PENGAMANAN DATA E-MAIL MENGGUNAKAN ENKRIPSI PARTIALLY HOMOMORPHIC ENCRYPTION (PHE)

Mohamad Aditya Muttaqin Ghozali[1], Wina Witanti[2], Gunawan Abdillah[3]

[1,2,3] Program Studi Informatika, Fakultas Sains dan Informatika, Universitas Jenderal Achmad Yani
[1]mohamadadityamg20@if.unjani.ac.id, [2]witanti@gmail.com, [3] gunawanabdillah03@gmail.com

Abstrak

Pengamanan data merupakan aspek penting dalam era digital untuk melindungi informasi sensitif dari akses tidak sah dan ancaman keamanan. Terutama pada email sebagai media komunikasi jarak jauh, pengamanan data sangat penting karena email rentan terhadap serangan yang dapat mencuri atau memanipulasi data. Salah satu teknik yang telah berkembang pesat untuk menghadapi tantangan keamanan yang kompleks adalah kriptografi, termasuk Homomorphic Encryption Partially. Homomorphic Encryption Partially dapat mengamankan data email dengan mengubah informasi menjadi ciphertext yang hanya dapat diakses oleh pemilik kunci. Teknik ini membuat pihak luar yang tidak memiliki izin sulit membaca data asli. Selain itu, teknik ini menunjukkan penggunaan memori yang efisien tanpa mengorbankan keamanan. Penelitian ini membandingkan Homomorphic Encryption Partially yang menggunakan algoritma RSA Homomorfik dengan algoritma AES dalam perbandingan penggunaan memori. Hasil penelitian menunjukkan bahwa Homomorphic Encryption Partially menggunakan 10.42% dalam pengunaan memori dibandingkan dengan AES yang menggunakan 102.69% dalam penggunaan memorinya, sehingga menghasilkan penggunaan memori yang besar. Selain itu, penelitian ini menunjukkan bahwa waktu untuk memecahkan pasangan kunci bisa mencapai beberapa bulan hingga tahun. Sebagai kesimpulan, Homomorphic Encryption Partially efektif dalam penggunaan memori, menghasilkan ukuran yang lebih kecil setelah enkripsi dibandingkan dengan AES yang menghasilkan ukuran lebih besar.

Kata kunci : *enkripsi homomorfik, kriptografi, e-mail, pengaman data.*

1. Pendahuluan

Perkembangan teknologi informasi dan internet saat ini telah mengubah kehidupan manusia dalam melakukan komunikasi. Era teknologi informasi saat ini tidak hanya digunakan untuk komunikasi saja, melainkan dapat memberikan kemudahan dalam melakukan segala hal. Dengan berkembangnya media sosial maka masalah pada keamanan informasi dan privasi juga menjadi penting saat ini (Betty Yel & M Nasution, 2022). Pada tahun 2019 terdapat 150 juta pengguna sosial media yang meningkat 20% dari tahun 2018 dan terjadi kebocoran data sejumlah 87 juta data pribadi (Betty Yel & M Nasution, 2022). Dengan demikian memerlukan pengamanan pada data atau informasi dengan menggunakan teknik Kriptografi. Salah satu tipe Kriptografi ini yaitu Homomorfik Parsial, tipe ini mendukung operasi perkalian dan juga operasi penambahan (Alexandru et al., 2021). Enkripsi Homomorfik ini merupakan teknik enkripsi yang menggunakan operasi matematika seperti penjumlahan dan perkalian yang dilakukan pada data terenkripsi tanpa melakukan dekripsi (Zhang et al., 2018). Enkripsi Homomorfik ini memiliki kemampuan untuk memproses data yang dienkripsi secara efisien, yang dimana enkripsi ini melakukan operasi matematika pada data yang dienkripsi tanpa mengurai datanya terlebih dahulu (Ameur et al., 2023). Penggunaan teknik Kriptografi Enkripsi Homomorfik ini digunakan untuk mengamankan data atau informasi pada alat komunikasi yaitu e-mail. Alat komunikasi ini sering digunakan untuk komunikasi terkait pekerjaan. E-mail ini digunakan untuk manajemen tugas, komunikasi sosial, penjadwalan, dan pertukaran informasi (Wang et al., 2019). Sehingga data atau informasi pada e-mail perlu diamankan karena dalam pertukaran informasi nya dapat terjadi sebuah serangan yang merugikan seperti Phising, Spam, Malware, Man-in-the-Middle Attack, dan E-mail Spoofing (Dada et al., 2019).

Pada penelitian sebelumnya dalam bidang Cloud Computing melakukan skema Enkripsi Homomorfik baru berdasarkan Enkirpsi Homomorfik Parsial Multistage yang memungkinkan untuk menggunakan operasi tententu pada data yang dienkripsi (Hikmat Mahmood & Khalel Ibrahem, 2018). Kemudian pada penelitian sebelumnya juga melakukan pengamanan teks pada dokumen yang dikirimkan melalui e-mail menggunakan teknik kriptografi dengan enkripsi rotor. Kriptografi ini berbasis subtitusi yang dimana mengganti karakter awal dengan karakter lainnya sesuai dengan kunci yang telah dibuat. Lalu kunci yang digunakan dikirimakan melalui jaringan aman dan hasil enkripsi dikirimkan melalui jaringan terbuka ke tujuan

(Arfriandi, 2018). Sama seperti sebelumnya terdapat pengamanan pesan e-mail dengan melakukan kombinasi dari dua algoritma kriptografi yaitu Blowfish dan RSA untuk proses enkripsi dan dekripsi. Blowfish digunakan untuk mengamankan isi pesan yang dikirim, sedangkan RSA digunakan untuk mengamankan kunci simetris yang digunakan untuk proses enkripsi dan dekripsi isi pesan. Kemudian hasil yang diberikan dari kedua teknik kriptografi ini menghasilkan ukuran yang lebih besar dari pada ukuran sebelum dilakukan enkripsi, yang dimana ini tidak berpengaruh signifikan dalam proses pengiriman e-mail (Iqbal Zulfikar et al., 2019). Penelitian lainnya juga melakukan pengamanan dengan menyembunyikan teks sensitif dalam pesan e-mail dengan menggunakan metode keamanan multi-level yang menggunakan stegnografi dan kriptografi yang dimana metode ini melibatkan kompresi dan enkripsi teks dengan penggunaan algoritma DHKE dan AES untuk enkripsinya (Alsaidi et al., 2018).

Enkripsi Homomorfik melakukan proses enkripsi terhadap data atau informasi pada suatu dokumen yang akan dikirim melalui e-mail untuk mengubah plaintext menjadi chipertext. Dalam pengenkripsian ini menggunakan sistem Public Key Infrastructure (PKI), yang dimana konsep dari sistem ini pengirim diharuskan memiliki kunci publik dari penerima, sehingga pembuatan kunci ini dilakukan oleh pihak penerima dan mengirimkan kunci publik tersebut ke pihak pengirim untuk melakukan proses enkripsi. Sehingga hanya pihak penerima saja yang mengetahui kunci privat untuk melakukan dekripsi pada chiperteks yang telah dikirim (Jarkasih et al., 2022). Terdapat beberapa metode yang digunakan untuk pengamanan data seperti pada penelitian sebelumnya yang menggunakan Algoritma Vignere, Kriptografi Simetris, Algoritma DHKE dan AES yang dimana metode-metode ini digunakan untuk mengamankan data. Dengan demikian penelitian ini akan melakukan pengamanan data atau informasi pada suatu dokumen yang akan dikirim melalui e-mail dengan teknik Kriptografi Enkripsi Homomorfik Parsial dengan menggunakan algoritma RSA Homomorfik yang memiliki kelebihan dalam penggunaan memori yang sedikit (Acar et al., 2018). Teknik ini akan menggunakan salah satu operasi matematika yaitu pertambahan atau perkalian.

Tujuan dari penelitian ini adalah untuk membuat sistem yang dapat mengamankan isi pesan yang ada didalam e-mail. Sistem yang dibangun dapat melakukan proses Enkripsi Homomorfik Parsial pada suatu dokumen pesan e-mail yang menampilkan hasil berupa chipertext, sehingga dapat mengamankan pesan e-mail dengan penggunaan sistem ini yang dapat digunakan oleh perusahaan atau orang-orang yang akan mengirimkan pesan e-mail berupa dokumen penting. Oleh karena itu dibutuhkan sistem pengamanan terhadap privasi pada e-mail dengan membuat suatu sistem yang dapat mengamankan pesan e-mail dengan penggunaan memori yang sedikit.

2. Kajian Pustaka

Dalam kajian pustaka ini menjelaskan beberapa teori yang terkait dengan penelitian seperti pengamanan data, enkripsi homomorfik, jenis enkripsi homomorfik, dan algoritma RSA.

2.1 Pengamanan Data

Pengaman data ini melakukan perlindungan terhadap data dari berbagai ancaman seperti kebocoran, kerusakan, atau akses yang tidak sah. Terdapat enam tahap siklus hidup data, yaitu membuat, menyimpan, menggunakan, berbagi, mengarsipkan, dan menghancurkan. Sehingga perlu meningkatkan keamanan data dengan menggunakan beberapa metode yang dapat diterapkan seperti enkripsi data (Ma et al., 2021). Data yang bersifat privasi perlu diamankan untuk melindungi dari kebocoran dan penyalahgunaan. Sehingga sangat penting untuk melakukan pengamanan data untuk melindungi privasi data, memastikan integritas data, dan mencegah penyalahgunaan informasi yang dapat merugikan pengguna atau organisasi (Jin et al., 2019). Beberapa data perlu dilakukan keamanan agar data tersebut tetap terjaga kerahasiaannya, dengan begitu beberapa data yang perlu diamankan seperti data pribadi, data hukum, data penelitian, dan data kesehatan (Kumar et al., 2018). Dalam lingkungan kesehatan data yang perlu diamankan antara lain Rekam Medis Elektronik (EMR), Informasi Kesehatan yang Dilindungi (PHI), Data Medis Besar, dan Data Transaksi (Jin et al., 2019).

2.2 Enkripsi Homomorfik

Enkripsi Homomorfik merupakan teknik yang memungkinkan untuk menggunakan operasi tertentu yang dilakukan pada data yang telah dienkripsi tanpa perlu mendekripsi data tersebut terlebih dahulu (Alaya et al., 2020). Enkirpsi Homomorfik diperkenalkan pada tahun 1978 yang memiliki skema operasi penjumlahan atau perkalian. Dan pada tahun 2009 berhasil membuat skema enkripsi dengan menggunakan kedua operasi tersebut (Alaya et al., 2020). Terdapat penelitian sebelumnya dari berbagai bidang yang menggunakan Enkripsi Homomorfik ini sebagai metode pengamanan data. Enkripsi Homomorfik pada bidang kesehatan melakukan pengamanan terhadap data pasien, seperti penggunaan Enkirpsi Homomorfik pada komputasi awan medis yang aman dan pribadi (Munjal & Bhatia, 2023). Data perlu diamankan untuk memastikan privasi dan kemanan informasi pribadi lainnya, yang dimana dengan meningkatnya penggunaan teknologi dan digitalisasi dapat meningkatkan juga risiko

terhadap kemanan data (Munjal & Bhatia, 2023), dan jika data tidak diamankan maka akan ada risiko data tersebut dapat dicuri oleh penyerang pada setiap proses pengolahan data (Kucherov et al., 2020), sehingga Enkripsi Homomorfik ini memiliki keunggulan tersendiri dari beberapa enkripsi lainnya, yang dimana memungkinkan operasi komputasi dilakukan secara langsung pada data terenkripsi tanpa memerlukan kunci rahasia. Dan hasil perhitunggannya tetap dalam bentuk terenkripsi sehingga tidak perlu mendekripsikannya terlebih dahulu (Gaid & Salloum, 2021), seperti pada kalimat pertama yang menjelaskan mengenai enkripsi homomorfik.

2.3 Jenis Enkripsi Homomorfik

Enkripsi Homomorfik ini memiliki dua jenis dan memiliki perbedaan dalam proses enkripsinya. Berikut merupakan jenis dari Enkripsi Homomorfik yaitu (Acar et al., 2018):

1) Partially Homomorphic Encryption

Enkripsi Homomorfik Parsial ini merupakan jenis enkripsi yang memungkinkan menggunakan operasi tertentu seperti pertambahan atau perkalian untuk dilakukan pada data terenkripsi dengan tidak melakukan dekripsi data terlebih dahulu. Hasil dari enkripsi ini saat melakukan dekripsi, akan menunjukan hasil yang sama dengan operasi yang dilakukan pada data asli sebelum dienkripsi. Enkripsi ini hanya melakukan satu operasi pertambahan atau perkalian saja, berbeda dengan Enkripsi Homomorfik lainnya. Kelebihan dari enkripsi ini antara lain:

a) Efisiensi: enkripsi ini efisien dalam penggunaan memorinya.
b) Keamanan: enkripsi ini meskipun menggunakan salah satu operasi dari pertambahan atau perkalian masih memiliki tingkat keamanan yang tinggi.

2) Fully Homomorphic Encryption

Enkripsi Homomorfik Penuh ini merupakan jenis enkripsi yang memungkinkan menggunakan operasi pertambahan dan perkalian. Enkripsi ini juga memungkinkan komputasi yang tidak terbatas pada data terenkripsi tanpa melakukan proses dekripsi data terlebih dahulu. Dan hasil pada operasi ini saat melakukan dekripsi akan menghasilkan sama dengan hasil operasi yang sama dilakukan pada data asli sebelum dienkripsi. Kelebihan dari enkripsi ini antara lain:

a) Komputasi pada Data Terenkripsi: enkripsi ini memungkinkan komputasi yang tidak terbatas dengan menggunakan dua operasi pertambahan dan perkalian.
b) Keamanan: enkripsi ini memberikan tingkat keamanan yang tinggi.
c) Privasi: enkripsi ini memungkinkan pengolahan data yang aman dan privasi, yang berarti dapat melakukan komputasi pada data sensitif tanpa mengungkapkan informasi apa pun tentang data tersebut.
d) Potensi: enkripsi ini memiliki potensi aplikasi yang luas, seperti dalam Cloud Computing, Biometric Authentication, dan lain-lainnya.

2.4 Rivest Shamir Adleman (RSA)

Algoritma RSA ini dibuat oleh tiga orang peneltii dari MIT (Massachussets Institute of Technology) pada tahun 1976. RSA ini merupakan singkatan dari Rivest Shamir Adleman yang merupakan nama-nama dari ketiga orang peneliti tersebut (Rizki & Farida Ariyani, 2021). Algoritma ini menggunakan proses enkripsi dan dekripsinya dengan konsep bilangan prima dan aritmatika modulo, sehingga kunci enkripsi dan kunci dekripsinya merupakan bilangan bulat (Anwar et al., 2021). Kunci yang digunakan pada algortima ini bertipe asimetris, yang artinya memiliki pasangan kunci-kunci yang salah satunya diterapkan pada proses enkripsi dan yang satu lagi untuk proses dekrips (Rizki & Farida Ariyani, 2021), sehingga keamanan algortima terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima untuk menemukan kunci privat (Anwar et al., 2021). Algoritma RSA ini didukung oleh persamaan-persamaan berikut:

1) Menentukan nilai dua bilangan prima p dan q.
2) Menentukan nilai n dengan Persamaan (1). Nilai n digunakan untuk proses enkripsi dan dekripsi.

$$n = p.q \tag{1}$$

3) Menghitung nilai $\phi(n)$ dengan Persamaan (2). Nilai $\phi(n)$ digunakan untuk mencari nilai kunci privat.

$$\phi(n) = (p-1)(q-1) \tag{2}$$

4) Menentukan bilangan bulat sembarangan sebagai nilai e dan harus relatif dengan prima terhadap $\phi(n)$.
5) Menentukan nilai d dengan Persamaan (3) atau dengan menggunakan Persamaan (4).

$$ed = 1\big(mod\ \phi(n)\big) \tag{3}$$

$$d = \frac{1 + k\ \phi(n)}{e} \tag{4}$$

6) Kunci publik (n, e) dan kunci privat (d, n) telah terbentuk.
7) Setelah kunci publik dan privat terbentuk, proses selanjutnya melakukan enkripsi dan dekripsi. Proses enkripsi menggunakan Persamaan (5) dengan parameter plaintext dan kunci publik. Proses dekripsi menggunakan Persamaan (6) dengan parameter ciphertext dan kunci privat.

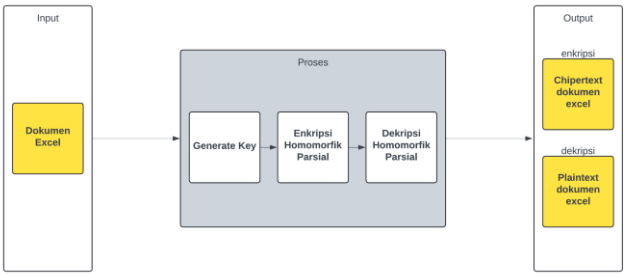
$$E(m) = c = m^e \bmod n \quad (5)$$

$$D(c) = m = c^d \bmod n \quad (6)$$

Di mana:
c = *ciphertext* e = kunci publik
m = plaintext n = nilai modulus
d = kunci privat

3. Metode Penelitian

Pada tahap penelitian diawali dengan pengumpulan data, penelitian ini diperoleh melalui studi pustaka dengan melakukan pencarian referensi penelitian yang sesuai. Pengamanan data ini akan menggunakan data Perusahaan Daerah Air Minum PDAM dari wilayah Cibeureum di Provinsi Jawa Barat mengenai kualitas air untuk diamankan. Tahap pengolahan data melibatkan tiga proses yaitu pembuatan kunci publik dan privat dengan menggunakan teknik RSA, enkripsi untuk mengubah data asli atau *plaintext* menjadi *ciphertext* menggunakan teknik algoritma RSA Homomorfik, dan dekripsi untuk mengubah data *ciphertext* menjadi *plaintext* menggunakan teknik algoritma RSA Homomorfik. Pengujian pada sistem ini dilakukan untuk melihat kemampuan dari algoritma RSA Homomorfik. Tahapan penelitian pengamanan data pada dokumen dapat dilihat pada Gambar 1.

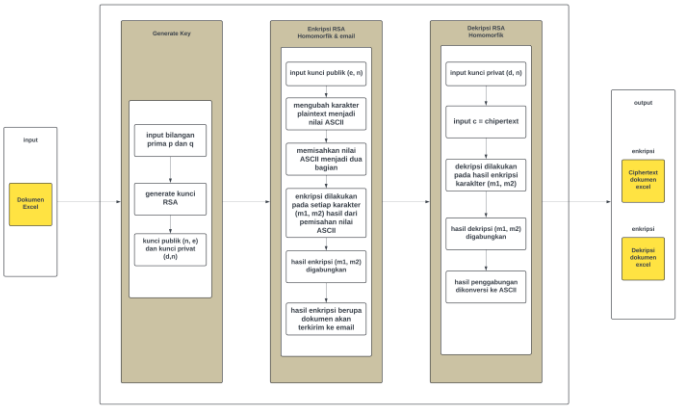


Gambar 1. Tahapan Penelitian

Proses penelitian ini dilakukan dengan tahap awal melakukan proses memasukkan data (*input*) dokumen berupa excel/xlsx. Data ini berupa data asli yang belum diproses dan belum terlindungi. Setelah data tersedia maka akan dilakukan proses pembuatan kunci publik dan kunci privat dan masuk ke tahap selanjutnya yaitu melakukan enkripsi pada dokumen excel dengan menggunakan Enkripsi Homomorfik Parsial, dan juga proses dekripsi menggunakan Enkripsi Homomorfik Parsial. Tahap terakhir menghasilkan dokumen excel berupa ciphertext dan dokumen excel berupa plaintext setelah melakukan dekripsi.

3.1 Perancangan Sistem

Perancangan sistem pengamanan data pada dokumen dapat dilihat pada Gambar 2.



Gambar 2. Perancangan Sistem

Analisis proses sistem pengamanan data pada dokumen saat akan melakukan pengiriman e-mail di mana sistem akan melakukan perubahan pada data dokumen yang akan dikirim menjadi bentuk ciphertext. Proses enkripsi dilakukan dengan menggunakan kunci publik dan proses dekripsi dilakukan dengan menggunakan kunci privat. Pada proses enrkispi setiap karakter plaintext akan diubah menjadi nilai ASCII, dan nilai tersebut setiap digit ASCII dipisahkan seperti contoh nilai ASCII 65 dipisahkan menjadi 6 dan 5 untuk dilakukan proses enkripsi setiap digit ASCII yang sudah dipisahkan. Lalu hasil enkripsi akan berupa dokumen yang terenkripsi dan secara otomatis email akan mengambil dokumen terenkripsi sebagai pesan untuk dikirim ke email tujuan. Proses dekripsi pun mengalami proses yang sama seperti proses enkripsi yaitu melakukan dekripsi pada setiap digit ASCII yang sudah terpisah. Berikut perhitungan mengenai proses yang terjadi pada sistem dengan contoh dokumen excel berisikan huruf A yang akan dienkripsi sebagai berikut:

a) Pembentukan kunci

1. Menentukan bilangan prima p dan q:
   - p = 31 dan q = 13
2. Membentuk kunci publik (n) dengan persamaan (1):
   - n = 31 * 13
   - n = 403
3. Hitung nilai $\phi(n)$ dari kunci public dengan persamaan (2):
   - $\phi(n) = (31-1) * (13-1)$
   - $\phi(n) = 30 * 12$
   - $\phi(n) = 360$
4. Menentukan nila e sembarang yang relatif prima terhadap nilai $\phi(n)$:
   - e = 7
   - Nilai e yang diambil harus tidak boleh nilai factorial dari hasil $\phi(n)$
   - 360 memiliki nilai faktorial 2, 3, dan 5, sehingga nilai e tidak boleh mengambil nilai tersebut
5. Menghitung nilai d dengan persamaan (4):

- $d \frac{1+2\,(360)}{7}$
- $d \frac{721}{7}$
- $d = 103$
- kunci publik (n, e) = (403, 7) dan kunci privat (d, n) = (103, 403)

b) Proses enkripsi
1. Mengubah nilai A menjadi ASCII
   - A = 65
2. Memisahkan nilai 65 menjadi 6 dan 5 untuk proses enkripsi dengan kunci publik (n, e) = (403, 7)
   - 6 = 6^7 mod 403
     = 279936 mod 403
     = 279936 / 403 = 694
     = 279936 – (694 x 403)
     = 279936 – 279682 = 254
   - 5 = 5^7 mod 403
     = 78125 mod 403
     = 78125 / 403 = 193
     = 78125 – (193 x 403)
     = 78125 – 77779 = 346
   - Maka hasilnya menjadi 254.346 dipisahkan oleh titik sebagai *ciphertext* dari A

c) Proses dekripsi
1. Melakukan dekripsi pada *ciphertext* (254.346) dengan kunci privat d = 103 dan n = 403
   - 254 = 254^103 mod 403
     = 6
   - 346 = 346^103 mod 403
     = 5
   - Maka hasilnya digabungkan menjadi 65, dan nilai 65 pada ASCII adalah A

Hasil dari proses sistem ini melakukan pembuatan pasangan kunci terlebih dahulu untuk digunakan dalam proses enkripsi dan dekripsi. Hasil enkripsi dokumen excel yang berisikan huruf A menghasilkan *ciphertext* 254.346, dan secara otomatis dokumen tersebut terkirim ke email tujuan. Hasil dekripsi melakukan perubahan pada *ciphertext* ke *plaintext* dengan menggunakan kunci privat dan menghasilkan nilai A kembali.

4. Hasil dan Pembahasan

Pengujian sistem ini adalah pengujian terhadap perangkat lunak dan kesesuaian antara hasil perancangan dengan tujuan yang diharapkan. Tujuan dari pengujian ini adalah untuk menguji apakah algoritma RSA Homomorfik memiliki penggunaan memori yang sedikit dalam melakukan *enkripsi* pada dokumen dengan melakukan pengujian pada ukuran dokumen terenkripsi, serta menguji kunci yang dihasilkan dari algoritma RSA dengan menggunakan tools *passwordmoster* untuk pengecekan durasi kunci dapat dipecahkan.

Hasil pengujian kunci dengan menggunakan tools *passwordmoster* mendapatkan hasil kunci yang cukup aman. Setiap pasangan kunci memiliki waktu pemecahan dalam hitungan bulan hingga tahun, hal ini dikarenakan panjang nya karakter kunci yang digunakan dan juga nilai p dan q yang besar. Kunci yang aman memiliki jumlah karakter yang lebih dari 10, jumlah karakter ini didapatkan dari nilai prima p dan q yang besar sehingga menghasilkan jumlah karakter yang banyak. Hasil pengujian kunci dapat disampaikan dalam Tabel 1.

Tabel 1. Hasil Pengujian Kunci

No	Kunci	Waktu
1	(143119, 107409)	68 tahun
2	(68753, 66155)	2 bulan
3	(378857, 47515)	4 tahun
4	(184871, 169475)	9 tahun
5	(85979, 44647)	8 bulan

Pengujian selanjutnya dilakukan proses enkripsi pada dokumen excel dengan melakukan perbandingan Enkripsi Homomorfik Parsial dengan Enkripsi AES. Perbandingan dua teknik ini dilakukan dengan menggunakan ukuran dokumen sebagai pengujiannya untuk mengetahui hasil ukuran dokumen berubah menjadi kecil setelah dilakukan proses enkripsi. Hal ini digunakan untuk mengetahui apakah Enkripsi Homomorfik Parsial dengan menggunakan algoritma RSA Homomorfik memiliki kelebihan dalam penggunaan memorinya yang sedikit. Hasil pengujian enkripsi dapat disampaikan dalam Tabel 2.

Tabel 2. Hasil Pengujian Enkripsi

Alg	Nama File	Size Awal	Size Akhir	Kecepatan
RSA	Kualitas Air IPA CBRM th 2017.xlsx Sampling	33 KB	29 KB	1.00 Detik
RSA	Kualitas Air Cibeureum oleh LPKL th 2017.xlsx Sampling	72 KB	62 KB	1.91 Detik
RSA	Kualitas Baku & Air besih Cibeureum oleh LPKL th. 2016.xlsx	19 KB	18 KB	0.27 Detik
AES	Kualitas Air IPA CBRM th 2017.xlsx Sampling	33 KB	100 KB	0.15 Detik
AES	Kualitas Air Cibeureum oleh LPKL th 2017.xlsx	72 KB	87 KB	0.89 Detik

AES	Sampling Kualitas Baku & Air besih Cibeureum oleh LPKL th. 2016.xlsx	19 KB	35 KB	0.08 Detik

Pada Tabel 2 dengan melakukan pengujian pada tiga dokumen dengan size awal yang berbeda menghasilkan ukuran dokumen yang berubah dengan menggunakan algoritma RSA Homomorfik dan AES. File excel yang di *enkprisi* berhasil untuk dilakukan proses *enkripsi* dan menghasilkan size yang lebih besar dari size sebelumnya untuk algoritma AES, sedangkan algoritma RSA Homomorfik menghasilkan size yang lebih kecil dari size sebelum dilakukan proses enkripsi pada file excel tersebut.

Kesimpulannya pada algoritma RSA Homomorfik terbukti bahwa algoritma tersebut efesien terhadap penggunaan memorinya, dari salah satu contoh pengujian dokumen dengan size awal yaitu 33 Kb menjadi 29 Kb setelah melakukan enkripsi. Sedangkan pada algoritma AES mengalami kenaikan yang cukup besar pada salah satu contoh pengujian dokumen dari size 33 Kb menjadi 100 Kb. Pada hasil kecepatan enkripsi, algoritma AES lebih unggul dan memiliki perbedaan cukup besar dari algoritma RSA Homomorfik. Hal ini dikarenakan algoritma RSA termasuk kedalam kriptografi yang lambat dan juga adanya operasi matematika seperti menghitung ekponen modular dari enkripsi dan dekripsi pada persamaan (5) dan (6), dan juga terdapat pada pembangkitan kunci yang melibatkan pemilihan dua bilangan prima besar lalu mengalikan keduanya untuk mendapatkan modulus N pada persamaan (1). Selain itu, diperlukan perhitungan invers modular untuk mendapatkan kunci privat dengan perhitungan pada persamaan (2) dan (4).

5. Kesimpulan

Penelitian ini melakukan pengamanan data PDAM di wilayah Cibeureum Provinsi Jawa Barat sebagai data email untuk dikirim, yang menggunakan teknik Enkripsi Homomorfik Parsial dengan menggunakan algoritma RSA Homomorfik untuk proses enkripsi dan dekripsi. Berdasarkan pada hasil pengujian dengan melakukan perbandingan antara RSA Homomorfik sebagai Enkripsi Homomorfik Parsial dengan Enkripsi AES pada ketiga dokumen excel yang diuji. Hasil dari RSA Homomorfik menunjukkan, bahwa ketiga dokumen excel yang sudah terenkripsi dengan size awal yang berbeda-beda mengalami penurunan dalam size dokumennya, dengan rata-rata penggunaan memorinya adalah 10.24%. Sedangkan pada ketiga dokumen yang di enkripsi oleh AES mengalami kenaikan pada size dokumennya, dengan rata-rata penggunaan memorinya adalah 102.69%. Hal ini menunjukkan bahwa Enkripsi Homomorfik Parsial lebih sedikit atau lebih efisien dalam penggunaan memorinya dibandingkan dengan enkripsi AES. Selain itu, hasil pengujian menunjukkan bahwa waktu komputasi untuk melakukan enkripsi cukup lama. Hal ini merupakan salah satu kekurangan dari Enkripsi Homomorfik Parsial dengan menggunakan algoritma RSA Homomorfik, karena adanya operasi matematika yang kompleks pada proses enkripsi. Pasangan kunci yang aman didapatkan dari nilai prima p dan q yang besar, sehingga menghasilkan kunci yang membutuhkan waktu pemecahan dalam hitungan bulan hingga tahun.

Daftar Pustaka:

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. In *ACM Computing Surveys* (Vol. 51, Issue 4). Association for Computing Machinery. https://doi.org/10.1145/3214303

Alaya, B., Laouamer, L., & Msilini, N. (2020). Homomorphic Encryption Systems Statement: Trends and Challenges. In *Computer Science Review* (Vol. 36). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2020.100235

Alexandru, A. B., Gatsis, K., Shoukry, Y., Seshia, S. A., Tabuada, P., & Pappas, G. J. (2021). Cloud-Based Quadratic Optimization With Partially Homomorphic Encryption. *IEEE Transactions on Automatic Control*, *66*(5), 2357–2364. https://doi.org/10.1109/TAC.2020.3005920

Alsaidi, A., Al-lehaibi, K., Alzahrani, H., AlGhamdi, M., & Gutub, A. (2018). Compression Multi-Level Crypto Stego Security of Texts Utilizing Colored Email Forwarding. *Journal of Computer Science & Computational Mathematics*, 33–42. https://doi.org/10.20967/jcscm.2018.03.002

Ameur, Y., Bouzefrane, S., & Thinh, L. V. (2023). Handling security issues by using homomorphic encryption in multi-cloud environment. *Procedia Computer Science*, *220*, 390–397. https://doi.org/10.1016/j.procs.2023.03.050

Anwar, B., Kustini, R., & Zulkarnain, I. (2021). Penerapan Algoritma RSA (Rivest Shamir Adelman) Untuk Mengamankan Nilai Siswa SMP HKBP P. Bulan. , *88*(1), 88–91.

Arfriandi, A. (2018). Pengamanan Teks Pada Dokumen Email Menggunakan Enkripsi Rotor. In *Edu Komputika* (Vol. 5, Issue 1). http://journal.unnes.ac.id/sju/index.php/edukom

Betty Yel, M., & M Nasution, M. K. (2022). Keamanan Informasi Data Pribadi PAda Media Sosial. *JIK)*, *6*(1).

Dada, E. G., Bassi, J. S., Chiroma, H., Abdulhamid, S. M., Adetunmbi, A. O., & Ajibuwa, O. E. (2019). Machine Learning for Email Spam Filtering: Review, Approaches and Open

Research Problems. *Heliyon*, *5*(6). https://doi.org/10.1016/j.heliyon.2019.e01802

Gaid, M. L., & Salloum, S. A. (2021). *Homomorphic Encryption* (pp. 634–642). https://doi.org/10.1007/978-3-030-76346-6_56

Hikmat Mahmood, Z., & Khalel Ibrahem, M. (2018). New Fully Homomorphic Encryption Scheme Based On Multistage Partial Homomorphic Encryption Applied In Cloud Computing. *Https://Ieeexplore.Ieee.Org/Xpl/Conhome/8630866/Proceeding*. https://ieeexplore.ieee.org/abstract/document/8640952

Iqbal Zulfikar, M., Abdillah, G., Komarudin Jurusan Informatika, A., & Sains dan Informatika Universitas Jenderal Achmad Yani Cimahi, F. (2019). Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA). In *Seminar Nasional Aplikasi Teknologi Informasi (SNATi)*.

Jarkasih, S., Fatimah, U., Psikologi, D., Negeri Padang, U., Hamka, J., Tawar, A., Padang Barat, K., Barat, S., Teknologi Informasi, P., Ilmu Pendidikan, F., Muhammadiyah Jakarta, U., Ahmad Dahlan, J. K., Ciputat Timur, K., & Tangerang Selatan, K. (2022). Penggunaan Public Key Infrastructure Kunci Persetujuan (Key Agreement). *Jurnal Pendidikan Teknologi Informasi*, 97–102.

Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A Review of Secure and Privacy-Preserving Medical Data Sharing. In *IEEE Access* (Vol. 7, pp. 61656–61669). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2916503

Kucherov, N. N., Deryabin, M. A., & Babenko, M. G. (2020). Homomorphic Encryption Methods Review. *Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2020*, 370–373. https://doi.org/10.1109/EICONRUS49466.2020.9039110

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Computer Science*, *125*, 691–697. https://doi.org/10.1016/j.procs.2017.12.089

Ma, H., Han, S., & Lei, H. (2021). Optimized Paillier's Cryptosystem with Fast Encryption and Decryption. *ACM International Conference Proceeding Series*, 106–118. https://doi.org/10.1145/3485832.3485842

Munjal, K., & Bhatia, R. (2023). A Systematic Review of Homomorphic Encryption and Its Contributions in Healthcare Industry. *Complex and Intelligent Systems*, *9*(4), 3759–3786. https://doi.org/10.1007/s40747-022-00756-z

Rizki, M., & Farida Ariyani, P. (2021). Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada Pt Trias Mitra Jaya Manunggal. *Skanika*, *4*(2), 1–6. https://doi.org/10.36080/skanika.v4i2.1991

Wang, W., Hosseini, S., Awadallah, A. H., Bennett, P. N., & Quirk, C. (2019). Context-Aware Intent Identification in Email Conversations. *SIGIR 2019 - Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval*, 585–594. https://doi.org/10.1145/3331184.3331260

Zhang, Z., Wu, J., Yau, D., Cheng, P., & Chen, J. (2018). Secure Kalman Filter State Estimation by Partially Homomorphic Encryption. *Proceedings - 9th ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS 2018*, 345–346. https://doi.org/10.1109/ICCPS.2018.00046

Halaman ini sengaja dikosongkan