

ABSTRAK

Judul : IMPLEMENTASI ALGORITMA KRIPTOGRAFI ADVANCED
ENCRYPTION STANDARD-128 (AES-128) UNTUK PENGAMANAN
BASISDATA BERBASIS WEB PADA PT. AL AMIR TOUR & TRAVEL

Saat ini data dan informasi menjadi hal yang penting. Berbagai perusahaan, organisasi, instansi, dan lainnya telah memanfaatkan teknologi database untuk menyimpan dan juga mengelola data organisasi atau perusahaannya. Keamanan terhadap data yang disimpan dalam database sudah menjadi hal yang sangat dibutuhkan. Namun keamanan pada database dengan pembatasan hak akses sudah tidak lagi dapat menjamin keamanan data karena kebocoran data dapat disebabkan oleh pihak-pihak yang langsung berhubungan dengan database itu sendiri seperti administrator database. Salah satu caranya adalah dengan menggunakan algoritma kunci simetris, dimana kunci enkripsi dan dekripsi tersebut sama namun jika kunci tidak dapat diketahui oleh penyadap, maka isi pesan tidak dapat diketahui oleh penyadap. PT. Al Amir Tour & Travel adalah perusahaan yang bergerak dibidang jasa wisata dan perjalanan, yang salah satunya adalah mengadakan keberangkatan Umroh dan Haji. PT. Al Amir Tour & Travel mempunyai tujuan untuk memberikan pelayanan yang baik kepada pelanggan. PT. Al Amir Tour & Travel memiliki data yang disimpan dalam sebuah database. Salah satu data tersebut adalah data jamaah haji yang merupakan data penting yang perlu dijaga keamanannya. Pada tugas akhir ini dirancang suatu aplikasi kriptografi yang digabungkan dengan *database*, dimana penulis mengharapkan aplikasi ini kriptografi yang dapat membantu segala kegiatan pada PT. Al Amir Tour & Travel. Dalam perancangan aplikasi ini menggunakan metode pengembangan sistem dengan model waterfall. Aplikasi menggunakan algoritma AES (*Advanced Encryption Standard*) 128 dengan bahasa pemrograman PHP, dimana kunci enkripsi dan dekripsi sudah diatur oleh sistem, hal ini dilakukan agar informasi kunci tidak dapat diketahui dengan mudah oleh penyadap. Algoritma AES (*Advanced Encryption Standard*) 128 diharapkan mampu memproses enkripsi dan dekripsi data dengan waktu yang lebih cepat dan pengamanan yang lebih aman.

Kata Kunci : *Database*, AES (*Advanced Encryption Standard*) 128, Enkripsi, Dekripsi.

xviii+163