JURNAL RESISTOR | ISSN 2598-7542 | E-ISSN 2598-9650
Vol. 3 No 1 – April 2020 | https://s.id/jurnalresistor
DOI: https://doi.org/10.31598
Publishing: Prahasta Publisher

Pengamanan Data Nilai Mahasiswa Menggunakan Algoritma *Caesar Chiper* dan *RSA* Berbasis *Web*

Nurhaliza Aulia Putri[1], Emilia Hesti[2,] Aryanti Aryanti[3]*
[1,2,3]Program Studi Teknik Telekomunikasi, Jurusan Teknik Elektro, Politeknik Negeri Sriwijaya
Jl. Srijaya Negara, Bukit Besar, Ilir Barat I, Kota Palembang, Sumatera Selatan, Indonesia

e-mail: lizaputri996@gmail.com[1], emiliahesti@ymail.com[2], aryanti@polsri.ac.id[3*]

Received : July, 2024	Accepted : July, 2024	Published : August, 2024

Abstract

The development of technology and information in the current digital era has profoundly influenced human activities, particularly in the field of education. In this highly sophisticated age, all academic activities utilize technology with appropriate security measures to safeguard confidential data. Various security techniques, including cryptographic methods, have been developed to ensure data confidentiality. The methods employed for data security utilize the Caesar Cipher and RSA algorithms. In applying these algorithms, several stages are involved: the original data (plaintext) is encrypted using the Caesar Cipher algorithm by determining a shift value K to displace each character. Subsequently, the data is encrypted using the RSA algorithm by determining two distinct keys p and q. The RSA algorithm involves two keys, namely the public and private keys. The public key is used for encryption, while the private key is used for decryption processes. This research focuses on securing student grade data from unauthorized access and falsification using the Caesar Cipher and RSA methods. Test results indicate that both the Caesar Cipher and RSA encryption processes successfully transform plaintext into ciphertext that cannot be directly read without appropriate decryption processes.

Keywords: *cryptography, education, caesar chipper, RSA*

Abstrak

Perkembangan ilmu teknologi dan informasi di era digital saat ini sangat berpengaruh besar terhadap aktfitas yang dilakukan manusia terutama di bidang Pendidikan. Di zaman yang serba canggih ini semua aktivitas akademik sudah menggunakan teknologi yang mempunyai keamanan yang tepat untuk memastikan keamanan suatu data yang bersifat rahasia. Untuk memastikan kerahasiaan data, berbagai teknik keamanan telah dikembangkan, termasuk metode kriptografi. Metode yang digunakan untuk pengamanan data menggunakan metode *Caesar Chiper* dan RSA. Dalam menggunakan metode algoritma tersebut ada beberapa tahapan yang dilakukan yaitu data asli (*plaintext*) di *encrypt* menggunakan algoritma *Caesar Chiper* dengan menentukan nilai K untuk menggeser setiap karakter, selanjutnya data di *encrypt* menggunakan algortima RSA dengan menentukan dua kunci yang berbeda yaitu nilai p dan q. Algoritma RSA terdapat 2 kunci antara lain publik dan privat. Kunci *public* digunakan untuk melakukan proses *encrypt*, sedangkan kunci privat digunakan untuk melakukan proses *decrypt*. Pada penelitian ini dilakukan terhadap keamanan data nilai mahasiswa yang bertujuan untuk mengamankan data dari pihak yang tidak berwenang mengaksesnya dan memalsukan data tersebut dengan menggunakan metode *Caesar Chiper* dan RSA. Hasil pengujian menunjukkan bahwa kedua proses *encrypt Caesar Cipher* dan RSA berhasil mengubah *plaintext* menjadi *ciphertext* yang tidak dapat dibaca secara langsung tanpa melakukan proses *decrypt* yang sesuai.

Kata Kunci: kriptografi, pendidikan, caesar chiper, RSA

1. PENDAHULUAN

Di zaman *modern* ini, kemajuan teknologi telah mengalami perkembangan cepat yang telah mengubah perspektif masyarakat terhadap cara berkomunikasi [1]. Semakin maju teknologi, semakin meningkat pula risiko keamanannya [2]. Dalam hal ini keamanan dan privasi adalah aspek yang sangat penting dalam hal data [3]. Adapun penelitian terkait sebelumnya membahas tentang pengujian teknik *encrypt* menggunakan algoritma *Caesar Chiper* untuk keamanan dalam pengiriman pesan [4]. Selanjutnya penelitian terkait membahas tentang pengujian teknik kriptografi terhadap pengamanan data transkrip akademik mahasiswa menggunakan algoritma *Rivest Shamir Adleman* (RSA) [5].

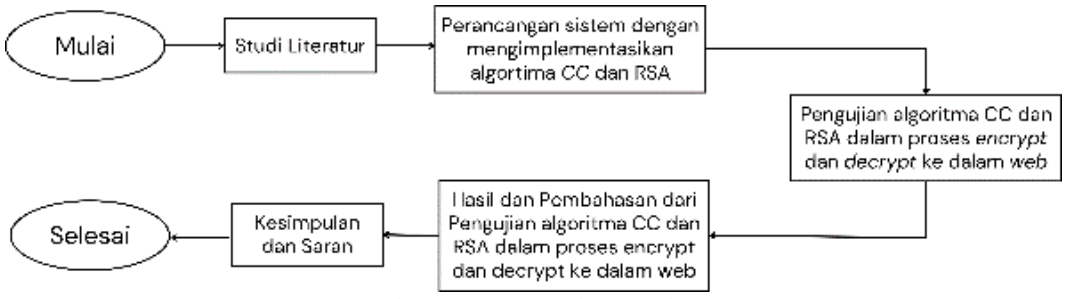
Penggunaan *Caesar Cipher* memberikan lapisan keamanan dengan menggeser nilai-nilai karakter teks [6], sementara RSA, dengan kekuatan kriptografi kuncinya, mengamankan proses *encrypt* dan *decrypt* yang lebih kompleks [5]. Kombinasi kedua algoritma ini memungkinkan sistem pengelolaan nilai siswa berbasis web untuk melindungi data sensitif dari pihak yang tidak berwenang mengaksesnya dan memalsukan data tersebut.

Dengan demikian, Implementasi ini tidak hanya meningkatkan keamanan terhadap potensi ancaman siber, tetapi juga memberikan keyakinan kepada pengguna bahwa data pribadi mereka terjaga dengan baik dalam era digital yang semakin terhubung [3].

Penelitian ini membahas tentang pengujian sistem pengamanan web terhadap data nilai mahasiswa dengan menggunakan metode kriptografi *Caesar Chiper* dan *Rivest Shamir Adleman* (RSA). Algoritma *Caesar Cipher* dan *Rivest Shamir Adleman* (RSA) terhadap keamanan data nilai mahasiswa berbasis *web* bertujuan untuk mengamankan data dari pihak yang tidak berwenang mengaksesnya dan memalsukan data tersebut. Hal ini merupakan langkah kritis dalam memastikan integritas dan kerahasiaan informasi Pendidikan [7]. Dalam konteks ini, *Caesar Cipher* digunakan untuk mengenkripsi nilai mahasiswa secara sederhana tetapi efektif [8], sementara RSA digunakan karena dianggap efektif dalam proses *encrypt*, sehingga data yang telah di *encrypt* memiliki tingkat keamanan yang tinggi terhadap upaya pencurian data [9].

2. METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur dengan mengumpulkan referensi dari berbagai sumber seperti buku, artikel, jurnal, dan situs web yang membahas tentang algoritma *Caesar Chiper* dan RSA.



Gambar 1: Rancang Alur Penelitian

Penjelasan dari Gambar 1 diatas dimulai dengan melakukan Studi Literatur. Studi Literatur merupakan tahapan peneliti dalam mengambil beberapa data yang berasal dari beberapa sumber seperti buku, skirpsi, thesis, jurnal dan dari internet sebagai acuan referensi dalam penelitian ini. Proses kedua melakukan pengujian algoritma CC dan RSA dalam proses *encrypt* dan *decrypt* ke dalam *web*. tahapan ini digambarkan dalam bentuk *flowchart* yang menunjukkan cara kerja dari web yang akan beroperasi. Proses ketiga Menjelaskan hasil dari Pengujian algoritma CC dan RSA dalam proses *encrypt* dan *decrypt* ke dalam web. Proses keempat membuat kesimpulan dan saran terhadap penelitian ini.

Perancangan tampilan *interface* sistem terdiri dari:

1. *Interface* Jurusan
2. *Interface* Program Studi
3. *Interface* Dosen
4. *Interface* Kelas
5. *Interface* Mahasiswa

6. *Interface* Mata Kuliah
7. *Interface* Nilai

Program komputer yang digunakan untuk membangun sistem ini menggunakan perangkat lunak *Visual Studio Code* dan menggunakan *database PhpMyAdmin*.

Algoritma *Caesar Cipher* salah satu metode terlama dan sangat sederhana [10]. *Caesar Chiper* diciptakan pada abad ke-19 oleh Julius Caesar untuk mengamankan data yang dikirim yaitu mengubah setiap huruf di dalam pesan atau mengubah huruf menjadi angka [4]. Rumus umum untuk *encrypt* dan *decrypt algoritma Caesar Cipher* sebagai berikut [4]:

Enkripsi:

$$E(x)= x + K \bmod 26 \quad (1)$$

Dekripsi:

$$D(x)= x – K \bmod 26 \quad (2)$$

K merupakan kunci yang digunakan untuk menggeser posisi karakter x.

RSA diciptakan dari hasil karya tiga peneliti dari MIT (*Massachusetts Institute of Technology*) pada tahun 1976, yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. RSA adalah teknik kriptografi di mana kunci untuk enkripsi berbeda dari kunci untuk dekripsi. Berikut ini menurut [9] adalah pembentukan kunci RSA :

1. Dua bilangan prima p dan q yang berbeda dipilih secara random, di mana $p \neq q$. Semakin besar bilangan prima tersebut, semakin baik tingkat keamanannya.
2. n = p*q. Nilai n digunakan sebagai modulus dalam perhitungan kunci publik dan privat.
3. Menghitung nilai $\phi(n) = (p –1) * (q –1)$. Perhitungan nilai $\phi(n)$ ini dijaga kerahasiaannya.
4. Menghitung nilai e menggunakan ketentuan $1 < e < \phi(n)$ dan GCD (*greater common divisor*) $(\phi(n), e) = 1$.
5. Menentukan nilai d sebagai bilangan bulat sehingga $(d * e) \bmod \phi(n) = 1$, yaitu $d = (1 + k * \phi(n)) / e$. Nilai d ditemukan dengan mencoba berbagai angka untuk memperoleh nilai d yang sesuai.

2.1 Proses *Encrypt* Data

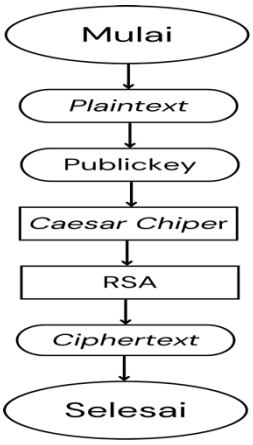
Proses *encrypt* data ditunjukkan oleh Gambar 2 yang dimulai dengan masuk ke halaman input data nilai mahasiswa terlebih dahulu. Pada halaman tersebut berisi kolom-kolom yang harus diisi dengan data asli (*plaintext*) berupa nama mahasiswa, nama dosen, mata kuliah, nilai, dan nilai huruf. Setelah semua selesai diinput selanjutnya data tersebut akan melakukan proses *encrypt.* Pada penelitian ini data yang melakukan proses *encrypt hanya* data nilai dan nilai huruf menggunakan algortima Caesar Chiper dan RSA. Setelah itu data hasil *encrypt* tersimpan ke dalam *database* dalam bentuk data acak (*ciphertext*).

Dalam kasus yang akan dibahas penulis menggunakan nilai K yang bernilai 9 dengan *plaintext* nilai = 50 dan nilai huruf = B

Algoritma *Caesar Chiper*:

Tabel 1: Substitusi

0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?	@	A	B
9	:	;	<	=	>	?	@	A	B	C	D	E	F	G	H	I	J	K



Gambar 2: *Flowchart Encrypt* Data

Berdasarkan tabel di atas diambil hasil *encrypt Caesar Chiper* yaitu:

Plaintext (nilai) : 50
Ciphertext : > 9

Algoritma RSA:

1. Menentukan dua buah bilangan prima yaitu inilai p dan nilai q, didalam kasus ini nilai prima tersebut dibuat menjadi nilai acak (random), sehingga didapatkan nilai seperti yang ditunjukkan pada Tabel 2.

Tabel 2: Nilai p dan q

p	104738371990314934962274654488168959301756674139033247930461890118561795895268028286332318531636926992821008722316936067730321349187889825654711254401 98313
q	123194897673497501995887885149543664686096299255584332241176097859025448233779901920344877680290097923316077937639557229225156018416551753217121149794 71241

2. Menghitung nilai n = p*q =
   1047383719903149349622746544881689593017566741390332479304618901185617958952680282863323185316369269928210087223169360677303213491878898256547112544019831 3 * 1231948976734975019958878851495436646860962992555843322411760978590254482337799019203448776802900979233160779376395572292251560184165517532171211497947124 1
   =1290323301983556530883230562089101277737687129324301319646618661119271471016717901962724757521461466888140878557497881619533037148829384958708364580758532425259014621034226032344183874601851935196557186973924188659882953799390975405913268033806039200195676485298109463260837390307143045745218390413949202164633.
3. Menghitung nilai ϕ(n) = (p –1) * (q –1) =
   1047383719903149349622746544881689593017566741390332479304618901185617958952680282863323185316369269928210087223169360677303213491878898256547112544019831 2 * 1231948976734975019958878851495436646860962992555843322411760978590254482337799019203448776802900979233160779376395572292251560184165517532171211497947124 0
   = 9194428684393071233300836078659424381911740232386242329133965306835408013279917850845022171408308787246740866214709133527250065708660622518351743009938759933226191991734261737950255036262784070947484307655677199241470664587533078063601629808311025251250651668700954019867783518802421510453068190636992083.
4. Menghitung nilai (kunci) e menggunakan ketentuan 1 < e < ϕ(n) dan GCD(ϕ(n), e) = 1. Kunci publik e yaitu 65537 (pilihan umum terhadap nilai e).
5. Mencari nilai d
   d = (1 + (k * ϕ (n)) / e)
   d = (1 + (k * 9194428684393071233300836078659424381911740232386242329133965306835408013279917850845022171408308787246740866214709133527250065708660622518351743009938759933226191991734261737950255036262784070947484307655677199241470664587533078063601629808311025251250651668700954019867783518802421510453068190636992083511802421510453068190636992083.
   nilai k adalah angka acak yang digunakan dalam pencarian sampai menghasilkan nilai d yang diinginkan, yaitu d = 1169180141980736393639772398783880712836639035778175832978238286340644476171579045274492988703396062524762469021445201978948531028977283006361864630113747593054183721251487287809981557950927146879646305526483255364575907767858283475326397540334741944092229313489917413215185638371170252016041765284441897016333.
6. Dari Langkah-langkah yang telah dijelaskan diatas, maka telah terbentuk pasangan kunci, yaitu *public key* (n,e) dan *private key* (n,d) seperti yang ditunjukkan pada Tabel 3 dan Tabel 4.

Tabel 3: *Public Key*

n	1290323301983556530883230562089101277737687129324301319646618661119271471016 7179019627247575214614668881408785574978816195330371488293849587083645807585 3242525901462103422603234418387460185193519655718697392418865988295379939097 5405913268033806039200195676485298109463260837390307143045745218390413949202 16433
e	65537

Tabel 4: *Private Key*

n	1290323301983556530883230562089101277737687129324301319646618661119271471016 7179019627247575214614668881408785574978816195330371488293849587083645807585 3242525901462103422603234418387460185193519655718697392418865988295379939097 5405913268033806039200195676485298109463260837390307143045745218390413949202 16433
d	1169180141980736393639772398783880712836639035778175832978238286340644476171 5790452744929887033960625247624690214452019789485310289772830063618646301137 4759305418372125148728780998155795092714687964630552648325536457590776785828 3475326397540334741944092229313489917413215185638371170252016041765284441897 01633

Ciphertext = > 9
> 9 di preprocessing
dimana > = 62, 9=57
dengan cara $57x256^1 + 62x256^0 = 15929$

$C_i = M_i^e \bmod N$
$C_1 = 15929^{65537} \bmod 12903233019835565308832305620891012777376871293243013196466186611192714710167179019627247575214614668881408785574978816195330371488293849587083645807585324525901462103422603234418387460185193519655718697392418865988295379939097540591326803380603920019567648529810946326083739030714304574521839041394920216433

C_1 = 3568307407781951583655345282377713920006539454747931995141238213950680897752170871528946554071231261928985387784654534372777083272886432690012943447242043825471457377398322625354723791146968927965484018078109952834950428563148427549432598367832506557082673652201378795156437698310195986951079374690776932788

Algoritma *Caesar Chiper*:
Berdasarkan table 1 di atas diambil hasil *encrypt Caesar Chiper* yaitu:
Plaintext (nilai huruf) : B
Cihphertext : K

Algoritma RSA:

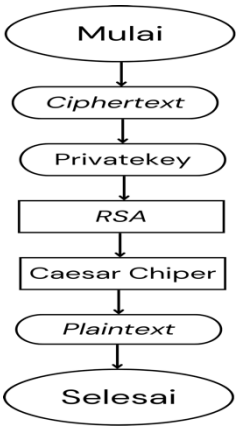
1. Menentukan dua buah bilangan prima secara acak, dalam kasus ini bilangan tersebut sama dengan table 2 diatas.
2. Menghitung nilai n = p*q =1047383719903149349622746544881689593901756674139033247930461890118561795895268028286332318531636926992821021087223169360677302134918788982565471125440198313 * 1231948976734975019958878851495436646860962992555843322411760978590254482337799019203448776802900979233160779376395572292251560184165517532171211497947124 1 =1290323301983556530883230562089102777376871293243013196466186611192714710167179019627247575214614668881408785574978816195330371488293849587083645807585324525901462103422603234418387460185193519655718697392418865988295379939097540591326803380603920019567648529810946326083739030714304574521839041394920216433.
3. Menghitung nilai ϕ(n) = (p –1) * (q –1) = 1047383719903149349622746544881689593017566741390332479304618901185617958952680282863323185316369269928210087223169360677302134918788982565471125440198312 *1231948976734

975019958878851495436646860962992555843322411760978590254482337799019203448776802900979233160779376395572292251560184165517532171211497947124
= 919442868439307123330083607865942438191174023238624232913396530683540801327991785084502217140830878724674086621470913352725006570866062251835174300993875993226199173426173795025503626278407094748430765567719924147066458753307806360162980831102525125065166870095401986778351880242151045306819063699208. |
| 4. | Menghitung nilai (kunci) e menggunakan ketentuan 1 < e < ϕ(n) dan GCD(ϕ(n), e) = 1. Kunci publik e yaitu 65537 (pilihan umum terhadap nilai e). |
| 5. | Mencari nilai d
d = (1 + (k * ϕ (n)) / e)
d = (1 + (k * 919442868439307123330836078659424381911740232386242329133965306835408013279917850845022171408308787246740866214709133527250065708660622514183517430099387599332261991734261737950255036262784070947484307655677199241470664587533078063601629808311025251250651668700954019867783518802421510453068190636992083.
Nilai k adalah angka acak yang digunakan dalam pencarian sampai menghasilkan nilai d yang diinginkan, yaitu d = 116918014198073639363977239878388071283663903577817583297823828634064447617157904527449298870339606252476246902144520197894853102897728300636186463011374759305418372125148728780998155795092714687964630552648325536457590776785828347532639754033474194409222931348991741321518563837117025201604176528444189701633Dari Langkah-langkah yang telah dijelaskan diatas, maka telah terbentuk pasangan kunci, yaitu *Public key* (n,e) dengan nilai sama dengan Tabel 3 di atas dan *private key* (n,d) dengan nilai sama dengan Tabel 4 di atas. |

Ciphertext: K
K di preprocessing
dimana K = 75
dengan cara $75x256^0 = 75$

$C_i = M^e \bmod N$
$C_1 = 75^{65537} \bmod 129032330198355653088323056208910127773768712932430131964661866111927147101671790196272475752146146688814087855749788161953303714882938495870836458075853242525901462103422603234418387460185193519655718697392418865988295379939097540591326803380603920019567648529810946326083739030714304574521839041394920216433
C_1 = 623378384382886590622901614067571125426765011787690663852051251577956777523551493262277749973411217287404207471851807254660583969621120573052200209151306224862230719489763392048944773776399781607097362522707347031741089411404709492777168824292862427446142534979601511094306409938733704218128950268579635509.

2.2 Proses *Decrypt* Data



Gambar 3: *Flowchart Decrypt* Data

Algoritma RSA:
Berdasarkan hasil *encrypt* RSA yaitu :
Ciphertext (nilai) :
35683074077819515836553452823777139200
06539454747931995141238213950680897752
17087152894655407123126192898538778465
45343727770832728864326900129434472420
43825471457377398322625354723791146968
92796548401807810995283495042856314842
75494325983678325065570826736522013787
95156437698310195986951079374690776932
788
$M_i = C_i^d \bmod N$
M_1 = 35683074077819515836553452823777713
92000653945474793199514123821395068089
77521708715289465540712312619289853877
84654534372777083272886432690012943447
24204382547145737739832262535472379114
69689279654840180781099528349504285631
48427549432598367832506557082673652201
37879515643769831019598695107937469077
6932788^{65537} mod 12903233019835565308832
30562089101277737687129324301319646618
66111927147101671790196272475752146146
68881408785574978816195330371488293849
58708364580758532425259014621034226032
34418387460185193519655718697392418865
98829537993909754059132680338060392001
95676485298109463260837390307143045745
21839041394920216433
= > 9

Algoritma CC:
> 9 melakukan proses *decrypt* menggunakan algoritma *Caesar Chiper* = 50

Algoritma RSA:
Berdasarkan hasil *encrypt* RSA yaitu:
Ciphertext (nilai huruf): 623378384382886590
62290161406757112542676501178769066385
20512515779567775235514932622777499734
11217287404207471851807295466058396962
11205730522002091513062248622307194897
63392048944773776399781607097362522707
34703174108941140470949277716882427492
86242744614253497960151109430640993873
37042181289502685796 3509
$M_i = C_i^d \bmod N$
M_1 = 623378384382886590622901614067571
12542676501178769066385205125157795677
75235514932622777499734112172874042074
71851807295466058396962112057305220020
91513062248622307194897633920489447737
76399781607097362522707347031741089411
40470949277716882427492862427446142534
97960151109430640993873370421812895026
857963509^{65537} mod 12903233019835565308832
30562089101277737687129324301319646618
66111927147101671790196272475752146146
68881408785574978816195330371488293849
58708364580758532425259014621034226032
34418387460185193519655718697392418865
98829537993909754059132680338060392001
95676485298109463260837390307143045745
21839041394920216433
M_1 = K

Algoritma CC:
K melakukan proses *decrypt* menggunakan algoritma *Caesar Chiper* = B

3. HASIL DAN PEMBAHASAN

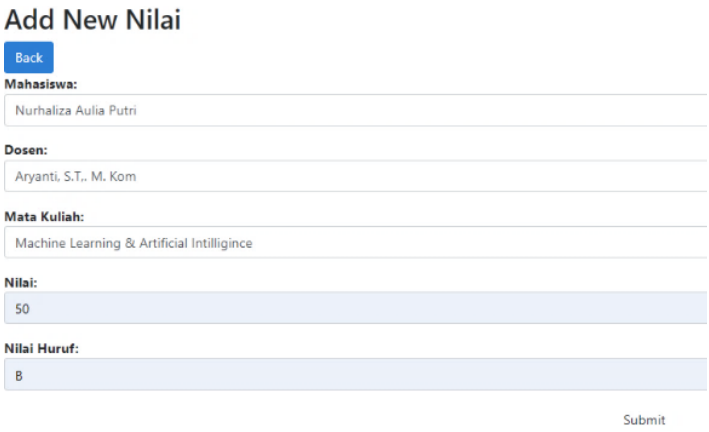
3.1 Deskripsi Data

Penelitian ini menunjukkan bahwa dengan menggunakan kombinasi algoritma *Caesar Cipher* dan RSA secara efektif meningkatkan keamanan data nilai siswa dalam sistem informasi berbasis *web*. *Caesar Cipher* digunakan untuk mengenkripsi nilai siswa dengan menggunakan pendekatan yang sederhana namun efektif, sementara RSA digunakan untuk mengamankan pertukaran kunci dan proses enkripsi yang lebih kompleks. Temuan ini menggambarkan bahwa pendekatan gabungan ini dapat melindungi data sensitif dari akses yang tidak sah dan gangguan, sehingga meningkatkan integritas informasi Pendidikan. Data yang di enkripsi berupa data nilai dan nilai huruf. *Plaintext* yang digunakan yaitu berupa data nilai = 50 dan data nilai huruf = B.

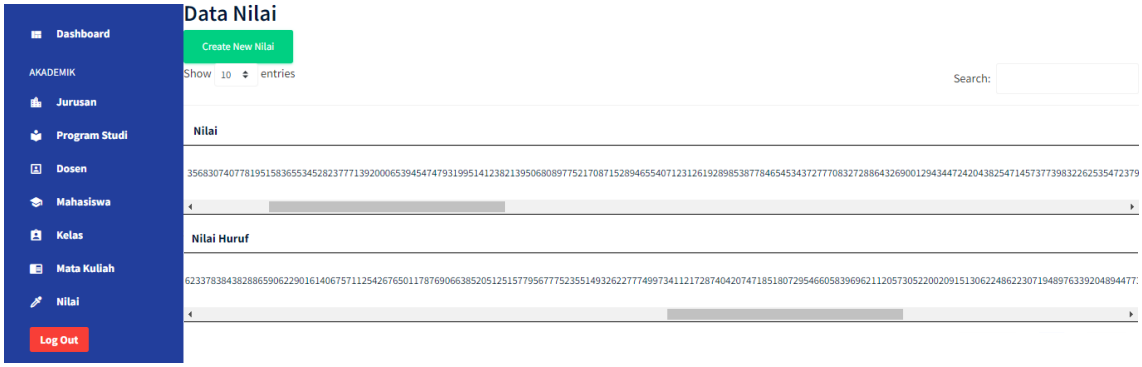
3.2 Pengujian Implementasi Algoritma

Penelitian ini menggunakan kunci secara acak, yang artinya setiap pengguna mendapatkan pasangan *public key* dan *private key* yang unik, untuk memastikan bahwa proses *encrypt* dan *decrypt* dilakukan dengan keamanan yang tinggi. Dengan menggunakan kombinasi *Caesar Cipher* dan RSA, Keamanan data pada level pengguna dalam *database* ditingkatkan, melindungi informasi sensitif dari akses yang tidak sah dan penggunaan yang tidak sah. Gambar 8 merupakan tampilan dari *database* yang berisi kunci yang digunakan pada proses *encrypt* dan *decrypt*.

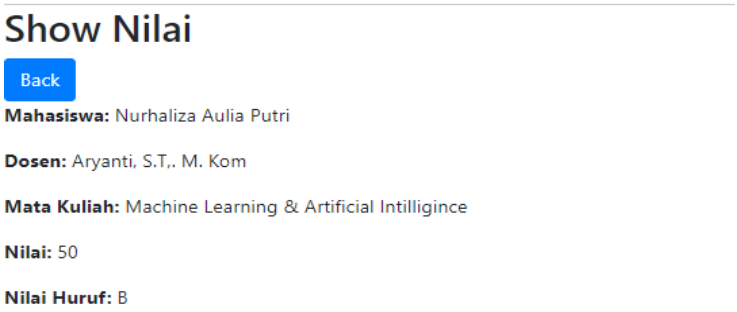
Gambar 4: *Interface* Sistem



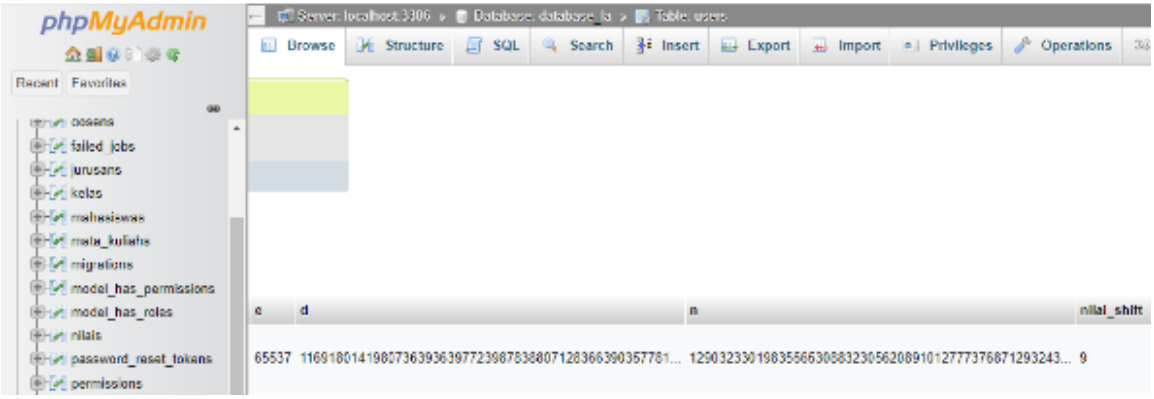
Gambar 5: Tampilan *Form Encrypt*



Gambar 6: Tampilan Daftar *Encrypt*



Gambar 7: Tampilan Data Berhasil di *Decrypt*



Gambar 8: Tampilan *Database*

4. KESIMPULAN

Penelitian ini menunjukkan bahwa penggunaan kombinasi algoritma Caesar Cipher dan RSA dapat efektif meningkatkan keamanan data nilai mahasiswa dalam sistem informasi berbasis *web*. *Caesar Cipher* digunakan untuk mengenkripsi nilai mahasiswa dengan pendekatan sederhana namun efektif, sementara RSA digunakan untuk mengamankan proses pertukaran kunci dan enkripsi yang lebih kompleks. Hasilnya menunjukkan bahwa kombinasi kedua algoritma ini dapat melindungi data sensitif dari pihak yang tidak berwenang mengaksesnya dan memalsukan, serta meningkatkan integritas informasi pendidikan.

Berdasarkan hasil penelitian ini, beberapa saran untuk pengembangan lebih lanjut sebagai berikut:

1. Melakukan penelitian lebih lanjut untuk mengoptimalkan penggunaan algoritma kriptografi yang lebih canggih dan efisien dalam konteks keamanan data nilai mahasiswa untuk keamanan yang lebih tinggi.
2. Mengimplementasikan manajemen kunci yang lebih terstruktur dan aman untuk RSA guna memastikan keamanan dan keabsahan pertukaran data yang lebih baik.
3. Melakukan pengujian penetrasi dan audit keamanan secara berkala untuk mengevaluasi potensi kerentanan baru dan memastikan sistem tetap aman dari serangan siber.
4. Integrasi teknologi keamanan baru yang relevan dengan perkembangan teknologi informasi, seperti blockchain untuk mengamankan integritas data secara lebih lanjut.

Dengan menerapkan saran-saran ini, diharapkan sistem keamanan data nilai mahasiswa berbasis web dapat terus ditingkatkan dalam menghadapi tantangan keamanan informasi yang semakin kompleks di era digital saat ini.

PERNYATAAN PENGHARGAAN

Ucapan terima kasih saya sampaikan kepada semua pihak yang telah memberi penulis

dukungan dan bantuan dalam penelitian ini. Terima kasih atas bimbingan, kontribusi, dan dorongan yang sangat berarti bagi kesuksesan penelitian ini. Dukungan tersebut telah membantu saya mengatasi setiap tantangan dan mencapai hasil yang memuaskan.

DAFTAR PUSTAKA

[1] R. N. Nizatsary, H. B. Seta, and B. T. Wahyono, "Penerapan Keamanan Data Siswa Menggunakan International Data Encryption Algorithm (IDEA) dan Rivest Shamir Adleman (RSA)".

[2] U. Potensi Utama Jl KLYos, "RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID Yusfrizal 1)," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, 2019.

[3] P. Aplikasi, P. Pesan, D. Algoritma, C. C. Oleh, R. Rio, and A. Gurning, "PERANCANGAN APLIKASI PENGAMANAN PESAN DENGAN ALGORITMA CAESAR CHIPER," *Pelita Inform. Budi Darma*, p. 3, 2014, [Online]. Available: www.stmik-budidarma.ac.id//

[4] R. Pratiwi, L. C. Utami, and R. B. Sakti, "Bulletin of Information Technology (BIT) Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher," vol. 3, no. 4, pp. 367–373, 2022, doi: 10.47065/bit.v3i1.

[5] A. Nidya Agustina *et al.*, "PENGAMANAN DOKUMEN MENGGUNAKAN METODE RSA (RIVEST SHAMIR ADLEMAN)BERBASIS WEB."

[6] M. Aziz and F. Rachman, "PERANCANGAN APLIKASI MEMO MENGGUNAKAN ALGORITMA KRIPTOGRAFI CAESAR CIPHER DAN RSA BERBASIS ANDROID," 2018.

[7] M. W. A. Saputra, S. A. Ashari, and E. Larosa, "Keamanan Data Sistem Informasi Akademik ITEkes Mahardika: Penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES," *Invert. J. Inf. Technol. Educ.*, vol. 4, no. 2, pp. 79–85, 2024, doi: 10.37905/inverted.v4i2.22969.

[8] A. B. Nasution, "IMPLEMENTASI PENGAMANAN DATA DENGAN MENGGUNAKAN ALGORITMA CAESAR CIPHER DAN TRANSPOSISI CIPHER," *J. Teknol. Inf.*, vol. 3, no. 1, 2019.

[9] A. Aryanti and I. Mekongga, "Implementation of Rivest Shamir Adleman Algorithm (RSA) and Vigenere Cipher in Web Based Information System," in *E3S Web of Conferences*, EDP Sciences, Feb. 2018. doi: 10.1051/e3sconf/20183110007.

[10] S. B. Dar, "Enhancing The Security of Caesar Cipher Using Double Substitution Method." [Online]. Available: http://practicalcryptography.com/ciphers/caesar-cipher/.