

IMPLEMENTASI ALGORITMA KRIPTOGRAFI *HYBRID AES DAN RSA*
DALAM RANCANG BANGUN APLIKASI BANK SAMPAH
PANCADAYA BERBASIS WEB UNTUK KEAMANAN DATA
TRANSAKSI NASABAH

TUGAS AKHIR

Diajukan sebagai salah satu syarat memperoleh gelar sarjana (S1)
Pada program studi informatika, departemen Teknik elektronika
Fakultas Teknik Universitas negeri padang

Acc Jua
13/10/25



Acc Jua
Hesmi
192039
7/9 - 2025

MARDHYAH FATHANIA 'IZZATI
21346013

PROGRAM STUDI INFORMATIKA
DEPARTEMEN TEKNIK ELEKTRONIKA
FAKULTAS TEKNIK
UNIVERSITAS NEGERI PADANG
2025

HALAMAN PERSETUJUAN TUGAS AKHIR

Implementasi Algoritma Kriptografi *Hybrid AES dan RSA* Dalam Rancang Bangun Aplikasi Bank Sampah Pancadaya Berbasis Web untuk Keamanan Data Transaksi Nasabah

Nama : Mardhyah Fathania 'Izzati
NIM/TM : 21346013/2021
Program Studi : Informatika
Departemen : Teknik Elektronika
Fakultas : Teknik

Padang, Oktober 2025

Disetujui oleh:
Pembimbing



Widya Darwin, S.Pd., M.Pd.T.
NIDN. 009059303

Mengetahui,
Kepala Departemen Teknik Elektronika



Dr. Dedy Irfan, S.H., M.kom.
NIP. 197604082005011002

HALAMAN PENGESAHAN TUGAS AKHIR

Dinyatakan Lulus Setelah Dipertahankan di Depan Tim Penguji Tugas Akhir
Program Studi Informatika
Departemen Teknik Elektronika Fakultas Teknik
Universitas Negeri Padang

Judul : **Implementasi Algoritma Kriptografi Hybrid AES dan RSA Dalam Rancang Bangun Aplikasi Bank Sampah Pancadaya Berbasis Web untuk Keamanan Data Transaksi Nasabah**
Nama : Mardhyah Fathania 'Izzati
NIM/TM : 21346013/2021
Program Studi : Informatika
Departemen : Teknik Elektronika
Fakultas : Teknik

Padang, Oktober 2025

Ketua Penguji

Nama

Tanda Tangan

1. Ketua

Ahmaddul Hadi, S.Pd., M.Kom.

1. 

2. Anggota

Widya Darwin, S.Pd., M.Pd.T

2. 

3. Anggota

Dr. Resmi Dami, S.Kom., M.Kom.

3. 

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Mardhyah Fathania 'Izzati

TM/NIM : 2021/21346013

Program Studi : Informatika

Departemen : Teknik Elektronika

Fakultas : Teknik

Dengan ini saya menyatakan bahwa Tugas Akhir saya yang berjudul **"Implementasi Algoritma Kriptografi Hybrid AES dan RSA Dalam Rancang Bangun Aplikasi Bank Sampah Pancadaya Berbasis Web untuk Keamanan Data Transaksi Nasabah"** ini benar-benar karya saya sendiri. Sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang ditulis dan diterbitkan orang lain kecuali sebagai acuan atau kutipan dengan mengikuti aturan tata penulisan karya ilmiah yang lazim. Demikian pernyataan ini saya buat dengan penuh kesadaran dan rasa tanggung jawab sebagai anggota masyarakat ilmiah.

Padang, 14 Oktober 2025

Yang menyatakan,



Mardhyah Fathania 'Izzati

NIM. 21346013

ABSTRAK

Mardhyah Fathania Izzati, 2025. “Implementasi Algoritma Kriptografi *Hybrid AES dan RSA* Dalam Rancang Bangun Aplikasi Bank Sampah Pancadaya Berbasis Web untuk Keamanan Data Transaksi Nasabah” Tugas Akhir. Padang: Program Studi Informatika, Departemen Elektronika, Fakultas Teknik, Universitas Negeri Padang

Permasalahan pengelolaan sampah di Kota Padang menjadi tantangan serius karena tingginya timbulan sampah harian yang mencapai 660,06 ton per hari. Salah satu solusi yang diterapkan adalah pembentukan Bank Sampah Pancadaya sebagai Bank Sampah Induk (BSI) untuk meningkatkan kesadaran dan partisipasi masyarakat dalam pengelolaan sampah berbasis 3R (*reduce, reuse, recycle*). Namun, dalam pelaksanaannya masih ditemukan berbagai kendala seperti kehilangan buku tabungan nasabah, sulitnya pendataan transaksi, serta kurangnya integritas data antara catatan nasabah dan pembukuan bank sampah. Penelitian ini bertujuan untuk mengimplementasikan algoritma kriptografi hybrid, yaitu Advanced Encryption Standard (AES) dan Rivest Shamir Adleman (RSA), pada aplikasi Bank Sampah Pancadaya berbasis web guna menjaga keamanan data transaksi nasabah. Metode yang digunakan meliputi tahapan analisis kebutuhan, perancangan sistem, implementasi algoritma, dan pengujian keamanan data. Proses enkripsi dilakukan dengan AES untuk mengenkripsi data transaksi, sedangkan RSA digunakan untuk mengenkripsi kunci AES agar meningkatkan lapisan keamanan. Hasil penelitian menunjukkan bahwa penerapan algoritma kriptografi hybrid mampu menjaga kerahasiaan dan integritas data transaksi nasabah, serta mendukung peningkatan kualitas pelayanan Bank Sampah Pancadaya yang mengusung program konversi saldo menjadi emas.

Kata kunci: Kriptografi Hybrid, AES, RSA, Bank Sampah, Keamanan Data

KATA PENGANTAR



Puji dan syukur peneliti ucapkan atas hadirat Allah SWT yang telah melimpahkan rahmat, karunia, beserta hidayah-Nya kepada peneliti sehingga mampu menyelesaikan Tugas Akhir yang berjudul “**Implementasi Algoritma Kriptografi Hybrid AES dan RSA Dalam Rancang Bangun Aplikasi Bank Sampah Pancadaya Berbasis Web untuk Keamanan Data Transaksi Nasabah**”. Tugas Akhir ini dibuat sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Pendidikan Strata Satu (S1) pada Program Studi Informatika Fakultas Teknik Universitas Negeri Padang.

Penyelesaian Tugas Akhir ini tidak terlepas dari bimbingan, bantuan, serta dukungan berbagai pihak. Oleh karena itu peneliti mempersembahkan Tugas Akhir ini kepada orang-orang yang peneliti sayangi yang telah berjuang, berdoa, serta membantu dalam terciptanya Tugas Akhir ini yakni:

1. Dr. Ir. Krismadinata, S.T., M.T., selaku Rektor Universitas Negeri Padang, yang telah memberikan fasilitas serta kesempatan bagi mahasiswa untuk berkarya dan mengembangkan diri dalam bidang ilmu pengetahuan dan teknologi.
2. Bapak Prof. Dr. Muhammad Anwar, S.Pd., M.T., selaku Dekan Fakultas Teknik Universitas Negeri Padang.
3. Bapak Dr. Dedy Irfan, S.Pd, M.Kom., selaku Kepala Departemen Teknik Elektronika, Fakultas Teknik, Universitas Negeri Padang.

4. Dr. Yeka Hendriyani, S.Kom., M.Kom., selaku Koordinator Program Studi Informatika (S1), atas dukungan dan arahan yang diberikan.
5. Widya Darwin, S.Pd., M.Pd.T, selaku Dosen Pembimbing Tugas Akhir, atas segala bimbingan, arahan, nasihat, dan ilmu yang telah diberikan, baik secara langsung maupun tidak langsung, serta kesabaran dalam membimbing penulis.
6. Bapak Ahmaddul Hadi, S.Pd., M.Kom selaku Dosen Penelaah Pertama yang telah meluangkan waktu untuk memberikan bimbingan, arahan, nasihat, serta motivasi dalam menyelesaikan tugas akhir ini.
7. Dr. Resmi Darni, S.Kom., M.Kom., selaku dosen penelaah kedua, yang telah memberikan bimbingan, evaluasi, saran, dan kritik konstruktif demi penyempurnaan proposal ini.
8. Seluruh dosen dan staf Universitas Negeri Padang yang telah memberikan bantuan, dukungan, dan pembinaan selama masa perkuliahan.
9. Kedua orang tua penulis Ayah Usfa Yandri dan Bunda Nely, dua orang yang sangat berjasa dalam hidup penulis, dua orang yang selalu mengusahakan anak pertamanya ini menempuh pendidikan setinggi-tingginya. Kepada ayah penulis, terima kasih atas setiap cucuran keringat dan kerja keras yang engkau tukarkan menjadi sebuah nafkah demi anakmu bisa sampai kepada tahap ini, demi anakmu dapat mengenyam pendidikan sampai ke tingkat ini. Untuk bunda penulis, terima kasih atas segala motivasi, pesan, doa, dan harapan yang selalu mendampingi setiap langkah dan ikhtiar anakmu untuk menjadi seseorang yang berpendidikan. Terakhir, terima kasih atas segala hal yang kalian berikan yang tak terhitung jumlahnya.

10. Seluruh keluarga besar penulis terkhusus One, Unyiang, Unang, dan Uncu dengan tulus dan penuh rasa syukur penulis ingin mengucapkan terima kasih kepada beliau yang senantiasa memberikan perhatian, kasih sayang, doa, dan dukungan yang tiada hentinya.
11. Kepada Elsa, Putri, Kak Desi, Kak Hilda, Kak Kiki, dan Nava, dalam setiap lembar Tugas Akhir ini tersimpan jejak kehadiran kalian yang menyenangkan, yang senantiasa memberikan keceriaan, kehangatan, serta warna tersendiri dalam perjalanan akademik penulis.
12. Si pemeran utama “panitia 9” yang sudah banyak memberikan memori yang baik. Terimakasih sudah hadir di setiap lembar Tugas Akhir ini. Sungguh, tanpa kalian perjalanan akademik ini tak akan pernah ku lalui dengan segenap ketegaran yang kumiliki sekarang.
13. Terakhir, penulis berterima kasih kepada satu sosok gadis sederhana dengan hati kecil tetapi dengan impian besar. Terima kasih kepada penulis tugas akhir ini yaitu diriku sendiri, Mardhyah Fathania ‘Izzati. Terimakasih untuk bahu yang masih bertahan hingga saat ini dan terimakasih untuk tidak memenuhi kedagingan yang ditawarkan oleh dunia. Terimakasih sudah tetap berjalan di jalan Tuhan di tengah kepahitan yang menekan untuk menyerah.
14. Pihak-pihak lain yang tidak bisa disebutkan satu persatu yang telah memberikan sedikit atau banyak andil dan do’a kepada penulis dalam menyelesaikan tugas akhir ini.

Semoga semua motivasi, semangat, ilmu yang selalu saya ingat serta do'a yang diberikan mendapat imbalan dari Allah SWT sebagai amal dan ibadah. Sebagai

manusia biasa penulis menyadari penyusunan tugas akhir ini jauh dari kata sempurna karena keterbatasan kemampuan dari ilmu pengetahuan yang dimiliki oleh penulis. Oleh karenanya atas kesalahan dan kekurangan dalam penulisan tugas akhir ini, penulis memohon maaf dan bersedia menerima kritikan yang membangun.

Terakhir, harapan penulis, semoga tugas akhir ini dapat memberikan manfaat bagi siapa saja yang membacanya.

Padang, Agustus 2025

Penulis

DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	ii
DAFTAR ISI.....	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL	xi
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Identifikasi Masalah	9
C. Batasan Masalah.....	9
D. Rumusan Masalah	10
E. Tujuan Penelitian	10
F. Manfaat Penelitian	10
BAB II LANDASAN TEORI	12
A. Kriptografi.....	12
B. Bank Sampah	30
C. Metode Pengembangan Sistem	32
D. Perangkat Pengembang	34
BAB III METODE PENELITIAN.....	37
A. Metode Penelitian.....	37
B. Metode Analisis	38
C. Metode Pengembangan Sistem	40

BAB IV HASIL DAN PEMBAHASAN	75
A. Hasil dan Pembahasan Rancangan Aplikasi Bank Sampah.....	75
B. Hasil dan Pembahasan Proses Algoritma <i>Hybrid</i> AES dan RSA	84
C. Pengujian Sistem.....	96
D. Pengujian Algoritma	98
BAB V PENUTUP.....	101
A. Kesimpulan	101
B. Saran.....	101
DAFTAR PUSTAKA	103

DAFTAR GAMBAR

Gambar 1 Perbandingan Performa Algoritma terhadap Kecepatan Data	7
Gambar 2 Pebandingan Nilai Entropi	8
Gambar 3 Enkripsi dan Dekripsi dalam Pengiriman Pesan	13
Gambar 4 Contoh Teknik Substitusi	15
Gambar 5 Proses Skema Kriptografi Simetri	16
Gambar 6 Proses Skema Kriptografi Asimetri	16
Gambar 7 Diagram Proses Enkripsi di dalam AES (Rijindael)	20
Gambar 8 Hasil Transformasi <i>State</i> dalam Proses Enkripsi AES	26
Gambar 9 Hasil Transformasi <i>State</i> dalam Proses Enkripsi AES 7 -10	26
Gambar 10 Alur Pengelolaan Sampah	31
Gambar 11 Alur <i>Rapid Aplication Development</i> (RAD)	33
Gambar 12 <i>Use case</i> Diagram Bank Sampah	43
Gambar 13 <i>Activity Diagram</i> Login	44
Gambar 14 <i>Activity Diagram</i> Register Nasabah	45
Gambar 15 <i>Activity Diagram</i> Mengubah Jenis Sampah	46
Gambar 16 <i>Activity Diagram</i> Menambah Kategori Sampah	47
Gambar 17 <i>Activity Diagram</i> Melakukan Penyetoran Sampah	48
Gambar 18 <i>Activity Diagram</i> Menarik Saldo Nasabah	49
Gambar 19 <i>Activity Diagram</i> Menjual Sampah	50
Gambar 20 <i>Activity Diagram</i> Melihat Semua Transaksi	51
Gambar 21 <i>Activity Diagram</i> Rekap Transaksi	52

Gambar 22 <i>Activity Diagram</i> Mengubah Data Nasabah.....	53
Gambar 23 <i>Activity Diagram</i> Mengubah Data Admin	54
Gambar 24 <i>Activity Diagram</i> Melihat Info Saldo dan Harga Sampah	55
Gambar 25 <i>Class Diagram</i>	55
Gambar 26 <i>Database Schema</i>	56
Gambar 27 Desain Algoritma Hybrid Encryption.....	62
Gambar 28 Halaman <i>Login</i>	63
Gambar 29 Halaman Register Nasabah	64
Gambar 30 Desain Antar Muka Halaman Beranda.....	64
Gambar 31 Halaman Kelola Sampah.....	65
Gambar 32 Halaman Kategori Sampah.....	66
Gambar 33 Halaman Setor Sampah	67
Gambar 34 Halaman Tarik Saldo.....	67
Gambar 35 Halaman Jual Sampah	68
Gambar 36 Halaman Semua Transaksi	69
Gambar 37 Halaman Rekap Transaksi.....	69
Gambar 38 Halaman Data Admin.....	70
Gambar 39 Halaman Data Nasabah	71
Gambar 40 Halaman Detail User	71
Gambar 41 Halaman <i>Dashboard</i> Nasabah.....	72
Gambar 42 Tampilan Halaman <i>Login</i>	75
Gambar 43 Tampilan Halaman Register Nasabah	76
Gambar 44 Tampilan <i>Dashboard</i> Admin	76

Gambar 45 Tampilan Halaman Data Sampah.....	77
Gambar 46 Tampilan Halaman Tambah Sampah	77
Gambar 47 Tampilan Halaman Manage Kategori	78
Gambar 48 Tampilan Halaman Setor Sampah.....	78
Gambar 49 Tampilan Halaman Tarik Saldo	79
Gambar 50 Tampilan Halaman Jual Sampah.....	79
Gambar 51 Tampilan Halaman Semua Transaksi.....	80
Gambar 52 Tampilan Halaman Rekap Transaksi	80
Gambar 53 Tampilan Halaman Nasabah	81
Gambar 54 Tampilan Halaman Admin	81
Gambar 55 Tampilan Halaman Detail <i>User</i> Admin	82
Gambar 56 Tampilan Halaman Nota Transaksi.....	82
Gambar 57 Tampilan Halaman <i>Dashboard</i> Nasabah	83
Gambar 58 Tampilan Halaman Detail <i>User</i> Nasabah.....	83
Gambar 59 Data Terenkripsi yang Tersimpan pada	93
Gambar 60 Data Terenkripsi yang Tersimpan pada	94
Gambar 61 Pengujian menggunakan GTmetrix.....	97

DAFTAR TABEL

Tabel 1 Tiga Versi AES	18
Tabel 2 Table S-Bok di dalam AES	21
Tabel 3 S-Box AES (Substitution Box AES).....	22
Tabel 4 Transformasi <i>SubBytes</i> terhadap <i>state</i> hasil.....	22
Tabel 5 Transformasi <i>ShiftRows()</i>	23
Tabel 6 Transformasi <i>ShiftRows</i> terhadap <i>state</i> hasil	23
Tabel 7 Hasil transformasi <i>ShiftRows()</i> sebelumnya	24
Tabel 8 Transformasi <i>MixColumns</i> terhadap <i>state</i> hasil	25
Tabel 9 Rubrik Wawancara.....	39
Tabel 10 Identifikasi Analisis Masalah.....	41
Tabel 11 Tabel <i>user</i>	56
Tabel 12 Tabel Transaksi	57
Tabel 13 Tabel Setor Sampah	58
Tabel 14 Tabel Tarik Saldo.....	58
Tabel 15 Tabel Dompot.....	59
Tabel 16 Tabel Sampah.....	59
Tabel 17 Tabel Kategori sampah	59
Tabel 18 Tabel Jual Sampah	59
Tabel 19 Hasil engujian menggunakan GTmetrix	97
Tabel 20 Hasil Pengujian Brute-Force	100

BAB I

PENDAHULUAN

A. Latar Belakang

Undang-undang Republik Indonesia Nomor 18 Tahun 2008 tentang Pengelolaan Sampah menyatakan sampah merupakan sisa dari kegiatan sehari – hari manusia dan/atau proses alam yang berbentuk padat. Situasi ini memerlukan penanganan yang tepat, salah satunya melalui pengelolaan sampah dengan menerapkan prinsip 3R (*reduce, reuse, recycle*). Penerapan prinsip ini berperan dalam mengurangi jumlah sampah yang *dihasilkan* serta meningkatkan kualitas sampah sebelum diproses di Tempat Pemrosesan Akhir Sampah (TPA).

Kota Padang menghasilkan timbulan sampah harian tertinggi di Provinsi Sumatera Barat yaitu 660,06 ton per hari (KLHK, 2024). Maka dari itu, perlu adanya perubahan dalam pengelolaan sampah, khususnya dengan beralih dari paradigma tradisional (kumpulkan – angkut – buang) ke pendekatan yang lebih berkelanjutan, yaitu konsep 3R (*reduce, reuse, recycle*). Menanggapi hal ini, pemerintah kota Padang mulai menemukan alternatif pemecahan masalah penumpukan sampah dengan pengelolaan sampah yang lebih berdaya guna. Badan Pengendalian Dampak Lingkungan Daerah (Bapedalda) Kota Padang berdasarkan Undang-Undang No.18 tahun 2008 tentang pengelolaan sampah, menggalakan pemberdayaan masyarakat berbasis pelestarian lingkungan hidup dengan mendirikan Bank Sampah di Kota Padang sampai ke tingkat kelurahan yang dikelola oleh warga setempat. Dengan adanya Bank Sampah dalam

kehidupan masyarakat kota Padang, Sampah yang dulunya dibuang sebagai sampah konsumen kini dikumpulkan dan disimpan karena memiliki nilai ekonomi. (Rahma Fitri et al., 2024).

Bank sampah di Kota Padang tersebar di seluruh kecamatan yang ada di Kota Padang terutama pada kawasan pemukiman yang padat. Bank sampah di Kota Padang umumnya dikelola oleh kelompok LSM (Lembaga Swadaya Masyarakat), masyarakat, dan pemerintah setempat. Jenis sampah yang dikelola umumnya merupakan sampah kering seperti plastik, logam, kaca, kertas, dan beberapa ada yang mengolah sampah organik. Menurut data dari Dinas Lingkungan Hidup Kota Padang Tahun 2023, terdapat 2 bank sampah yang merupakan Bank Sampah Induk (BSI) salah satunya yaitu BSI Panca Daya di Kecamatan Kuranji (Ramadhani, 2024).

Bank sampah Pancadaya merupakan salah satu bank sampah yang ada di Kota Padang dan merupakan Bank Sampah Induk (BSI) untuk daerah Kota Padang. Bank sampah ini secara resmi didirikan pada tahun 2017, namun cikal bakal terbentuknya sudah direncanakan sejak 2011. Bank sampah ini terus berkembang dan memberikan edukasi kepada masyarakat maupun anggota bank sampahnya tentang apa dan bagaimana mengelola bank sampah, serta memberikan pelatihan membuat kerajinan dari sampah. BSI Panca Daya saat ini sudah memiliki lebih dari 1000 nasabah bank sampah dari setiap unit-unit bank sampah yang ada dan akan terus meningkatkan (Ramadhani, 2024).

Akan tetapi dalam proses pengimplementasiannya, dari hasil wawancara dengan salah satu pihak Dinas Lingkungan Hidup Kota Padang, masih terdapat

beberapa masalah, antara lain: nasabah sering tidak membawa buku tabungan, bahkan ada yang hilang, sulitnya mendata pemasukan sampah, kurangnya integritas data antara buku tabungan nasabah dengan pembukuan bank sampah, maka diperlukan sebuah aplikasi untuk pengolahan data yang efektif dan efisien, yang didalamnya dapat memiliki sistem penyimpanan data yang aman dan tentunya melengkapi aplikasi dengan teknik pengaman yang cukup baik untuk mengantisipasi adanya kemungkinan buruk yang akan terjadi seperti manipulasi data.

Dalam penelitian ini peneliti akan mengimplementasikan sistem pengamanan dengan menggunakan teknik kriptografi untuk transaksi nasabah khususnya setor sampah dan tarik saldo. Kriptografi adalah salah satu teknik yang sering digunakan untuk keamanan data. Kata kriptografi sendiri berasal dari bahasa Yunani, yakni *crypto* yang berarti rahasia dan *graphia* yang berarti tulisan. Secara sederhana, kriptografi dapat diartikan sebagai tulisan rahasia atau teknik untuk menyembunyikan isi informasi dari pihak yang tidak berwenang.

Salah satu jenis kriptografi yang digunakan dalam sistem ini adalah kriptografi simetris, yaitu metode enkripsi di mana kunci yang digunakan untuk mengenkripsi dan mendekripsi data adalah sama. Algoritma *Advanced Encryption Standard* (AES) merupakan algoritma simetris yang terkenal karena kecepatan. Dalam penerapannya, algoritma AES memerlukan sebuah kunci simetris yang harus dijaga kerahasiaannya, karena jika kunci tersebut diketahui oleh pihak tidak berwenang, maka seluruh data yang dienkripsi dapat dengan mudah diakses. Untuk menjaga keamanan kunci simetris dalam aplikasi ini,

penyimpanan kunci dilakukan secara terenkripsi menggunakan pendekatan kriptografi asimetris, yaitu RSA (*Rivest Shamir Adleman*). Berbeda dengan AES yang menggunakan satu kunci (simetris), RSA menggunakan sepasang kunci, yaitu kunci publik dan kunci privat.

Pendekatan ini dikenal sebagai *hybrid cryptosystem*, yaitu penggunaan gabungan antara algoritma enkripsi simetris AES dan asimetris RSA untuk meningkatkan keamanan proses enkripsi dan dekripsi data. Dalam *hybrid cryptosystem*, algoritma AES digunakan untuk mengenkripsi pesan karena kemampuannya dalam menangani data dalam jumlah besar dengan cepat dan efisien, sementara RSA digunakan untuk mengenkripsi kunci simetris tersebut menggunakan kunci publik. Dengan cara ini, sistem tidak hanya menjaga kerahasiaan isi pesan melalui AES, tetapi juga memastikan bahwa hanya penerima yang memiliki kunci privat RSA yang dapat membuka kunci AES dan membaca data tersebut. Proses ini diimplementasikan dengan memanfaatkan *library* OpenSSL, yang menyediakan berbagai fungsi kriptografi untuk mendukung proses enkripsi, dekripsi, dan manajemen kunci. Pendekatan ini bertujuan untuk mencegah kebocoran kunci akibat akses tidak sah terhadap sistem, serta meminimalisasi risiko penyalahgunaan kunci enkripsi oleh pihak yang tidak berwenang.

Penerapan pengamanan ini menjadi penting, meskipun secara nominal nilai transaksi dalam kegiatan setor sampah dan tarik saldo relatif kecil. Hal ini dikarenakan data transaksi memiliki nilai krusial dalam akumulasi saldo, keakuratan pencatatan, serta menjaga kepercayaan nasabah terhadap sistem. Jika

data ini tidak dilindungi dengan baik, maka potensi penyalahgunaan atau manipulasi data dapat terjadi. Terlebih lagi, Bank Sampah Pancadaya mengusung slogan “Memilah Sampah, Menabung Emas”, yang memungkinkan nasabah menukarkan saldo hasil setor sampah dengan emas.

Slogan ini merupakan bagian dari program kerja sama antara Bank Sampah Pancadaya dan PT Pegadaian, yang bertujuan untuk mendorong partisipasi masyarakat dalam pengelolaan sampah sekaligus memberikan manfaat ekonomi melalui tabungan emas. Dalam implementasinya, nasabah melakukan penyetoran dan pencairan saldo, baik dalam bentuk uang tunai maupun emas, langsung melalui pihak Bank Sampah Pancadaya. Dana hasil tabungan tersebut kemudian dikelola oleh Bank Sampah dan disimpan di Pegadaian melalui kerja sama resmi yang telah terjalin. Bank Sampah akan melakukan proses koordinasi dan transaksi dengan pihak Pegadaian untuk mengelola saldo emas atau uang dan memenuhi kebutuhan pencairan yang diajukan oleh nasabah sesuai dengan data yang tercatat dalam sistem.

Hal ini menunjukkan bahwa konversi saldo menjadi emas dalam sistem Bank Sampah tidak hanya memberikan manfaat ekonomi, tetapi juga turut meningkatkan nilai dan sensitivitas data transaksi nasabah. Tidak lagi sekadar mencatat hasil setor atau tarik saldo, transaksi kini mencerminkan kepemilikan aset yang bernilai dan memiliki stabilitas jangka panjang. Emas telah lama dikenal sebagai simbol kekayaan dan salah satu instrumen investasi yang paling stabil di tengah dinamika ekonomi global. Dalam beberapa dekade terakhir, harga emas menunjukkan tren peningkatan yang signifikan (Siagian, 2025). Jika

tidak dikelola dengan sistem keamanan yang baik, maka kebocoran atau perubahan data dapat menimbulkan kerugian nyata bagi nasabah dan menurunkan tingkat kepercayaan terhadap sistem bank sampah secara keseluruhan.

Seiring dengan meningkatnya sensitivitas dan nilai data transaksi akibat akibat penerapan sistem konversi saldo menjadi emas, maka kebutuhan akan sistem pengamanan menjadi semakin penting. Data transaksi tidak lagi hanya menyangkut saldo biasa, tetapi juga berkaitan dengan konversi ke dalam bentuk nilai tukar yang signifikan. Oleh karena itu, penerapan algoritma kriptografi *hybrid cryptosystem*, yang menggabungkan kecepatan dan efisiensi algoritma simetris AES dengan keamanan distribusi kunci dari algoritma asimetris RSA, menjadi solusi yang tepat. Pendekatan ini tidak hanya memastikan bahwa data transaksi tetap terlindungi dari akses yang tidak sah, tetapi juga menjamin keamanan kunci enkripsi itu sendiri.

Untuk mendukung pemilihan metode kriptografi yang tepat dalam pengamanan data transaksi, peneliti merujuk pada beberapa hasil studi sebelumnya. Berdasarkan jurnal yang peneliti dapatkan, terdapat tiga metode algoritma kriptografi yang paling sering digunakan, yaitu AES dan RSA, dan metode *Hybrid*. Ketiga metode tersebut mempunyai karakteristik keamanan yang berbeda, yang ditunjukkan melalui analisis hasil simulasi performa algoritma terhadap kecepatan pemrosesan data dan nilai entropi, sebagai berikut:

1. Performa algoritma terhadap kecepatan pemrosesan data

Untuk mengevaluasi efisiensi algoritma dalam proses enkripsi dan

dekripsi, dilakukan pengujian terhadap waktu pemrosesan pada berbagai jumlah data. Berikut adalah analisis berdasarkan hasil pengukuran waktu:

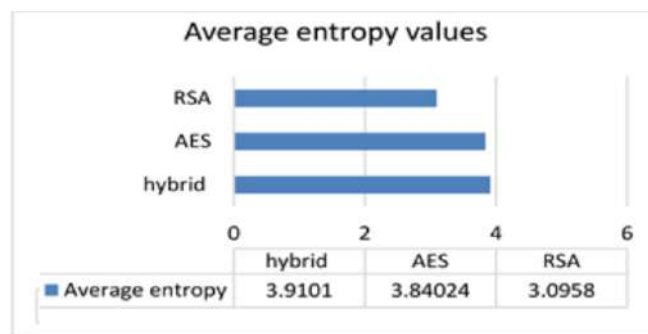
- a. AES menunjukkan performa tercepat. Untuk data 20 MB, proses enkripsi memakan waktu 19,067 detik dan dekripsi 305,064 detik. Ini membuktikan efisiensi tinggi dalam menangani data besar.
- b. RSA merupakan yang paling lambat. Bahkan untuk data 1 MB, enkripsi memerlukan waktu 2.777 detik dan dekripsi 229 detik. Pada data 20 MB, waktunya melonjak drastis, menunjukkan bahwa RSA kurang cocok untuk enkripsi data besar dan lebih sesuai untuk enkripsi kunci.
- c. *Hybrid encryption* (gabungan AES dan RSA) memberikan hasil yang stabil. Untuk data 20 MB, waktu enkripsi 19,867 detik dan dekripsi 315,064 detik. Meskipun sedikit lebih lambat dari AES, metode ini jauh lebih efisien dibanding RSA dan menawarkan keseimbangan antara kecepatan dan keamanan.

TYPE	Amount of data	Encrypted data (M)	Encryption time (s)	Decryption time (s)
AES	1	2.034	0.153	0.305
	5	10.172	0.763	1.525
	10	101.724	3.813	15.253
	20	2034.472	19.067	305.064
RSA	1	1.001	2777.778	229,166.667
	5	5.007	13,888.889	1,145,833.333
	10	25.035	69,444.444	11,458,333.333
	20	125.174	347,222.222	229,166,666.667
Hybrid encryption	1	2.134	0.183	0.405
	5	11.172	0.963	1.895
	10	109.724	4.213	16.153
	20	2087.472	19.867	315.064

Gambar 1 Perbandingan Performa Algoritma terhadap Kecepatan Data
(Sumber : Lu & Mohamed, 2021)

2. Nilai entropi

Nilai entropi menunjukkan tingkat keacakan data hasil enkripsi. Berdasarkan hasil pengukuran, metode *Hybrid* memiliki nilai entropi tertinggi, diikuti oleh AES, sedangkan RSA memiliki nilai entropi terendah. Hal ini mengindikasikan bahwa data terenkripsi dengan metode *Hybrid* cenderung lebih sulit untuk diprediksi atau diurai.



Gambar 2 Pebandingan Nilai Entropi
(Sumber : Lu & Mohamed, 2021)

Berdasarkan hasil analisis (Lu & Mohamed, 2021), algoritma *Hybrid* terbukti paling unggul karena mampu menggabungkan kecepatan dan keamanan secara seimbang. Dengan nilai entropi tertinggi (3.9101), *Hybrid* menghasilkan data terenkripsi yang paling acak dan sulit diprediksi, sekaligus tetap efisien dalam waktu pemrosesan. AES memang lebih cepat, namun sedikit kalah dalam aspek keamanan. Sementara RSA menunjukkan performa paling lambat dan entropi terendah, sehingga kurang efektif untuk data dalam jumlah besar.

Merujuk pada kelebihan yang dimiliki oleh metode kriptografi *Hybrid*, yang menggabungkan kecepatan algoritma simetris AES dan keamanan pertukaran kunci dari algoritma asimetris RSA, pada penjelasan yang sudah disebutkan diatas maka penulis mengangkat topik dengan judul Implementasi Algoritma

Kriptografi *Hybrid AES dan RSA* dalam Rancang Bangun Aplikasi Bank Sampah Pancadaya Berbasis Web untuk Keamanan Data Transaksi Nasabah.

B. Identifikasi Masalah

Berdasarkan latar belakang yang diuraikan terdapat beberapa masalah yang diidentifikasi terkait:

1. Nasabah sering tidak membawa atau bahkan kehilangan buku tabungan, sehingga menyulitkan proses pencatatan transaksi dan pengecekan saldo.
2. Pencatatan pemasukan sampah masih dilakukan secara manual, yang berisiko menyebabkan kesalahan data dan keterlambatan dalam pengolahan informasi.
3. Belum diterapkannya teknik pengamanan yang cukup baik dalam sistem pengolahan data meningkatkan risiko akses tidak sah terhadap informasi transaksi nasabah.

C. Batasan Masalah

Dalam penelitian ini, terdapat beberapa batasan yang diterapkan untuk memperjelas ruang lingkup dan fokus penelitian, yaitu:

1. Penelitian ini mengimplementasikan algoritma kriptografi *hybrid*, yaitu kombinasi AES dan RSA. AES digunakan untuk mengenkripsi data transaksi nasabah, sedangkan RSA digunakan untuk mengenkripsi kunci AES guna mengamankan proses pertukaran kunci.
2. Untuk memfasilitasi proses enkripsi data dan pengelolaan kunci, penelitian ini menggunakan *library* OpenSSL yang mendukung integrasi algoritma AES dan RSA.

3. Bahasa pemrograman dan sistem *Database* yang digunakan adalah PHP sebagai bahasa pemrograman, MySQL sebagai *Database server*, XAMPP sebagai *webserver*.

D. Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah bagaimana mengimplementasikan algoritma kriptografi *hybrid* kombinasi *Advanced Encryption Standard* (AES) dan *Rivest Shamir Adleman* (RSA) dalam rancang bangun Aplikasi Bank Sampah Pancadaya untuk Keamanan Data Transaksi Nasabah?

E. Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma kriptografi *hybrid* yaitu *Advanced Encryption Standard* (AES) dan *Rivest Shamir Adleman* (RSA) dalam perancangan aplikasi Bank Sampah Pancadaya guna menjaga keamanan data transaksi nasabah serta meningkatkan kualitas pelayanan Bank Sampah Induk Pancadaya Kota Padang.

F. Manfaat Penelitian

Sesuai dengan permasalahan dan tujuan penelitian, maka manfaat penelitian dapat dirumuskan sebagai berikut:

1. Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan kontribusi pemikiran yang substansial sebagai tambahan kepada pengetahuan atau literatur ilmiah yang

ada, yang dapat digunakan sebagai referensi oleh peneliti lain yang tertarik dalam melakukan studi serupa.

2. Manfaat Praktis

a. Bagi Penulis

- 1) Memberikan pemahaman mengenai penerapan algoritma kriptografi *hybrid*, yaitu kombinasi *Advanced Encryption Standard* (AES) dan *Rivest Shamir Adleman* (RSA), dalam mengamankan data transaksi nasabah, sehingga dapat meningkatkan kesadaran akan pentingnya keamanan data dalam sistem informasi.
- 2) Menambah pengetahuan tentang cara kerja bank sampah, termasuk mekanisme pencatatan transaksi, pengelolaan saldo, serta dampak sosial dan lingkungan dari penerapan sistem digital dalam pengelolaan sampah.

b. Bagi tempat penelitian

- 1) Pengurus dapat melakukan transaksi nasabah dengan lebih efisien tanpa perlu mencatat secara manual di buku besar, sehingga data lebih terintegrasi dan mudah dipantau, termasuk dalam pencatatan pemasukan sampah serta pengelolaan saldo.
- 2) Proses pengelolaan keuangan yang terstruktur dengan baik dan valid.
- 3) Memudahkan nasabah dalam melakukan pengecekan riwayat transaksi mereka.
- 4) Tingkat keamanan data yang tinggi agar meningkatkan kepercayaan nasabah dalam berpartisipasi di kegiatan bank sampah.

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan hasil dan pembahasan untuk menjawab rumusan masalah yang ada di dalam penelitian ini, maka dapat ditarik kesimpulan bahwa implementasi kriptografi hybrid berhasil diterapkan dalam Aplikasi Bank Sampah Pancadaya dengan menggabungkan algoritma AES untuk mengenkripsi data transaksi nasabah dan RSA untuk mengenkripsi kunci AES. Penerapan ini tidak hanya meningkatkan lapisan keamanan data, tetapi juga mendukung kualitas pelayanan Bank Sampah Induk Pancadaya Kota Padang melalui pengelolaan data yang lebih aman dan terintegrasi antara bank sampah dengan nasabah.

B. Saran

Aplikasi yang penulis buat tentu saja masih belum sempurna, masih banyak hal yang dapat dikembangkan guna membuat manfaat aplikasi menjadi lebih baik lagi untuk kedepannya. Oleh karena itu penulis juga menyampaikan beberapa saran untuk pengembangan selanjutnya, yaitu:

1. Sistem ini nantinya masih dapat dikembangkan lebih lanjut dengan mengintegrasikan algoritma kriptografi tambahan. Tidak hanya terbatas pada penggunaan AES dan RSA, namun juga dapat memanfaatkan algoritma keamanan lain yang menawarkan tingkat perlindungan data yang lebih sempurna.

2. Penelitian selanjutnya diharapkan dapat mengembangkan aplikasi menjadi lebih baik, dengan tampilan yang lebih dinamis. Pengembangan dapat diarahkan menggunakan pendekatan *mobile-first* agar antarmuka pengguna lebih responsif dan optimal digunakan pada perangkat *mobile*.

DAFTAR PUSTAKA

- Arywa, V. U. (2025). *Sistem Distribusi E-Book Berbasis Kriptografi Asimetris Menggunakan Algoritma Rsa Untuk Perlindungan Hak Cipta*. Universitas Islam Indonesia.
- Fadillah, S. N. (2021). *IMPLEMENTASI ALGORITMA KRIPTOGRAFI HILL CIPHER DENGAN KUNCI TERENKRIPSI RIVEST SHAMIR ADLEMAN (RSA) UNTUK MENINGKATKAN KEAMANAN CITRA DIGITAL*. Universitas Hasanuddin.
- Hardiyantik, N. (2023). *Implementasi Algoritma Blum-Blum Shub pada Algoritma One Time Pad (OTP) Cipher dalam Pengamanan Pesan*. Universitas Islam Negeri Maulana Malik Ibrahim Malang.
- Hidayat, M., Tahir, M., Sukriyadi, A., & Sulton, A. (2023). Penerapan Kriptografi Caesar Chiper dalam Pengamanan Data. *Jurnal Ilmiah Multidisiplin*, 2(03), 35–41.
- Hidayat, N., & Hati, K. (2021a). Penerapan Metode Rapid Application Development (RAD) dalam Rancang Bangun Sistem Informasi Rapor Online (SIRALINE). *Jurnal Sistem Informasi*, 10(1), 8–17.
- Hidayat, N., & Hati, K. (2021b). Penerapan Metode Rapid Application Development (RAD) dalam Rancang Bangun Sistem Informasi Rapor Online (SIRALINE). *Jurnal Sistem Informasi*, 10(1), 8–17.
- KLHK, K. L. H. dan K. (2024). *Timbulan Sampah Kota Padang Tahun 2024*. Kementerian Lingkungan Hidup Dan Kehutanan. <https://sipsn.kemenlh.go.id/sipsn/public/data/timbulan>
- Lu, Z., & Mohamed, H. (2021). A Complex Encryption System Design Implemented by AES. *Journal of Information Security*, 12(02), 177–187. <https://doi.org/10.4236/jis.2021.122009>
- Munir, R. (2023a). *Advanced Encryption Standard (AES)*. <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/08%20-%20AES-2023.pdf>
- Munir, R. (2023b). *Kriptografi Klasik (Bagian 1)*. Program Studi Teknik Informatika, STEI ITB.

- Ningsih, K. S., Aruan, N. J., & Ikhsan, M. (2022). Aplikasi buku tamu menggunakan fitur kamera dan Ajax berbasis website pada Kantor Dispora Kota Medan. *SITek (Jurnal Sains, Informasi Dan Teknologi)*, 1(3), 94–95.
- Nurmasari, N., Komalasari, E., Mulianto, B., Nurman, N., & Amrillah, M. F. (2024). PELATIHAN INOVASI BANK SAMPAH PLASTIK UNTUK PENINGKATAN PENDAPATAN EKONOMI MASYARAKAT DI BANK SAMPAH PUAN SARI MANDIRI. *Jurnal ADAM: Jurnal Pengabdian Masyarakat*, 3(1), 35–40.
- Rahma Fitri, N., Surya Himawan, A., Syiendi Fadillah, A., Putri Dahayu, H., & Marweny, E. (2024). *Mengulas Regulasi Terkait Mekanisme Pengelolaan Sampah Melalui Bank Sampah Di Kota Padang*. 02(1), 38–42. <https://jurnal.kopusindo.com/index.php/jkhkp>
- Ramadhani, H. (2024). *Kajian kinerja pengelolaan Bank Sampah Induk Panca Daya Kota Padang berdasarkan PermenLHK No. 14 Tahun 2021*.
- Rudianto, B., Achyani, Y. E., & Ariyati, I. (2021). Rancang Bangun Sistem Informasi Persediaan Obat Berbasis Web Menggunakan Model RAD. *Jurnal Khatulistiwa Informatika*, 7(2), 214–221.
- Safitri, S. I. (2023). *Algoritma Hybrid Menggunakan Myszkowski Cipher Dan Rsa Untuk Mengamankan Pesan Teks*. Universitas Islam Negeri Maulana Malik Ibrahim Malang.
- Setyawati, N. Y., Khofid, A. N., Rundi, A. U. B., & Wati, V. (2021). Modifikasi Kriptografi Klasik Kombinasi Metode Vigenere Cipher dan Caesar Cipher. *Journal of Smart System*, 1(1), 1–8.
- Siagian, R. R. A.-A. (2025). Persepsi Masyarakat Indonesia Terhadap Kenaikan Harga Emas Sebagai Instrumen Investasi Jangka Panjang: Sebuah Tinjauan Literatur. *Future Academia: The Journal of Multidisciplinary Research on Scientific and Advanced*, 3(1), 72–79. <https://doi.org/10.61579/future.v3i1.298>
- Widyawan, D., & Imelda, I. (2021). Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi. *SKANIKA: Sistem Komputer Dan Teknik Informatika*, 4(1), 15–22.

Wijaya, M. E. B. A., & Megawati, S. (2024). Implementasi Kebijakan Pengelolaan Sampah Pada Bank Sampah Induk Dhuawar Sejahtera di Dinas Lingkungan Hidup Kabupaten Kulon Progo. *Publika*, 991–997.