Penerapan Keamanan Data Siswa Menggunakan *International Data Encryption Algorithm* (IDEA) dan *Rivest Shamir Adleman* (RSA)

Raina Nabila Nizatsary [1], Henki Bayu Seta [2], Bambang Tri Wahyono[3]
Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. Rs. Fatmawati, Pondok Labu, Jakarta Selatan, DKI Jakarta, 12450, Indonesia
rainanabila@upnvj.ac.id, henkiseta@upnvj.ac.id, bambang.triwahyono@upnvj.ac.id

Abstrak. Perkembangan sistem informasi khususnya dalam dunia pendidikan saat ini berkembang pesat, perkembangan sistem informasi ini memberikan manfaat terutama dalam mendukung proses/operasional sekolah. Data dalam sistem informasi untuk suatu instansi maupun sekolah harus dikelola dengan baik dan aman. Penelitian ini dilakukan untuk meningkatkan keamanan data pada data siswa menggunakan *International Data Encryption Algorithm* (IDEA) dan *Rivest Shamir Adleman* (RSA). Proses pengamanan data dalam penelitian ini menggunakan kombinasi algoritma, kombinasi algoritma ini dilakukan dengan menggunakan algoritma kriptografi simetris yaitu *International Data Encryption Algorithm* (IDEA) terlebih dahulu untuk melindungi data siswa, lalu proses pengamanan data selanjutnya melindungi kunci dari algoritma kriptografi simetris yaitu *International Data Encryption Algorithm* (IDEA) menggunakan algoritma asimetris *Rivest Shamir Adleman* (RSA). Penelitian ini menggunakan data sebanyak 72 data siswa yang digunakan untuk pendaftaran SNMPTN di sekolah. Hasil luaran pada penelitian ini yaitu sebuah penerapan *hybrid cryptosystem* pada keamanan data siswa yang agar dapat mengamankan suatu data dengan baik.

Kata Kunci: *Data, Keamanan Data, IDEA, RSA*

1 Pendahuluan

Perkembangan teknologi informasi khususnya dalam dunia pendidikan saat ini berkembang pesat terutama di masa pandemi. Dalam dua tahun terakhir ini, Hampir semua kegiatan yang biasanya berlangsung di sekolah sebagian besar telah beralih online. Selain pandemi kemarin, proses pengiriman data secara online dari sekolah ke dinas pendidikan atau lembaga untuk tujuan tertentu, misalnya, SNMPTN, setiap siswa terpilih mengirimkan data pribadi untuk tujuan daftar universitas.

Penggunaan teknologi dalam proses pengiriman data secara online tentunya diharapkan berjalan sesuai rencana. Namun, tidak dapat dipungkiri bahwa orang yang tidak bertanggung jawab dapat melakukan kejahatan dunia maya untuk mencuri, mengubah, atau merusak hal-hal lain yang dapat membahayakan. Artikel berita (cyberthreat.id) Menurut laporan tersebut, telah terjadi sekitar 12 pelanggaran data di Indonesia sejak tahun 2019. Ini adalah peringatan bahwa kejahatan dunia maya yang membahayakan suatu data di Indonesia sangat mungkin terjadi.

Data sangat penting, terutama di dunia akademis, sehingga *database* harus memiliki keamanan yang tepat. Untuk memastikan keamanan suatu data, diperlukan keamanan data. Dalam penelitian ini, pengamanan data dilakukan dengan menggunakan dua metode yaitu kriptografi kunci simetris dan asimetris, yaitu *International Data Encryption Algorithm* (IDEA) dan *Rivest Shamir Adleman* (RSA). Menggunakan algoritma kriptografi simetris untuk melindungi data siswa dan algoritma kriptografi asimetris untuk melindungi kunci dari algoritma kriptografi simetris.

2 Landasan Teori

2.1 Keamanan Data

Keamanan data meliputi:

1. Privasi(Kerahasiaan): 3 sudut pandang Privasi (*Privacy of a Person's Personal, Privacy of Data about Person, Privacy of a Person's Communication*).
2. *Integrity*(Konsisten): Memastikan data yang dikirimkan benar-benar asli dan dikirimkan oleh orang yang tepat.
3. *Authenticity* (keaslian): Data atau informasi yang diterima harus dijaga dengan baik.
4. *Availability* (ketersediaan): Data atau informasi digunakan oleh orang yang berwenang.
5. *Access Control*: Mengatur hak akses pada data atau informasi[1].

2.2 Kriptografi

Kriptografi merupakan ilmu yang mempelajari metode matematika yang dapat diterapkan dalam tingkat keamanan yang berkaitan dengan keamanan data, seperti keandalan, integritas, dan keandalan[1].

2.3 *International Data Encryption Algorithm* (IDEA)

Berdasarkan [2] metodologi perancangan disamping algoritma IDEA adalah berdasarkan pada penggabungan tiga operasi yang berbeda. Ketiga operasi tersebut adalah:
⊕Bit-By-bit XOR dari 16-bit sub-blocks
⊞Penambahan Integer 16-bit modulo 2^{16}
⊙Perkalian Integer 16-bit modulo $2^{16} + 1$.

Berdasarkan [2] Langkah-langkah pada setiap putaran proses enkripsi menggunakan IDEA, adalah sebagai berikut:

1. $(X_1 * K_1) \bmod 12^{16} + 1$ (1)
2. $(X_2 + K_2) \bmod 12^{16}$
3. $(X_3 + K_3) \bmod 12^{16}$
4. $(X_4 * K_4) \bmod 12^{16} + 1$
5. Langkah1⊕Langkah3
6. Langkah2 ⊕ Langkah 4
7. (Langkah 5 * K_5) mod $12^{16} + 1$
8. (Langkah 6+Langkah7) mod 12^{16}
9. (Langkah 8 * K_6) mod $12^{16} + 1$
10. (Langkah 7 + Langkah 9) mod 12^{16}
11. Langkah 1 ⊕ Langkah 9
12. Langkah 3 ⊕ Langkah 9
13. Langkah 2 ⊕ Langkah10
14. Langkah 4 ⊕ Langkah 10

Hasil setiap putaran pada 4 sub-block terakhir yang terdapat pada langkah 11-14.
Transformasi output setelah delapan putaran tersebut adalah sebagai berikut:
Ambil langkah 11-14 pada putaran ke 8

1. $(X_1 * K_{49}) \bmod 12^{16} + 1$
2. $(X_2 + K_{50}) \bmod 12^{16}$
3. $(X_3 + K_{51}) \bmod 12^{16}$
4. $(X_4 * K_{52}) \bmod 12^{16} + 1$.

2.4 *Rivest Shamir Adleman* (RSA)

Kelebihan algoritma RSA terletak pada kesulitan proses memfaktorkan bilangan besar menjadi faktor-faktor bilangan prima, oleh karna itu semakin besar bilangan prima yang digunakan semakin baik atau aman. Kunci yang terdapat pada RSA tedapat 2 kunci antara lain publik dan privat [3].

Menurut [3] Pembentukan kunci RSA adalah sebagai berikut:

1. Secara acak masukan 2 bilangan prima yang berbeda p dan q dengan $p \neq q$. Lebih besar bilangan prima tersebut, tingkat keamanan menjadi lebih baik.
2. n = p*q. Mencari nilai n untuk mendapatkan modulus pada perhitungan kunci publik dan privat.
3. $\varphi(n) = (p-1) * (q-1)$. Perhitungan nilai $\varphi(n)$ ini bersifat rahasia.
4. Menghitung nilai e dengan aturan $1 < e < \varphi(n)$ dan $GCD(\varphi(n), e) = 1$.
5. Mencari nilai d yang merupakan bilangan bulat sehinggga $(d * e) \bmod \varphi(n) = 1$ atau $d = (1 + k * \varphi(n)) / e$. Nilai k dapat diperoleh dengan mencoba berbagai angka untuk mendapatkan nilai d.

Rumus untuk melakukan proses enkripsi menggunakan RSA berdasarkan [3] adalah sebagai berikut:

$$C = M^e \bmod n \quad (2)$$

Dimana:
C = *Chipertext*
M = *Message/Plaintext*
e = kunci publik
n = p*q

Rumus untuk melakukan proses enkripsi menggunakan RSA berdasarkan [3] adalah sebagai berikut:

$$P = C^d \bmod n \quad (3)$$

Dimana:
C = *Chipertext*
P = *Plaintext*
d = kunci privat
n = p*q

2.5 Pengujian *Black Box*

Pengujian dalam penelitian ini menggunakan pengujian *black box*. Tes ini menguraikan serangkaian kondisi input dan menjalankan tes untuk menjelaskan fungsionalitas program. Solusi lain untuk menguji bug yang tidak dapat dicakup oleh pengujian *White Box* adalah dengan menggunakan pengujian *Black Box* [4]. Salah satu metode pengujian yang berfokus pada spesifikasi fungsionalitas dari perangkat lunak disebut *Black Box Testing* [4].

2.6 Pengujian *Wireshark*

Wireshark adalah alat yang ditujukan untuk menganalisis paket data di Internet. *Wireshark* juga menyertakan penganalisis paket jaringan. Fungsi dari penganalisis ini adalah untuk mengumpulkan semua data informasi yang ada dan menampilkan informasi data sedetail mungkin selama komunikasi data melalui jaringan internet [5].

3 Hasil

3.1 Analisis Cara Proses Algortima *International Data Encryption Algorithm* (IDEA)

Algoritma IDEA bekerja pada suatu plaintext yang mempunyai panjang plaintext sebesar 64-bit dan panjang dari kunci sebesar 128-bit. Proses enkripsi dan dekripsi yang dilakukan menggunakan algoritma ini dilakukan 8 putaran yang masing-masing setiap putaran dilakukan 14 langkah, setelah 8 putaran tersebut dilakukan maka dilakukan proses transformasi yang akan menghasilkan suatu ciphertext berformat ASCII. Pembentukan kunci ini dilakukan dengan cara pembagian kunci menjadi subkey lalu dilakukan pergeseran ke kiri sebanyak 25 bit. Dalam proses enkripsi dan dekripsi yang dilakukan oleh algoritma IDEA ini setiap putaran dilakukan langkah-langkah yang sama, langkah-langkah tersebut dapat berupa perkalian, penjumlahan, perpangkatan, XOR, dan juga modulus yang dilakukan sampai 14 kali dalam satu putaran.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

3.2 Analisis Cara Proses Algoritma *Rivest Shamir Adleman* (RSA)

Algoritma RSA ini merupakan algoritma asimetris yang memiliki 2 kunci pada setiap prosesnya. Kunci yang digunakan pada proses enkripsi ini adalah kunci publik. Ketika pembentukan kunci pada RSA ini menghasilkan sebuah nilai e, d, dan n yang akan dimasukan kedalam rumus enkripsi berikut:

$$C = M^e \bmod n \quad (4)$$

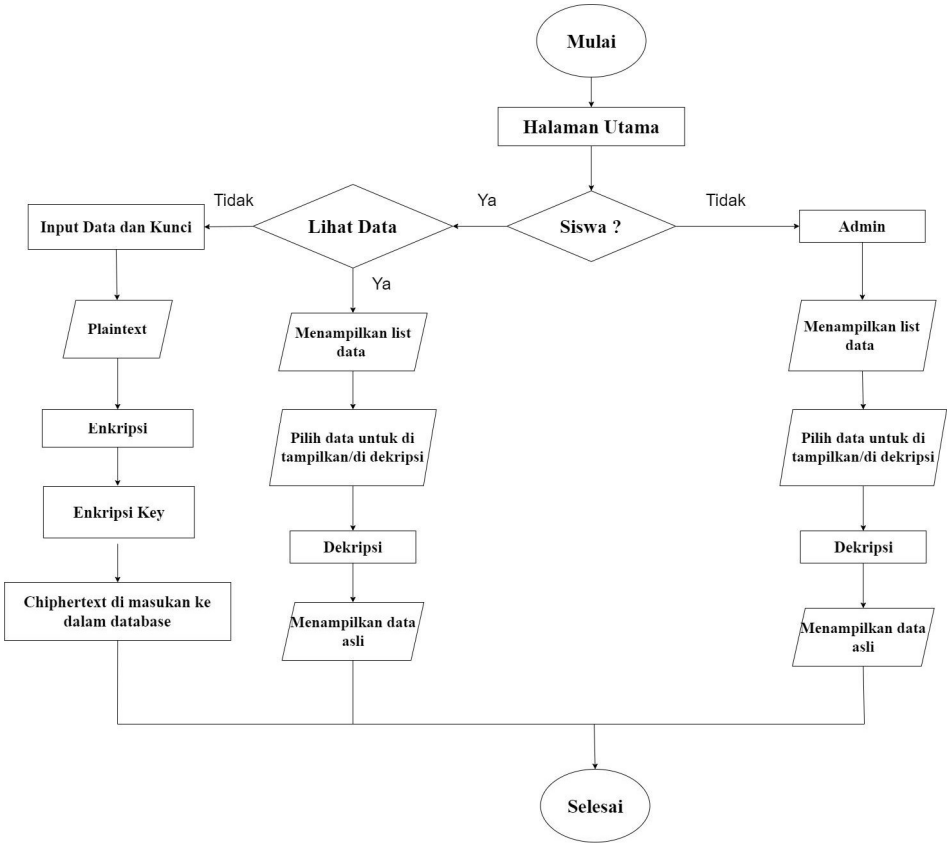
Dimana:
C = Chipertext
M = Message/Plaintext
e = kunci publik
n = p*q

rumus dekripsi berikut:

$$P = C^d \bmod n \quad (5)$$

Dimana:
C = Chipertext
P = Plaintext
d = kunci privat
n = p*q

3.3 Perancangan Perangkat Lunak Enkripsi dan Dekripsi



Gambar. 1. Rancangan Enkripsi-Dekripsi Perangkat Lunak

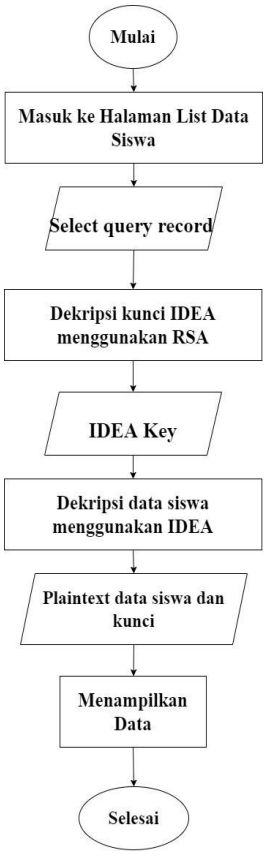
Pada Gambar 1 *flowchart* di atas digambarkan alur dari proses enkripsi dan dekripsi pada perangkat lunak berbasis *website*. Proses penggunaan aplikasi pada flowchart tersebut dibagi menjadi 2 bagian yang proses enkripsi dan proses dekripsi. Kemudian pada proses dekripsi ini dapat dilakukan oleh 2 aktor yaitu admin dan *user*(siswa).

3.4 Rancangan *FlowChart* Enkripsi

Gambar. 2. *Flowchart* Rancangan Enkripsi

Pada Gambar 2 mengagambarkan proses enkripsi ini hanya dapat dilakukan oleh *user*(siswa) untuk menginput nilai mereka yang akan disimpan datanya di *database*. Proses enkripsi ini dimulai dengan memasuki halaman input data terlebih dahulu. Pada halaman tersebut berisi kolom-kolom yang harus diisi oleh setiap user. Kolom - kolom tersebut berisi NIS, NISN, Kelas, Nama, nilai Bahasa Indonesia semester 1 -5, nilai matematika semester 1-5, Bahasa Inggris semester 1-5, biologi semester 1-5, fisika semester 1-5, kimia semester 1-5 dan kunci untuk proses enkripsi tersebut. Setelah semua terinput lalu dilanjutkan dengan proses enkripsi dari kunci algoritma yang digunakan setelah itu hasil-hasil enkripsi semua dimasukan ke dalam *database*.

3.5 Rancangan *FlowChart* Dekripsi

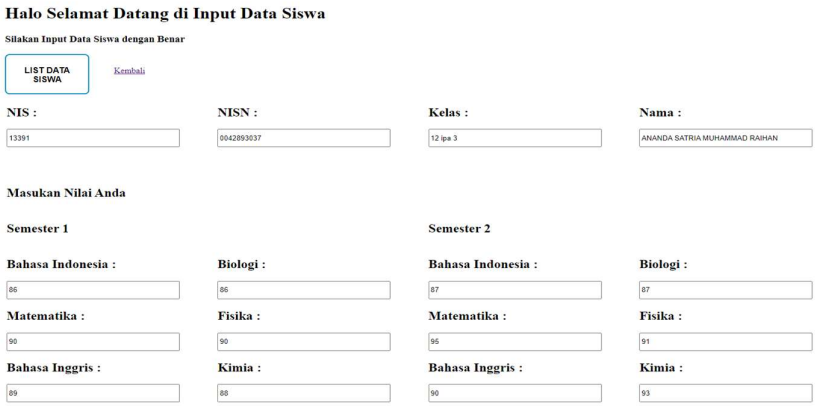


Gambar. 3. *Flowchart* Rancangan Dekripsi

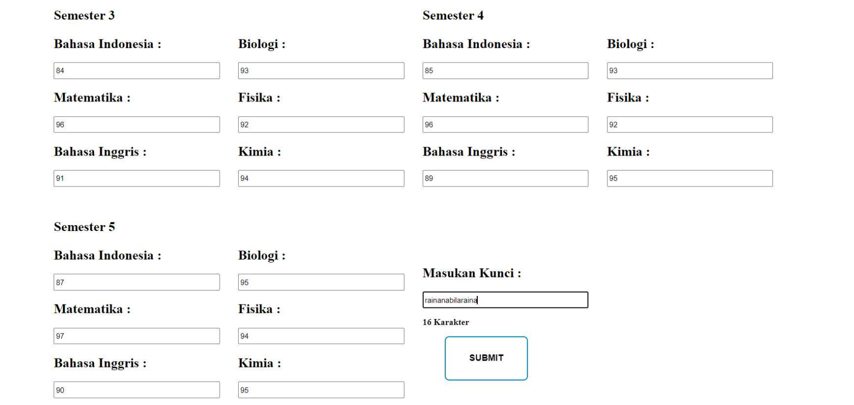
Pada Gambar 3 Proses dekripsi ini dapat dilakukan oleh 2 aktor yaitu admin dan *user*. Pada alur dekripsi ini akan menjelaskan mengenai proses pengembalian nilai yang telah diubah menjadi *ciphertext* pada tahap sebelum nya dan menghasilkan sebuah *plaintext* yang sama seperti yang diinputkan.

3.6 Implementasi Perangkat Lunak

1. Implementasi Proses Enkripsi



Gambar. 4. Implementasi Proses Enkripsi



Gambar. 5. Implementasi Proses Enkripsi

Pada Gambar 4 dan 5 diatas merupakan suatu tampilan dari halaman input data yang telah diisi oleh data siswa yang akan diproses melalui proses enkripsi ketika klik tombol submit. Data siswa yang akan di input berisi NIS, NISN, Kelas, Nama, nilai Bahasa Indonesia semester 1 -5, nilai matematika semester 1-5, Bahasa Inggris semester 1-5, biologi semester 1-5, fisika semester 1-5, kimia semester 1-5 dan kunci untuk proses enkripsi tersebut.

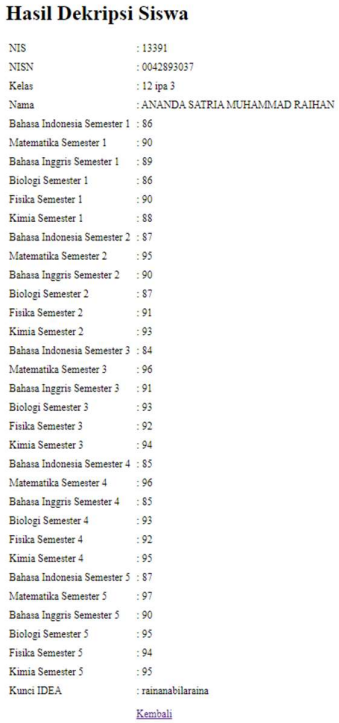
2. Implementasi Proses Dekripsi

CIPHERTEXT DATA SISWA dan KUNCI

No.	NIS	NISN	Kelas	Nama	Bahasa Indonesia Sem 1	Matematika Sem 1	Bahasa Inggris Sem 1	Biologi Sem 1	Fisika Sem 1	Kimia Sem 1	Bahasa Indonesia Sem 2	Matematika Sem 2	Bahasa Inggris Sem 2	Biologi Sem 2	Fisika Sem 2	Kimia Sem 2	Bahasa Indonesia Sem 3	Matematika Sem 3	Bahasa Inggris Sem 3	Biologi Sem 3
1	k?? Y?□??	?O?W?□? ?? KI??s	□□}? 9□??	□??□?d?? {q??□t$□?? wB□Î□	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s
2	??P???B?	p□x?□???? r?%???	?p?□ 乄#S	?ŜoL?□y2??e{7o? iM? ???~????d4	?,□?????	?? KI??s	□□??? =v?	?,□?????	?? KI??s	(8c?□???	???*?+??	□???辭?	?? KI??s	???*?+??	?? KI??s	3hg??/??	b????Tx?	?v? lM(	???? {M??	3hg??/??
3	b)H?□!? ^	???T🡅?>R? s/???.?	?-□?f? 5nu??? 2?>?	?O??? W%□h???□?????? x}?&	□??% [o??	b????Tx?	(8c?□???	□??□Iy??	???*? +??	□??% [o??	???*?+??	???*?+??	□□??? =v?	?? KI??s	□□??? =v?	3hg??/??	b????Tx?	□□???=v?	?? KI??s	?□□7??? [
4	k?? Y?□??	?O?W?□? ?? KI??s	?p?□ 乄#S	□??□?d?? {q??□t$□?? wB□Î□	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s
5	?□□??? w?	?? I5X?□?□□ nGY(?	?-□?f? 5n	?8?u|{□?$g?□h?H	?5?&?E? O	□??%[o??	???*?+??	□??% [o??	□??% [o??	□??% [o??	□??□Iy??	???*?+??	(8c?□???	?,□?????	???*? +??	^??□? N??	?? KI??s	????{M??	?? KI??s	□□??? =v?
6	?□?>? h□?	?□|???q? ^??□?N??	□Gí????	?xc? 짚,H???□IM??↲?? ↲K	A??t???$	(8c?□???	???*?+??	?,□?????	?,□?????	□??□Iy??	b????Tx?	3hg??/??	(8c?□???	(8c?□???	A??t??? $	□□??? =v?	???*?+??	?□□7???[	□□??? =v?	???? {M??
7	□□??□(? 1	?6?□#Q? x%C,?□:_□	□Gí????	??[ꞓ□ C >+? +D?????$R?Oa	□??% [o??	(8c?□???	□??□Iy??	?,□?????	???? {M??	?? KI??s	?,□?????	?? KI??s	A??t???$	□□??? =v?	?? KI??s	^??□? N??	(8c?□???	?,□?????	b????Tx?	?? KI??s
8	k?? Y?□??	?O?W?□? ?? KI??s	?-□?f? 5n	□??□?d?? {q??□t$□?? wB□Î□	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s	?? KI??s
9	攷□®??	???Q□? ┌#E%1?t□	□Gí????	□?+?煨![?□?? ¸i0v??Z□SJ	A??t???$	(8c?□???	□□??? =v?	?,□?????	?? KI??s	?5?&?E? O	□??% [o??	□□???=v?	?? KI??s	(8c?□???	?,□?????	???*? +??	b????Tx?	???*?+??	???? {M??	?,□?????
10	?< 6□]□?	LQ?S??A?? s/???.?	8Rs? bi□?	Rz?F? ‴+g`tzOLə-□? &?z	?? KI??s	???*?+??	?? KI??s	?5?&?E? O	A??t??? $	b????Tx?	□??□Iy??	???*?+??	???? {M??	□??□Iy??	□??% [o??	?? KI??s	b????Tx?	?? KI??s	?□□7??? [	(8c?□???

Gambar. 6. Tabel Ciphertext

Pada Gambar 6 tersebut terdapat *list data* yang berupa ciphertext hasil dari enkripsi seluruh data siswa mulai dari NIS, NISN, Kelas, Nama, nilai Bahasa Indonesia semester 1 -5, nilai matematika semester 1-5, Bahasa Inggris semester 1-5, biologi semester 1-5, fisika semester 1-5, kimia semester 1-5 dan kunci untuk proses enkripsi tersebut.



Hasil Dekripsi Siswa

NIS	: 13391
NISN	: 0042893037
Kelas	: 12 ipa 3
Nama	: ANANDA SATRIA MUHAMMAD RAIHAN
Bahasa Indonesia Semester 1	: 86
Matematika Semester 1	: 90
Bahasa Inggris Semester 1	: 89
Biologi Semester 1	: 86
Fisika Semester 1	: 90
Kimia Semester 1	: 88
Bahasa Indonesia Semester 2	: 87
Matematika Semester 2	: 95
Bahasa Inggris Semester 2	: 90
Biologi Semester 2	: 87
Fisika Semester 2	: 91
Kimia Semester 2	: 93
Bahasa Indonesia Semester 3	: 84
Matematika Semester 3	: 96
Bahasa Inggris Semester 3	: 91
Biologi Semester 3	: 93
Fisika Semester 3	: 92
Kimia Semester 3	: 94
Bahasa Indonesia Semester 4	: 85
Matematika Semester 4	: 96
Bahasa Inggris Semester 4	: 85
Biologi Semester 4	: 93
Fisika Semester 4	: 92
Kimia Semester 4	: 95
Bahasa Indonesia Semester 5	: 87
Matematika Semester 5	: 97
Bahasa Inggris Semester 5	: 90
Biologi Semester 5	: 95
Fisika Semester 5	: 94
Kimia Semester 5	: 95
Kunci IDEA	: rainanabilaraina

Kembali

Gambar. 7. Implementasi Hasil Dekripsi

Pada Gambar 7 terdapat hasil dari proses dekripsi dari data siswa dan kuncinya yang terdiri dari NIS, NISN, Nama, nilai Bahasa Indonesia semester 1 -5, nilai matematika semester 1-5, Bahasa Inggris semester 1-5, biologi semester 1-5, fisika semester 1-5, kimia semester 1-5 dan kunci untuk proses enkripsi tersebut.

3.7 Pengujian Fungsionalitas Menggunakan *BlackBox*

Pengujian menggunakan *BlackBox* ini untuk menguji fungsionalitas dari suatu perangkat lunak dalam proses enkripsi dan dekripsi. Berikut hasil dari pengujian menggunakan *BlackBox* pada perangkat lunak proses enkripsi dan dekripsi menggunakan algoritma IDEA dan RSA. Hasil pengujian *BlackBox* di gambarkan pada tabel 1 Hasil Pengujian *BlackBox* dibawah ini:

Tabel 1. Hasil Pengujian *BlackBox*

No	Pengujian	Tindakan Pengujian	Hasil Pengujian	Kesimpulan Pengujian
1	Input Data Siswa/Enkripsi Data	Melakukan input data siswa.	Data berhasil dimasukan ke dalam database dalam bentuk ciphertext	Berhasil
2	Menampilkan *List Data siswa /Ciphertext*	Melakukan klik button pada List Data Siswa dan akan tampil tabel yang berisi ciphertext dari data siswa	Data siswa yang berupa ciphertext pada database berhasil ditampilkan pada tabel	Berhasil
3	Menampilkan Data Siswa berupa *Plaintext*	Melakukan klik pada data yang ingin ditampilkan secara detail dalam berupa plaintext	Data siswa yang sebelumnya berupa ciphertext berhasil berubah dan berhasil ditampilkan dalam berupa plaintext	Berhasil

3.8 Pengujian Waktu Proses

1. Pengujian Waktu Enkripsi

Pada tabel 2 menampilkan hasil pengujian waktu proses enkripsi data siswa, pada tabel tersebut diambil dari data nama karna dalam setiap data yang terinput perbedaan panjang karakter terdapat di pada data nama, pengambilan data nama dalam tabel tersebut diambil dari data nama yang memiliki panjang karakter terpanjang dan terpendek. Pada hasil pengjian waktu secara keseluruhan rata-rata waktu enkripsi dengan RSA adalah 0,21(mikrodetik) dan untuk rata-rata waktu enkripsi tanpa RSA adalah 0.14(mikrodetik), lalu untuk rata rata selisih perbedaan waktu antara dengan RSA dan tanpa RSA adalah 0,06(mikrodetik). Perubahan waktu tersebut disebabkan karna perbedaan panjang karakter yang diinputkan, semakin panjang karakter yang dienkripsi maka waktu yang dibutuhkan semakin lama.

Tabel 2. Hasil Pengujian Waktu Enkripsi

No	Nama	Jumlah Karakter	Dengan RSA (mikrodetik)	Tanpa RSA (mikrodetik)
1	RADEN FITZAL BINTANG NUGRAHA WIRADIKOESOEMA	43	0.35	0.25
2	REZA APRIONO	12	0.15	0.10

1. Pengujian Waktu Dekripsi

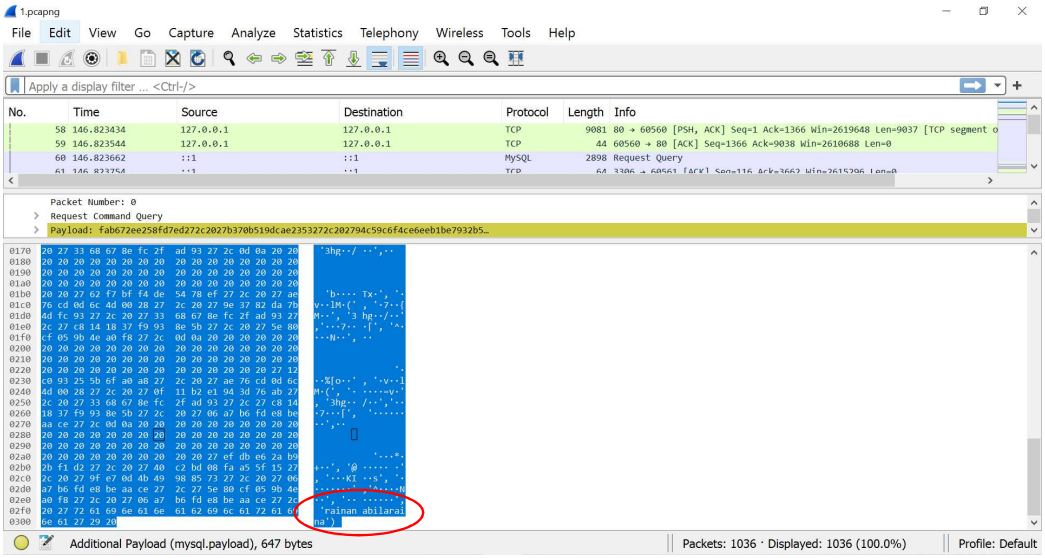
Pada tabel 4.16 menampilkan hasil pengujian waktu proses dekripsi data siswa, pengambilan data dalam tabel tersebut diambil dari data nama yang memiliki panjang karakter terpanjang dan terpendek. Pada hasil pengujian waktu secara keseluruhan rata-rata waktu dekripsi dengan RSA adalah 0,01(mikrodetik) dan untuk rata-rata waktu dekripsi tanpa RSA adalah 0.01(mikrodetik), lalu untuk rata rata selisih perbedaan waktu antara dengan RSA dan tanpa RSA adalah 0. Tidak terdapat perbedaan waktu proses dalam pengujian waktu dekripsi data siswa, oleh karna itu penggunaan atau tidak RSA dalam proses dekripsi data siswa ini tidak mempengaruhi.

Tabel 3. Hasil Pengujian Waktu Dekripsi

No	Nama	Jumlah Karakter	Dengan RSA (mikrodetik)	Tanpa RSA (mikrodetik)
1	RADEN FITZAL BINTANG NUGRAHA WIRADIKOESOEMA	43	0.01	0.01
2	REZA APRIONO	12	0.01	0.01

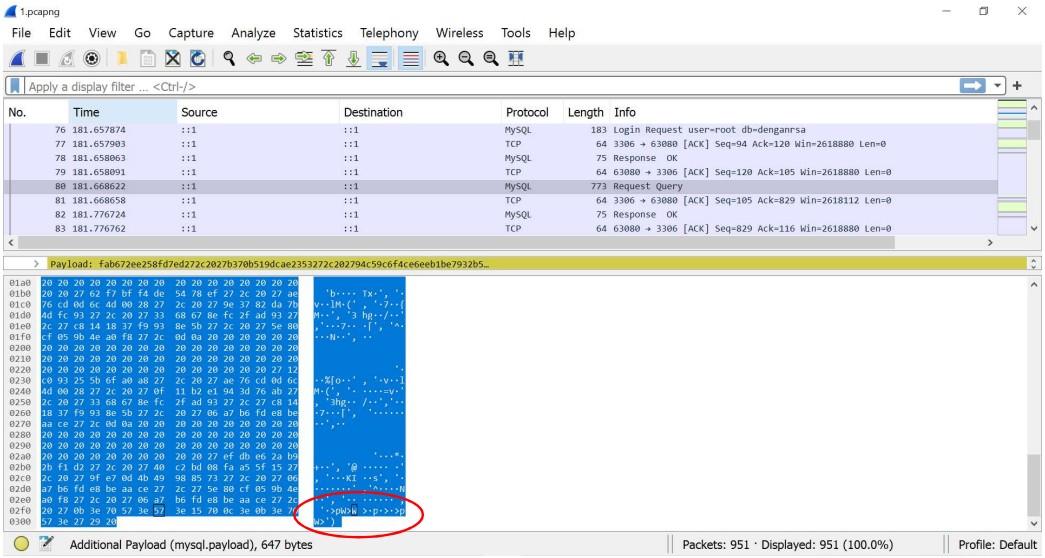
3.9 Pengujian Menggunakan *Wireshark*

Pengujian ini dilakukan dengan menggunakan suatu aplikasi bernama wireshark. Wireshark digunakan untuk menguji keamanan data pada data siswa yang telah di lakukan penerapan keamanan data menggunakan algoritma IDEA dan RSA dan algortima IDEA tanpa RSA.



Gambar. 8. Hasil Pengujian *Wireshark* Tanpa RSA

Gambar 8 merupakan suatu gambar dari proses *capture data* menggunakan *wireshark* pada proses input data menggunakan algoritma IDEA saja. Pada hasil *capture data* tersebut didapat sebuah kunci yang berupa plaintext dari proses enkripsi data siswa menggunakan algoritma IDEA sehingga kunci tersebut dapat dibaca dan dimengerti maknanya.



Gambar. 9. Hasil Pengujian *Wireshark* Tanpa RSA

Gambar 9 merupakan suatu gambar dari proses *capture data* menggunakan *wireshark* pada proses input data menggunakan algoritma IDEA saja. Pada hasil *capture data* tersebut didapat sebuah kunci yang berupa ciphertext dari proses enkripsi data siswa menggunakan algoritma IDEA sehingga kunci tersebut tidah dapat dibaca dan tidak dimengerti maknanya.

3.10 Analisis Hasil Luaran

Analisis hasil luaran pada penelitian ini dilihat dari perbedaan panjang karakter Ketika proses enkripsi dan dekripsi berlangsung, pada data yang terinput ini terdapat perubahan karakter menjadi minimal mempunyai 8 karakter atau kelipatannya. Perubahan karakter ini terjadi ketika jumlah karakter dari data yang diinput tersebut bukan kelipatan 8 maka akan terjadi penambahan karakter sampai dengan kelipatan 8. Untuk input data kunci ini digunakan algoritma yang berbeda dengan data siswa dapat dianalisis bahwa panjang karakter yang dihasilkan dari proses enkripsi menggunakan algoritma RSA tidak berubah masih sama 16 karakter.

4 Kesimpulan dan Saran

4.1 Kesimpulan

1. Menggunakan algortima IDEA data siswa dapat diamankan karna terjadinya perubahan plainteks menjadi cipherteks yang dimana ini menyebabkan data siswa tidak dapat dibaca dan dimengerti maknanya.
2. Menggunakan kombinasi algoritma IDEA dan RSA menghasilkan suatu perubahan karakter pada kunci IDEA yang menyebabkan kunci IDEA tidak dapat dimengerti maknanya, lalu untuk penggunaan algoritma IDEA saja tidak menghasilkan perubahan karakter sehingga kunci IDEA ini dapat dimengerti maknanya.
3. Pengujian waktu proses menggunakan IDEA dan RSA lebih lama dengan rata-rata perbedaan waktu 0,06 (mikrodetik). Sedangkan untuk pengujian waktu dekripsi tidak terdapat perubahan, oleh karna itu penggunaan RSA dalam proses dekripsi tidak berpengaruh.
4. Proses enkripsi menggunakan algoritma IDEA berhasil dibuat dan untuk kunci IDEA menggunakan algoritma RSA berhasil dibuat dengan menghasilkan suatu ciphertext.
5. Proses dekripsi menggunakan algoritma IDEA berhasil dibuat dan untuk kunci IDEA menggunakan algoritma RSA berhasil dibuat dengan menghasilkan suatu plaintext.
6. Pada proses enkripsi dan dekripsi menghasilkan perubahan panjang karakter. Penambahan karakter sampai jumlahnya 8 atau kelipatan 8.

4.2 Saran

1. Penelitian selanjutnya dapat menerapkan algoritma kriptografi kunci asimetris dan simetris yang lainnya agar proses keamanan data bisa dilakukan secara maksimal.

Referensi

[1] Mukhtar, H. (2018). Kriptografi untuk Keamanan Data. Yogyakarta: CV Budi Utama.

[2] Janner Simarmata, S. d. (2019). Kriptografi Teknik Keamanan Data dan Informasi. Yogyakarta: CV. ANDI OFFSET.

[3] Martono. (2017). Model Modifikasi Kriptografi Algoritma Rsa Untuk Keamanan Data Pada Database E-Voting. Jurnal Ilmiah Media Sisfo, 11(2), 896–910. http://ejournal.stikom-db.ac.id/index.php/mediasisfo/article/view/245

[4] Nurudin, M., Jayanti, W., Saputro, R. D., Saputra, M. P., & Yulianti, Y. (2019). Pengujian Black Box pada Aplikasi Penjualan Berbasis Web Menggunakan Teknik Boundary Value Analysis. Jurnal Informatika Universitas Pamulang, 4(4), 143. https://doi.org/10.32493/informatika.v4i4.3841

[5] Luthfansa, Z. M., & Rosiani, U. D. (2021). Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet. Journal of Information Engineering and Educational Technology, 5(1), 34–39. https://doi.org/10.26740/jieet.v5n1.p34-39