



**PENERAPAN KEAMANAN *DATABASE WEBSITE* RUMAH BATIK
PALBATU UNTUK MELINDUNGI *INFORMASI PENGGUNA*
MENGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD*
(*AES-128*)**

COVER SKRIPSI

**ENNO TEGAR DWI SAPUTRA
2010511004**

**PROGRAM STUDI *INFORMATIKA*
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
2025**



**PENERAPAN KEAMANAN *DATABASE WEBSITE* RUMAH BATIK
PALBATU UNTUK MELINDUNGI *INFORMASI PENGGUNA*
MENGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD*
(*AES-128*)**

**SKRIPSI
DIAJUKAN SEBAGAI SALAH SATU SYARAT UNTUK
MEMPEROLEH GELAR SARJANA KOMPUTER**

**ENNO TEGAR DWI SAPUTRA
2010511004**

**PROGRAM STUDI *INFORMATIKA*
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
2025**

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa tugas akhir berikut :

Nama : Enno Tegar Dwi Saputra

NIM : 2010511005

Program Studi : S1 Informatika

Judul : penerapan keamanan *database website* rumah batik palbatu untuk melindungi informasi pengguna menggunakan algoritma *advanced encryption standard (aes-128)*

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian dari persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta



(Neny Rosmawarni, S.Kom, M.Kom.)

Penguji I



(Muhammad Panji Muslim, S.Pd., M.Kom)

Penguji II



(Henki Bayu Seta, S.Kom., MTL.)

Dosen Pembimbing I



(Novi Trisman Hadi, S.Pd., M.Kom.)

Dosen Pembimbing II



(Prof. Dr. S. Priyanto, ST., M.Sc., IPM)
Dekan Fakultas Ilmu Komputer



(Dr. Widya Cholil, M.T.)

Koordinator

Ditetapkan di : Jakarta

Tanggal Persetujuan : 15 Januari 2025

PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Enno Tegar Dwi Saputra

NIM : 2010511004

Tanggal : 15 Desember 2024

Bilamana dikemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 15 Desember 2024

Yang Menyatakan,



(Enno Tegar Dwi Saputra)

**SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta,
saya yang bertanda tangan dibawah ini.

Nama : Enno Tegar Dwi Saputra

NIM : 2010511004

Fakultas : Ilmu Komputer

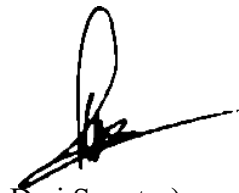
Program Studi : *Informatika*

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional “Veteran” Jakarta. Hak Bebas Royalti Non Eksklusif (Non-Exclusive Royalty Free Right) atas karya ilmiah saya yang berjudul “ PENERAPAN KEAMANAN *DATABASE WEBSITE* RUMAH BATIK PALBATU UNTUK MELINDUNGI *INFORMASI PENGGUNA MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD (AES-128)**.”

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 30 September 2024

Yang menyatakan,



(Enno Tegar Dwi Saputra)

**PENERAPAN KEAMANAN *DATABASE WEBSITE* RUMAH BATIK
PALBATU UNTUK MELINDUNGI *INFORMASI PENGGUNA*
MENGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD*
(*AES-128*)**

ENNO TEGAR DWI SAPUTRA

ABSTRAK

Rumah Batik Palbatu adalah sebuah usaha yang fokus pada pelestarian budaya batik tradisional melalui edukasi dan produksi batik. Sistem transaksi saat ini yang dilakukan secara manual menghadirkan berbagai tantangan, termasuk risiko keamanan data pengguna. Penelitian ini bertujuan untuk meningkatkan keamanan informasi pengguna pada *database website* Rumah Batik Palbatu menggunakan algoritma *Advanced encryption standard (AES-128)*. Dengan menerapkan metode *Rapid application development (RAD)*, penelitian ini mencakup analisis kebutuhan, desain sistem, implementasi algoritma *AES*, dan pengujian aplikasi. Hasil penelitian menunjukkan bahwa algoritma *AES-128* berhasil mengenkripsi data pengguna, sehingga memberikan tingkat keamanan yang lebih tinggi untuk melindungi informasi pribadi pengguna dalam transaksi online.

Kata kunci: Keamanan Informasi, *database*, *Advanced encryption standard (AES-128)*, *E-commerce*, Rumah Batik Palbatu.

**PENERAPAN KEAMANAN *DATABASE WEBSITE* RUMAH BATIK
PALBATU UNTUK MELINDUNGI *INFORMASI PENGGUNA*
MENGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD*
(*AES-128*)**

ENNO TEGAR DWI SAPUTRA

ABSTRACT

Rumah Batik Palbatu is a business dedicated to preserving traditional batik culture through education and production. The current manual transaction system poses several challenges, including *Userdata* security risks. This research aims to enhance the security of *User* information on the Rumah Batik Palbatu *database website* using the *Advanced encryption standard (AES-128)* algorithm. Employing the *Rapid application development (RAD)* method, the study includes requirement analysis, system design, *AES* algorithm implementation, and application *testing*. The results demonstrate that the *AES-128* algorithm successfully *encrypts Userdata*, providing a higher level of security to protect personal information during online transactions.

Keywords: Information Security, *Advanced encryption standard (AES-128)*, *E-commerce*, Rumah Batik Palbatu.

KATA PENGANTAR

Puji dan syukur kami panjatkan kehadiran Tuhan Yang Maha Esa, karena hanya atas berkat dan rahmat-Nya, sehingga Laporan Tugas Skripsi *Informatika* yang berjudul “Penerapan Keamanan *Database Website* Rumah Batik Palbatu Untuk Melindungi Informasi Pengguna Menggunakan *ADVANCED ENCRYPTION STANDARD (AES)*” dapat diselesaikan dengan baik dan tepat waktu. Adapun tujuan penulisan laporan ini adalah untuk memenuhi persyaratan dalam menempuh kelulusan Strata Satu *Informatika* Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.

Tanpa Untuk itu pada kesempatan ini penulis menyampaikan rasa penghargaan dan terima kasih kepada yang terhormat:

1. Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM selaku Dekan Fakultas Ilmu Komputer.
2. Ibu Widya Cholil, M.I.T selaku ketua prodi *informatika* yang telah memberikan kemudahan dan kelancaran dalam pelaksanaan tugas akhir skripsi ini.
3. Bapak Henki Bayu Seta, S.Kom., MTI. selaku dosen pembimbing pertama yang telah memberikan banyak masukan dan saran dalam proses pembuatan laporan tugas akhir skripsi ini.
4. Bapak Novi Trisman Hadi, S.Pd., M.Kom selaku pembimbing kedua yang telah memberikan banyak masukan, saran serta membangun cara berpikir logis dan kritis, dalam proses penyusunan laporan tugas akhir skripsi ini.
5. Ayah dan Ibu yang selalu mendoakan, mendukung penuh penyelesaian tugas akhir skripsi ini, dengan memberikan semangat dan motivasi yang tiada henti.
6. Terima kasih untuk Seluruh pihak yang terlibat.

Penulis menyadari bahwa laporan tugas akhir ini masih banyak kekurangan didalamnya, maka kritik dan saran sangat diharapkan penulis untuk perbaikan laporan tugas akhir skripsi ini. Semoga Tuhan Yang Maha Esa memberikan imbalan yang setimpal atas segala bantuan yang diberikan.

Tangerang, 10 Januari 2025

Penyusun



Enno Tegar Dwi Saputra

DAFTAR ISI

| | |
|--|-------------------------------------|
| COVER SKRIPSI | i |
| SKRIPSI..... | ii |
| PERNYATAAN ORISINALITAS..... | iii |
| SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS | iv |
| LEMBAR PERSETUJUAN | Error! Bookmark not defined. |
| ABSTRAK | vii |
| ABSTRACT | vii |
| DAFTAR ISI..... | ix |
| DAFTAR TABEL | xii |
| DAFTAR GAMBAR | xiii |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang Masalah..... | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Tujuan Penelitian..... | 4 |
| 1.4 Manfaat Penelitian | 4 |
| 1.4.1 Bagi Penulis | 4 |
| 1.4.2 Bagi Peneliti Lain..... | 4 |
| 1.4.3 Bagi Instansi Terkait..... | 4 |
| 1.5 Batasan Masalah..... | 4 |
| 1.6 Luaran Yang Diharapkan..... | 5 |
| BAB II TINJAUAN PUSTAKA..... | 6 |
| 2.1 Kriptografi..... | 6 |
| 2.1.1 Kriptografi Klasik | 6 |
| 2.1.2 Kriptografi Modern | 7 |
| 2.2 Keamanan Informasi | 8 |
| 2.3 <i>E-commerce</i> | 9 |
| 2.4 <i>ADVANCED ENCRYPTION STANDARD (AES)</i> | 9 |
| 2.4.1 Algoritma <i>ADVANCED ENCRYPTION STANDARD (AES)</i> | 10 |
| 2.4.2 Algoritma Deskripsi atau Chiper Kebalikan <i>ADVANCED ENCRYPTION STANDARD (AES)</i> | 14 |

| | | |
|--|--|-----------|
| 2.5 | <i>PHP</i> | 15 |
| 2.6 | <i>Code igniter</i> | 16 |
| 2.7 | <i>Rapid application development (RAD)</i> | 17 |
| 2.8 | <i>Database MySQL</i> | 19 |
| 2.9 | Penelitian Relevan..... | 20 |
| BAB III METODOLOGI PENELITIAN | | 24 |
| 3.1 | Metodologi Penelitian..... | 24 |
| 3.1.1 | Wawancara | 24 |
| 3.1.2 | Observasi..... | 24 |
| 3.1.3 | Studi Literatur | 25 |
| 3.2 | Metode Pengembangan Sistem | 25 |
| 3.2.1 | Fase Perencanaan Syarat-syarat | 25 |
| 3.2.2 | Fase Pelaksanaan atau Implementasi | 27 |
| 3.3 | Kerangka Penelitian | 28 |
| 3.4 | Alat Bantu Penelitian | 29 |
| 3.4.1 | Perangkat Keras (tambah tempat penelitian) | 29 |
| 3.4.2 | Perangkat Lunak..... | 29 |
| 3.5 | Jadwal Penelitian..... | 30 |
| BAB IV HASIL DAN PEMBAHASAN..... | | 31 |
| 4.1 | Metode Pengumpulan Data dan Informasi..... | 31 |
| 4.1.1 | Tahap Pengumpulan Data dan Informasi | 31 |
| 4.2 | Metode Pengembangan Sistem | 33 |
| 4.2.1 | Fase Perencanaan Syarat-syarat | 34 |
| 4.2.2 | Sistem Yang Berjalan | 35 |
| 4.2.3 | Identifikasi Masalah | 35 |
| 4.2.4 | Sistem Yang Diusulkan | 36 |
| 4.2 | Fase <i>Workshop design</i> | 37 |
| 4.2.1 | Perancangan <i>UML</i> | 37 |
| 4.2.2 | Desain Proses Dekripsi <i>AES</i> | 40 |
| 4.2.3 | Desain <i>Database</i> | 40 |
| 4.2.3.1 | Spesifikasi <i>Database</i> | 42 |
| 4.2.5 | Perancangan <i>Graphics Userinterface</i> | 47 |
| 4.2.6 | Implementasi Algoritma <i>AES</i> | 50 |
| 4.3 | Hasil Enkripsi Data | 75 |

| | | |
|----------------------------|--|-----------|
| 4.3.1 | Data Sebelum Enkripsi..... | 75 |
| 4.3.2 | Data Setelah Enkripsi..... | 75 |
| 4.4 | Pengujian (<i>Testing</i>)..... | 76 |
| 4.4.1 | Tahap Pengujian..... | 77 |
| 4.4.2 | UAT (<i>UserAcceptance Testing</i>)..... | 79 |
| BAB V PENUTUP | | 80 |
| 5.1 | Kesimpulan | 80 |
| 5.2 | Saran..... | 81 |
| DAFTAR PUSTAKA..... | | 82 |
| RIWAYAT HIDUP..... | | 85 |
| LAMPIRAN..... | | 86 |

DAFTAR TABEL

| | |
|--|----|
| Table 2. 1 Perbedaan ukuran kunci algoritma <i>AES</i> | 10 |
| Table 2. 2 Tabel S-box yang digunakan dalam transformasi <i>ByteSub()</i> <i>AES</i> (Cristy and Riandari, 2021)..... | 11 |
| Table 2. 3 Tabel S-box yang digunakan dalam transformasi <i>InvByteSub()</i> <i>AES</i> (Cristy and Riandari, 2021)..... | 15 |
| Table 2. 4 Peneliatian Rele van | 20 |
| Table 3. 1 Jadwal Penelitian | 30 |
| Table 4.1 Tabel User..... | 42 |
| Table 4. 2 Table Pelanggan | 42 |
| Table 4. 3 Tabel <i>order</i> | 43 |
| Table 4. 4 Tabel <i>History</i> | 43 |
| Table 4. 5 Tabel Produk..... | 44 |
| Table 4. 6 Tabel Tag | 44 |
| Table 4. 7 Tabel Bank..... | 44 |
| Table 4. 8 Tabel Expedisi | 45 |
| Table 4. 9 Tabel <i>Event</i> | 45 |
| Table 4. 10 Tabel <i>Workshop</i> | 45 |
| Table 4. 11 Tabel Paket | 47 |
| Table 4. 12 Tabel Saran | 47 |
| Table 4. 13 <i>Pseudocode AES Chiper block</i> | 57 |
| Table 4. 14 <i>Pseudocode AES Key Expansion</i> | 58 |
| Table 4. 15 <i>Pseudocode Enkripsi AES</i> | 60 |
| Table 4. 16 <i>Pseudocode dekripsi AES</i> | 73 |
| Table 4. 17 Pengujian Level <i>Admin</i> | 77 |
| Table 4. 18 Pengujian Level Pelanggan | 78 |

DAFTAR GAMBAR

| | |
|---|----|
| Gambar 2. 1 Metode Enkripsi (Prakoso, 2023) | 6 |
| Gambar 2. 2 CIA Triad(Veale, Brown and Getulio, 2020) | 8 |
| Gambar 2. 3 Diagram Proses Enkripsi <i>AES</i> (Cristy and Riandari, 2021)..... | 11 |
| Gambar 2. 4 Ilustrasi Transformasi <i>ByteSub()</i> <i>AES</i> (Lung and Munir, 1997) | 12 |
| Gambar 2. 5 Ilustrasi Transformasi <i>ShiftRow()</i> <i>AES</i> (Cristy and Riandari, 2021) | 12 |
| Gambar 2. 6 Ilustrasi Transformasi <i>Mixcolumn()</i> <i>AES</i> (Cristy and Riandari, 2021) | 13 |
| Gambar 2. 7 Ilustrasi Transformasi <i>Addroundkey()</i> <i>AES</i> (Cristy and Riandari, 2021) | 13 |
| Gambar 2. 8 Diagram Proses Enkripsi <i>AES</i> (Cristy and Riandari, 2021)..... | 14 |
| Gambar 2. 9 Tahapan Metode RAD (Hariyanto, 2021) | 18 |
| Gambar 3.1 Kerangka Berpikir..... | 28 |
| | |
| Gambar 4. 1 Logo Rumah Batik Palbatu | 32 |
| Gambar 4. 2 Enkripsi Pada Codeigniter..... | 53 |
| Gambar 4. 3 Library <i>AES</i> | 54 |
| Gambar 4. 4 Hasil Implementasi Enkripsi Data Pelanggan..... | 55 |
| Gambar 4. 5 Pembagian Block <i>Plaintext</i> | 61 |
| Gambar 4. 6 Pembuatan Counter Block..... | 63 |
| Gambar 4. 7 Proses <i>addroundkey</i> Awal..... | 64 |
| Gambar 4. 8 Proses <i>subbytes</i> tahap 1 | 66 |
| Gambar 4. 9 Proses <i>Shiftrows</i> tahap1 | 68 |
| Gambar 4. 10 Proses <i>mixcolumn</i> tahap 1 | 70 |
| Gambar 4. 11 Deskripsi Pada Codeigniter | 71 |
| Gambar 4. 12 Deskripsi Pada Codeigniter | 73 |
| Gambar 4. 13 Data Pelanggan Sebelum Enkripsi | 75 |
| Gambar 4. 14 Data Pelanggan Setelah Enkripsi | 76 |