – DES, AES – Blowfish, DES – Blowfish dan AES – DES* dan *Blowfish* menghasilkan tabel seperti dibawah.

Tabel 7 Rekapitulasi Hasil Pengujian

	AES - DES	AES - Blowfish	DES - Blowfish	AES - DES - Blowfish
Encryption Time (s) (Text)	0,00065	0,00056	0,00034	0,00017
Decryption Time (s) (Text)	0,00037	0,00040	0,00015	0,00010
Encryption Time (s) (Image)	0,00617	0,00260	0,00593	0,00713
Decryption Time (s) (Image)	0,00443	0,00228	0,00582	0,00652
Encryption Time (s) (Pdf)	0,01237	0,00594	0,01598	0,01624
Decryption Time (s) (Pdf)	0,01090	0,00521	0,01531	0,01434

Dari rekapitulasi hasil pengujian enkripsi dan dekripsi kombinasi *AES – DES, AES – Blowfish, DES – Blowfish dan AES – DES* dan *Blowfish* menggunakan inputan inputan text (kombinasi huruf, angka dan spesial karakter), image dan pdf. Hasil enkripsi dan dekripsi dengan inputan text (kombinasi huruf, angka dan spesial karakter) kombinasi algoritma *AES – DES* dan *Blowfish* mendapatkan hasil enkripsi 0,00017 detik dan dekripsi 0,00010 detik yang lebih kecil dari kombinasi algoritma yang lain, Hasil enkripsi dan dekripsi dengan inputan gambar kombinasi algoritma *AES* dan *Blowfish* mendapatkan hasil enkripsi 0,00260 detik dan dekripsi 0,00228 detik yang lebih kecil dari kombinasi algoritma yang lain dan untuk Hasil enkripsi dan dekripsi dengan inputan pdf kombinasi algoritma *AES* dan *Blowfish* mendapatkan hasil enkripsi 0,00594 detik dan dekripsi 0,00521 detik yang lebih kecil dari kombinasi algoritma yang lain.

Kesimpulan :
Penerapan algoritma AES, DES, dan Blowfish dalam sistem enkripsi memberikan tingkat keamanan yang tinggi dan fleksibilitas dalam melindungi berbagai jenis data, baik itu password pada website maupun file dokumen.

Untuk password pada website, kombinasi enkripsi dengan *AES*, *DES*, dan *Blowfish* menawarkan perlindungan berlapis yang kuat. Proses dimulai dengan hashing password untuk konsistensi dan kemudahan penyimpanan. Kemudian, data yang telah di *hash* dienkripsi secara berurutan dengan *AES*, *DES*, dan *Blowfish*. *Blowfish* memberikan enkripsi awal yang cepat dengan kunci variabel, diikuti oleh *DES* yang menambah lapisan kompleksitas, dan akhirnya *AES* yang menawarkan tingkat keamanan tinggi. Penggunaan beberapa algoritma ini secara berurutan membuat password sulit dipecahkan bahkan jika *ciphertext* jatuh ke tangan yang salah, memperkuat perlindungan terhadap serangan *brute force* dan teknik kriptanalisis lainnya.

Untuk file dokumen seperti gambar, teks, PDF, dan XLS, penerapan *AES* dan *Blowfish* memastikan keamanan data yang efisien. Proses dimulai dengan enkripsi file menggunakan *Blowfish*, yang mengatasi data dalam blok 64-bit dengan kecepatan tinggi dan fleksibilitas kunci. *Ciphertext* dari *Blowfish* kemudian dienkripsi lebih lanjut menggunakan *AES*, algoritma dengan standar enkripsi yang diakui secara internasional dan memberikan perlindungan tambahan. Pendekatan ini memastikan bahwa data yang terenkripsi sangat sulit diakses tanpa kunci yang benar, baik saat penyimpanan maupun transmisi.

Secara keseluruhan, penerapan kombinasi *AES*, *DES*, dan *Blowfish* untuk password dan file dokumen memberikan solusi enkripsi yang komprehensif dan handal. Dengan menggabungkan kelebihan masing-masing algoritma cepatnya *Blowfish*, kerumitan *DES*, dan kekuatan *AES* sistem ini menawarkan perlindungan yang mendalam terhadap data sensitif. Penggunaan berlapis dalam enkripsi password dan metode gabungan untuk file dokumen menjamin tingkat keamanan yang tinggi, menjaga integritas dan kerahasiaan data dari akses yang tidak sah. Hal ini menunjukkan bahwa pemilihan kombinasi algoritma enkripsi yang optimal sangat bergantung pada jenis data yang akan diamankan, di mana antara keamanan dan kecepatan harus dipertimbangkan dengan cermat.