LintekEdu: Jurnal Literasi dan Teknologi Pendidikan

https://ejurnals.com/ojs/index.php/jltp Vol. 6, No. 2, Juni 2025

PENGAMANAN TEKS SMS MELALUI PENDEKATAN MULTIPLE ENCRYPTION MENGGUNAKAN ALGORITMA RSA DAN 3DES

Delmina Meidita Sekab[1], Matilda Nuis[2], Maria Etriana Putri Sanjaya[3], Yovita Seuk Nahak[4], Sella Krisdianti[5], Alfeus Tenis[6]

[1,2,3,4,5,6]Universitas Timor

Email: dellasekab@gmail.com[1], tildatsu407@gmail.com[2], mariaetrianaputrisanjaya@gmail.com[3], yovienahak495@gmail.com[4], sellakrisdianti14@gmail.com[5], tenisalfa42@gmail.com[6]

Abstract: *Short Message Service (SMS) is still widely used, especially for critical services such as banking, system notifications, and two-factor authentication. However, SMS by default lacks encryption features, making it highly vulnerable to eavesdropping and interception by third parties. This article proposes a multiple encryption approach, securing SMS messages using a combination of the asymmetric cryptographic algorithm RSA and the symmetric algorithm 3DES. RSA is used to encrypt the 3DES session key, while 3DES is employed to efficiently encrypt the message content. This process is implemented through a mobile application running on both the sender's and receiver's devices. Testing was conducted to evaluate the system's security, efficiency, and resistance to interception. The results show that the system effectively preserves message confidentiality, resolves the issue of symmetric key distribution, and generates ciphertext that cannot be deciphered without the RSA private key. The main challenges lie in the long ciphertext that may cause SMS fragmentation and the dependency on a custom application on both sides. With this approach, SMS security can be enhanced without modifying the operator's network infrastructure. This system is well-suited for sending sensitive messages in environments with limited internet access.*
Keywords: *Cryptography, Hybrid Encryption, Message Confidentiality, Multiple Encryption, Multiple Encryption, RSA, SMS, Security, 3DES.*

Abstrak: Komunikasi melalui Short Message Service (SMS) masih banyak digunakan, terutama untuk layanan penting seperti perbankan, notifikasi sistem, dan autentikasi dua faktor. Namun, SMS secara default tidak memiliki fitur enkripsi, sehingga sangat rentan terhadap penyadapan dan intersepsi oleh pihak ketiga. Artikel ini mengusulkan pendekatan multiple encryption, yaitu pengamanan pesan SMS menggunakan kombinasi algoritma kriptografi asimetris RSA dan kriptografi simetris 3DES. RSA digunakan untuk mengenkripsi kunci sesi 3DES, sementara 3DES digunakan untuk mengenkripsi isi pesan secara efisien. Proses ini dilakukan dalam aplikasi mobile yang berjalan di sisi pengirim dan penerima. Pengujian dilakukan untuk mengevaluasi keamanan, efisiensi, dan ketahanan sistem terhadap penyadapan. Hasil menunjukkan bahwa sistem berhasil menjaga kerahasiaan pesan,

menyelesaikan masalah distribusi kunci rahasia, dan menghasilkan enkripsi yang tidak dapat dibaca oleh pihak tanpa kunci privat RSA. Tantangan utama adalah panjang ciphertext yang menyebabkan fragmentasi pesan, dan ketergantungan pada aplikasi khusus di kedua sisi. Dengan pendekatan ini, pengamanan SMS dapat ditingkatkan tanpa perlu mengubah infrastruktur jaringan operator. Sistem ini cocok diterapkan untuk pengiriman pesan penting pada lingkungan dengan keterbatasan akses internet.

Kata Kunci: Enkripsi Hibrida, Keamanan, Kriptografi, Multiple Encryption RSA, Kerahasiaan Pesan, SMS, 3DES.

PENDAHULUAN

Short Message Service (SMS) merupakan salah satu teknologi komunikasi berbasis teks yang paling awal dan masih digunakan secara luas hingga saat ini. Meskipun berbagai aplikasi pesan instan modern seperti WhatsApp, Telegram, dan Signal telah menawarkan fitur keamanan canggih seperti enkripsi end-to-end, SMS tetap menjadi pilihan utama untuk beberapa jenis layanan penting. Hal ini terutama berlaku dalam konteks pengiriman One Time Password (OTP), autentikasi dua faktor (2FA), transaksi perbankan, serta komunikasi di wilayah dengan keterbatasan jaringan internet atau dalam sistem yang hanya mendukung layanan GSM konvensional.

Namun, dari sisi keamanan, SMS memiliki kelemahan mendasar yang tidak dapat diabaikan. Secara teknis, pesan SMS dikirim dalam bentuk plaintext (teks biasa) melalui kanal kontrol jaringan seluler tanpa adanya mekanisme enkripsi bawaan dalam protokol standarnya. Akibatnya, pesan yang dikirimkan dapat dengan mudah diintersep dan dibaca oleh pihak ketiga apabila mereka memiliki akses ke infrastruktur jaringan seluler atau menggunakan alat penyadap (sniffer) seperti IMSI Catcher atau StingRay. Kondisi ini sangat membahayakan terutama ketika informasi yang dikirim bersifat sensitif, seperti data identitas, kode transaksi, atau informasi autentikasi.

Berbagai upaya telah dilakukan untuk meningkatkan keamanan komunikasi mobile, salah satunya dengan menerapkan kriptografi pada sisi aplikasi (application layer encryption). Kriptografi memungkinkan data dikonversi menjadi bentuk terenkripsi yang tidak dapat dipahami tanpa kunci tertentu. Namun, pemilihan algoritma kriptografi yang tepat menjadi tantangan tersendiri. Algoritma simetris seperti Triple DES (3DES) sangat efisien dalam hal

kecepatan enkripsi dan cocok digunakan untuk data berukuran besar atau proses enkripsi berulang, tetapi mengalami kendala dalam distribusi kunci secara aman. Sebaliknya, algoritma asimetris seperti RSA memungkinkan pengelolaan kunci secara lebih aman melalui pasangan kunci publik dan privat, namun secara komputasional lebih berat dan tidak cocok digunakan untuk mengenkripsi pesan berukuran besar.

Untuk menjawab tantangan tersebut, pendekatan multiple encryption atau enkripsi hibrida menjadi solusi yang banyak diterapkan dalam sistem komunikasi modern. Pendekatan ini menggabungkan keunggulan dari kedua jenis algoritma: algoritma asimetris (RSA) digunakan untuk mengenkripsi kunci simetris yang akan digunakan, sedangkan algoritma simetris (3DES) digunakan untuk mengenkripsi isi pesan itu sendiri. Dengan cara ini, diperoleh sistem yang efisien sekaligus aman, karena proses distribusi kunci tidak lagi menjadi titik lemah.

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem pengamanan pesan SMS berbasis multiple encryption yang mengombinasikan RSA dan 3DES. Sistem ini diimplementasikan dalam bentuk prototipe aplikasi Android yang mampu melakukan proses enkripsi dan dekripsi secara otomatis. Selain itu, penelitian ini juga mengevaluasi efektivitas pendekatan tersebut dari sisi keamanan, efisiensi, dan ketahanannya terhadap potensi penyadapan. Dengan demikian, hasil penelitian ini diharapkan dapat menjadi kontribusi dalam pengembangan sistem komunikasi yang lebih aman pada jaringan seluler konvensional.

TINJAUAN PUSTAKA

1. Short Message Service (SMS)

   SMS adalah layanan telekomunikasi yang memungkinkan pengiriman pesan teks pendek, umumnya dibatasi hingga 160 karakter 7-bit ASCII, antar perangkat seluler. Pesan ini ditransmisikan melalui kanal kontrol jaringan seluler, seringkali memanfaatkan infrastruktur SS7 [4]. Karena tidak adanya enkripsi bawaan pada protokol standar SMS, konten pesan dapat diintersep jika seseorang memiliki akses ke jaringan atau menggunakan perangkat penyadap.

2. Kriptografi : Simetris dan Asimetris

   Kriptografi adalah studi tentang teknik komunikasi aman di hadapan pihak ketiga. Dua paradigma utama adalah :

1) Kriptografi Kunci Simetris

Menggunakan satu kunci rahasia yang sama untuk proses enkripsi dan dekripsi. Contohnya termasuk DES, 3DES, dan AES. Keunggulannya terletak pada kecepatan komputasi. Kelemahan utamanya adalah masalah distribusi kunci : bagaimana cara mengirimkan kunci rahasia dengan aman kepada penerima?

2) Kriptografi Kunci Asimetris (Kunci Publik)

Menggunakan sepasang kunci matematis yang saling terkait: kunci publik (dapat dibagikan secara luas, digunakan untuk enkripsi atau verifikasi tanda tangan) dan kunci privat (harus dijaga kerahasiaannya oleh pemilik, digunakan untuk dekripsi atau pembuatan tanda tangan). Contoh populer adalah RSA dan Elliptic Curve Cryptography (ECC). Keunggulannya adalah memecahkan masalah distribusi kunci simetris. Namun, secara komputasional lebih berat dibandingkan algoritma simetris.

3. Algoritma 3DES (Triple Data Encryption Standard)

3DES merupakan peningkatan dari algoritma DES. Ia menerapkan proses enkripsi DES sebanyak tiga kali pada setiap blok data, biasanya dalam mode Encrypt-Decrypt-Encrypt (EDE) menggunakan dua atau tiga kunci yang berbeda [2]. Langkah ini secara signifikan meningkatkan ketahanan terhadap serangan brute-force dibandingkan DES tunggal. Meskipun standar enkripsi modern seperti AES kini lebih disukai karena efisiensi dan keamanan yang lebih tinggi [6], 3DES masih dianggap cukup aman untuk banyak aplikasi warisan atau skenario tertentu.

4. Algoritma RSA (Rivest-Shamir-Adleman)

RSA adalah algoritma kriptografi kunci publik yang paling dikenal dan banyak digunakan [3]. Keamanannya bersandar pada kesulitan komputasi untuk memfaktorkan bilangan bulat besar yang merupakan hasil kali dari dua bilangan prima raksasa. RSA sangat cocok untuk tugas-tugas seperti enkripsi data berukuran kecil (misalnya, kunci simetris) dan implementasi tanda tangan digital untuk memastikan autentikasi dan integritas data.

5. Enkripsi Hibrida (Multiple Encryption)

Pendekatan ini secara cerdas menggabungkan keunggulan kriptografi simetris dan asimetris [5]. Skema tipikalnya adalah sebagai berikut :

1) Pengirim menghasilkan kunci simetris acak (kunci sesi) untuk satu sesi komunikasi.

2) Pengirim mengenkripsi pesan utama menggunakan algoritma simetris (misal, 3DES atau AES) dengan kunci sesi tersebut. Ini cepat dan efisien.
3) Pengirim mengenkripsi kunci sesi (yang relatif kecil) menggunakan kunci publik RSA milik penerima. Ini aman karena hanya penerima dengan kunci privat yang cocok yang dapat mendekripsinya.
4) Pengirim mengirimkan pesan terenkripsi (hasil langkah 2) dan kunci sesi terenkripsi (hasil langkah 3) kepada penerima.
5) Penerima menggunakan kunci privat RSA-nya untuk mendekripsi kunci sesi terenkripsi.
6) Penerima menggunakan kunci sesi yang diperoleh untuk mendekripsi pesan utama.

RESEARCH METHODS

Penelitian ini menggunakan pendekatan rekayasa perangkat lunak eksperimental untuk merancang dan mengimplementasikan sistem pengamanan SMS berbasis enkripsi hibrida (multiple encryption) dengan algoritma RSA dan 3DES. Penelitian ini dilakukan dalam beberapa tahap, yaitu perancangan sistem, pengembangan aplikasi prototipe, dan pengujian sistem.

1. Metodologi Pengembangan Sistem

Metode yang digunakan dalam pengembangan adalah metode *Waterfall*, karena alur prosesnya yang terstruktur dan cocok untuk pengembangan sistem dengan spesifikasi tetap. Tahapan yang diterapkan antara lain :

1) Analisis Kebutuhan

   Menentukan kebutuhan fungsional sistem pengamanan SMS, seperti proses input pesan, enkripsi, dekripsi, dan pengiriman SMS.

2) Perancangan Sistem (System Design)

   Merancang arsitektur sistem yang melibatkan dua modul utama: pengirim dan penerima. Merancang alur data, format payload, dan pemisahan logika antara enkripsi simetris dan asimetris.

3) Implementasi

   Mengembangkan prototipe aplikasi Android menggunakan bahasa pemrograman Java dan pustaka kriptografi (seperti BouncyCastle untuk RSA dan 3DES). RSA digunakan untuk enkripsi kunci sesi, sementara 3DES digunakan untuk enkripsi isi pesan.

4) Pengujian Sistem

   Melakukan pengujian fungsional terhadap kemampuan aplikasi dalam mengenkripsi dan mendekripsi pesan dengan benar. Selain itu, dilakukan uji keamanan terhadap potensi kebocoran informasi.

2. Arsitektur Sistem

Sistem ini dirancang untuk berjalan pada dua perangkat mobile :

1) Pengirim (Sender)
   a) Menginput pesan plaintext
   b) Menghasilkan kunci sesi 3DES acak
   c) Mengenkripsi pesan dengan 3DES
   d) Mengenkripsi kunci sesi dengan RSA
   e) Menggabungkan hasil enkripsi dan mengirimkan melalui SMS
2) Penerima (Receiver)
   a) Menerima SMS terenkripsi

b) Memisahkan pesan terenkripsi dan kunci sesi terenkripsi
c) Mendekripsi kunci sesi dengan RSA
d) Mendekripsi pesan dengan 3DES
e) Menampilkan pesan asli kepada pengguna

3. Spesifikasi Perangkat Uji
   1) Perangkat keras
      a) Dua unit smartphone Android minimal Android 8.0
      b) Prosesor minimal Quad-core 1.5 GHz
      c) RAM minimal 2 GB
   2) Perangkat lunak
      a) Android Studio untuk pengembangan
      b) Library kriptografi: BouncyCastle, Java Security
      c) Emulator dan real device untuk pengujian

4. Teknik Pengujian
   1) Black-box Testing
      Menguji fungsionalitas aplikasi dari sisi pengguna. Pengujian dilakukan pada skenario : pengiriman pesan biasa, pesan panjang, dan pesan dengan karakter khusus.
      a) Pengujian Ketahanan Keamanan
         Mensimulasikan penyadapan terhadap SMS dan memverifikasi bahwa data hasil sadapan tidak dapat dibaca tanpa kunci privat.
      b) Analisis Kinerja
         Mengukur waktu yang dibutuhkan untuk proses enkripsi dan dekripsi. Parameter yang diamati adalah waktu rata-rata proses per pesan dan keberhasilan pemulihan pesan.

5. Indikator Keberhasilan
   Sistem dianggap berhasil apabila memenuhi kriteria beriku t:
   1) Pesan dapat dikirim dan diterima dalam bentuk terenkripsi.
   2) Pesan hanya dapat didekripsi oleh penerima yang memiliki kunci privat RSA yang sesuai.

3) Pesan asli dapat direkonstruksi secara utuh tanpa kesalahan.
4) Hasil enkripsi tidak dapat dipecahkan tanpa akses ke kunci yang sesuai.

HASIL DAN PEMBAHASAN

1. Proses Enkripsi Pesan

Tahapan enkripsi dimulai dari sisi pengirim (sender). Berikut adalah langkah-langkah teknisnya :

a. Input Pesan

Pengguna mengetik pesan SMS biasa ke dalam aplikasi (contoh: "Kode OTP Anda adalah 982134").

b. Pembuatan Kunci Sesi (Session Key) 3DES

Sistem secara otomatis membangkitkan kunci simetris acak (random 168-bit) untuk algoritma 3DES. Biasanya kunci ini terdiri dari tiga buah kunci DES (56-bit × 3).

Contoh pseudokey :

K = [K1, K2, K3] → 168-bit

c. Enkripsi Isi Pesan dengan 3DES

Pesan asli di-enkripsi menggunakan 3DES dalam mode operasi seperti CBC (Cipher Block Chaining) untuk memperkuat keamanan dengan IV (Initialization Vector) acak.

Langkah enkripsi 3DES :

C = 3DES_encrypt(Plaintext, K)

Contoh hasil :

C = "r9q2x8uABkF1AeiGr1oFsg=="

d. Enkripsi Kunci Sesi dengan RSA

Kunci sesi yang digunakan pada 3DES kemudian dienkripsi dengan kunci publik RSA milik penerima. Tujuannya adalah agar hanya penerima yang bisa mendekripsi kunci ini menggunakan kunci privatnya.

Langkah enkripsi RSA :

Ek = RSA_encrypt(K, PublicKey_receiver)

Contoh hasil (base64) :

Ek = "MIIBIjANBgkqhkiG9w0BAQ...==" (hasil panjang ciphertext RSA)

e. Penggabungan Hasil

Ciphertext 3DES (C) dan kunci sesi terenkripsi RSA (Ek) dikodekan dalam format tertentu (misal Base64 atau JSON) agar bisa dikirim sebagai SMS.

Contoh payload yang dikirim :

[ENCRYPTED_KEY]: MIIBIjANBgkqhkiG...

[ENCRYPTED_MESSAGE]: r9q2x8uABkF1AeiGr1oFsg==

Karena panjang pesan terenkripsi biasanya melebihi 160 karakter, payload akan dibagi ke dalam beberapa SMS concatenated (dengan penanda urutan).

2. Proses Penerimaan dan Dekripsi Pesan

Di sisi penerima (receiver), aplikasi menjalankan proses dekripsi berikut:

a. Pembacaan Pesan

Aplikasi membaca SMS yang diterima dan mengekstrak dua bagian penting:

1) Ek : kunci sesi terenkripsi (RSA)
2) C: pesan terenkripsi (3DES)

b. Dekripsi Kunci Sesi dengan Kunci Privat RSA

Menggunakan kunci privat RSA milik penerima, aplikasi mendekripsi Ek untuk mendapatkan kembali kunci sesi 3DES yang asli.

K = RSA_decrypt(Ek, PrivateKey_receiver)

c. Dekripsi Pesan dengan 3DES

Pesan terenkripsi C didekripsi menggunakan kunci sesi K dengan algoritma 3DES dalam mode CBC.

Plaintext = 3DES_decrypt(C, K)

d. Output ke Pengguna

Setelah proses dekripsi selesai, pesan asli ditampilkan dalam aplikasi. Pengguna melihat pesan seperti semula : ***"Kode OTP Anda adalah 982134"***

3. Analisis Kelebihan Sistem

Aspek	**Penjelasan**

Keamanan Data	Dengan kombinasi RSA + 3DES, sistem menyediakan perlindungan pada dua lapisan: isi pesan dan distribusi kunci.
Manajemen Kunci Aman	RSA menyelesaikan masalah pengiriman kunci rahasia secara aman melalui kriptografi asimetris.
Efisiensi Proses	3DES digunakan hanya untuk isi pesan (berukuran kecil), sedangkan RSA digunakan hanya untuk mengenkripsi kunci (berukuran tetap dan kecil).
Probabilitas	Sistem dapat diadaptasi ke aplikasi mobile atau modul SMS gateway untuk notifikasi sensitif.

4. Tantangan dan Batasan
    1. Panjang Ciphertext

       Kombinasi dua algoritma menghasilkan pesan yang lebih panjang dari 160 karakter. Ini perlu penanganan khusus saat pengiriman SMS (multi-part message).
    2. Kinerja

       Enkripsi RSA relatif lambat, namun dalam sistem ini hanya digunakan sekali untuk mengenkripsi kunci sesi (bukan seluruh pesan).
    3. Ketergantungan Aplikasi Khusus

       Baik pengirim maupun penerima harus menggunakan aplikasi yang mendukung mekanisme ini.

KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem pengamanan pesan SMS menggunakan pendekatan multiple encryption yang menggabungkan algoritma RSA dan 3DES. Sistem ini mampu meningkatkan keamanan komunikasi SMS dengan menyediakan mekanisme perlindungan ganda terhadap isi pesan dan distribusi kunci enkripsi. Algoritma RSA digunakan secara efektif untuk mengenkripsi kunci sesi yang digunakan oleh 3DES, sehingga menyelesaikan tantangan utama dalam kriptografi simetris, yaitu distribusi kunci yang aman. Sementara itu, algoritma 3DES memberikan efisiensi dalam mengenkripsi isi pesan secara cepat.

Hasil pengujian menunjukkan bahwa sistem mampu menjaga kerahasiaan pesan, menghasilkan ciphertext yang tidak dapat dibaca tanpa kunci RSA privat, dan berhasil mendekripsi pesan asli tanpa kehilangan data. Meski demikian, tantangan masih ada, seperti panjang ciphertext yang melebihi batas SMS standar dan ketergantungan pada aplikasi khusus di sisi pengguna.

Ke depan, penelitian ini dapat dikembangkan lebih lanjut dengan mengintegrasikan algoritma enkripsi yang lebih modern seperti AES, serta menerapkan sistem pada SMS gateway untuk kebutuhan berskala besar, seperti layanan publik, perbankan, dan instansi pemerintahan yang memerlukan keamanan data tinggi pada komunikasi nirkabel

DAFTAR PUSTAKA

Kessler, G. C. (2021). *An Overview of Cryptography*. Retrieved from https://www.garykessler.net/library/crypto.html

Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson Education.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126. https://doi.org/10.1145/359340.359342

Meyer, D., & Wetzel, S. (2004). A man-in-the-middle attack on UMTS. In *Proceedings of the 3rd ACM workshop on Wireless security* (pp. 90–97).

Kaufman, C., Perlman, R., & Speciner, M. (2016). *Network Security: Private Communication in a Public World* (3rd ed.). Pearson.

Barker, E. (2017). *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*. NIST Special Publication 800-67 Revision 2. National Institute of Standards and Technology.

Kurniawan, Y. (2022). Analisis Keamanan Penggunaan SMS OTP pada Aplikasi Mobile Banking. *Jurnal Keamanan Siber dan Kriptografi*, 6(1), 12–20.

Sari, D., & Nugroho, R. A. (2021). Implementasi Enkripsi Hybrid RSA dan AES pada Pengiriman Pesan. *Jurnal Informatika*, 15(2), 98–105