



**PENERAPAN KEAMANAN DATA SISWA MENGGUNAKAN  
*INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) DAN  
RIVEST SHAMIR ADLEMAN (RSA)***

**SKRIPSI**

**RAINA NABILA NIZATSARY**

**1810511062**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA  
PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
2022**



**PENERAPAN KEAMANAN DATA SISWA MENGGUNAKAN  
*INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) DAN  
RIVEST SHAMIR ADLEMAN (RSA)***

**SKRIPSI**

**Diajukan Sebagai Syarat untuk Memperoleh Gelar Sarjana Komputer**

**RAINA NABILA NIZATSARY**

**1810511062**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA  
PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER**

**2022**

## PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Raina Nabila Nizatsary

NIM : 1810511062

Tanggal : 27 Juli 2022

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai ketentuan yang berlaku.

Jakarta, 27 Juli 2022

Yang Menyatakan,



MATERAI  
TEMPEL  
9E4A1X91027125

(Raina Nabila Nizatsary)

**PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK  
KEPENTINGAN AKADEMIS**

Sebagai civitas akademika Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Raina Nabila Nizatsary

NIM : 1810511062

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non Eksklusif (Non-Exclusive Royalty Free Right) atas karya ilmiah saya yang berjudul:

**PENERAPAN KEAMANAN DATA SISWA MENGGUNAKAN  
INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) DAN RIVEST  
SHAMIR ADLEMAN (RSA)**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 27 Juli 2022

Yang Menyatakan,



(Raina Nabila Nizatsary)

## Lembar Pengesahan

Dengan ini dinyatakan bahwa Skripsi berikut :

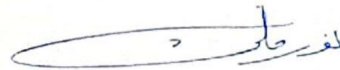
Nama : Raina Nabila Nizatsary  
NIM : 181051062  
Program Studi : Informatika  
Judul Skripsi : Penerapan Keamanan Data Siswa Menggunakan International Data Encryption Algorithm (IDEA) dan Rivest Shamir Adleman (RSA)

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Bayu Hananto, S.Kom., M.Kom.

Penguji I



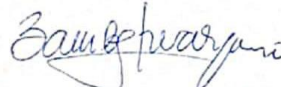
Noor Falih, S.Kom., M.T.

Penguji II



Henki Bayu Seta, S.Kom., MTI.

Dosen Pembimbing I



Bambang Tri Wahyono, S.Kom., M.Si.

Dosen Pembimbing II



Desta Sandya Prasvita, M.Kom

Ketua Program Studi

Ditetapkan di : Jakarta  
Tanggal Pengesahan : 18 Juli 2022



# **PENERAPAN KEAMANAN DATA SISWA MENGGUNAKAN INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) DAN RIVEST SHAMIR ADLEMAN (RSA)**

**Raina Nabila Nizatsary**

## **Abstrak**

Sebuah data untuk suatu instansi atau sebuah sekolah harus dikelola dengan baik dan harus terjamin suatu keamanannya. Penelitian ini dilakukan untuk menambah keamanan pada data siswa. Penelitian ini dilakukan dengan menggunakan metode dari kriptografi simetris dan asimetris yaitu *International Data Encryption Algorithm* (IDEA) dan *Rivest Shamir Adleman* (RSA). Proses keamanan data menggunakan metode tersebut dilakukan dengan mengamankan terlebih dahulu data siswa menggunakan algoritma kriptografi simetris yaitu *International Data Encryption Algorithm* (IDEA), kemudian proses keamanan data selanjutnya mengamankan kunci dari algoritma kriptografi simetris yaitu *International Data Encryption Algorithm* (IDEA) menggunakan algoritma kriptografi asimetris *Rivest Shamir Adleman* (RSA). Pada penelitian ini menghasilkan suatu *hybrid cryptosystem* pada suatu data siswa yang dimana dapat mengamankan suatu data dengan baik.

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

# **PENERAPAN KEAMANAN DATA SISWA MENGGUNAKAN INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) DAN RIVEST SHAMIR ADLEMAN (RSA)**

**Raina Nabila Nizatsary**

## *Abstact*

A data for an agency or a school must be managed properly and its security must be guaranteed. This research was conducted to increase the security of student data. This research was conducted using symmetric and asymmetric cryptographic methods, namely the International Data Encryption Algorithm (IDEA) and Rivest Shamir Adleman (RSA). The data security process using this method is carried out by first securing student data using a symmetric cryptographic algorithm, namely the International Data Encryption Algorithm (IDEA), then the next data security process secures the key from a symmetric cryptographic algorithm, namely the International Data Encryption Algorithm (IDEA) using the Rivest asymmetric cryptography algorithm. Shamir Adleman (RSA). In this study resulted in a hybrid cryptosystem on a student data which can secure a data well.

**Keywords:** Data, Data Security, IDEA, RSA

## KATA PENGANTAR

Puji syukur ke hadirat Allah SWT atas segala limpahan Rahmat dan Karunia-Nya, serta Shalawat beserta salam kepada Nabi Muhammad SAW sehingga penulis dapat menyelesaikan skripsi ini dengan judul “Penerapan Keamanan Data Siswa Menggunakan International Data Encryption Algorithm (IDEA) Dan Rivest Shamir Adleman (RSA)” yang mana ditunjukkan sebagai salah satu syarat untuk menyelesaikan studi agar memperoleh gelar Sarjana Pendidikan Strata Satu pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.

Dalam penyusunan dan penulisan skripsi ini tak lepas dari bantuan, dukungan, serta doa dari berbagai pihak. Oleh karena itu, dalam kesempatan kali ini penulis senantiasa menyampaikan rasa terima kasih yang sebesar-besarnya kepada pihak yang sudah membantu dalam penyusunan skripsi ini terutama kepada:

1. Umi, papa, dan adik saya atas semua doa-doanya, perhatian, semangat serta dukungan yang selalu diberikan kepada saya dalam menyelesaikan skripsi ini sampai selesai.
2. Bapak Henki Bayu Seta, S.Kom., MTI. selaku dosen pembimbing 1 dan Bambang Tri Wahyono, S.Kom., M.Si. selaku dosen pembimbing 2 yang telah bersedia dalam meluangkan waktu untuk memberikan bimbingan, masukan, kritik, saran, serta dukungan selama penelitian dan penulisan skripsi saya.
3. Bapak Desta Sandya Prasvita, M.Kom. selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
4. Seluruh dosen Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta yang telah mendidik dan memberikan ilmu yang bermanfaat kepada penulis.
5. Kepada Kucing Peliharaan saya Odi, yang telah menemani saya sepanjang waktu untuk menyelesaikan skripsi ini hingga selesai.
6. Teman-teman seperjuangan Informatika 2018 yang tidak bisa disebutkan satu persatu, yang telah memberikan dukungan serta berjuang untuk bisa lulus tepat waktu.

Semoga Allah SWT memberikan balasan yang berlipat ganda kepada kita semua. Penulis menyadari bahwa skripsi ini belum sempurna, baik dari segi materi maupun penyajiannya. Oleh



karena itu, saran dan kritik yang membangun sangat diharapkan dalam penyempurnaan skripsi ini. Akhir kata, semoga skripsi ini dapat bermanfaat dan menambah wawasan bagi para pembacanya.

Jakarta, 24 Juni 2022

Penulis,

A handwritten signature in black ink, consisting of several loops and a long horizontal stroke extending to the right.

Raina Nabila Nizatsary

## DAFTAR ISI

|   |             |
|---|-------------|
| <b>PERNYATAAN ORISINALITAS .....</b>  | <b>iii</b>  |
| <b>PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK<br/>KEPENTINGAN AKADEMIS.....</b> | <b>iv</b>   |
| <b>Lembar Pengesahan.....</b>   | <b>v</b>    |
| <b>Abstrak.....</b>   | <b>vi</b>   |
| <i>Abstact .....</i>  | <i>vii</i>  |
| <b>KATA PENGANTAR.....</b>  | <b>viii</b> |
| <b>DAFTAR ISI.....</b>  | <b>x</b>    |
| <b>DAFTAR GAMBAR.....</b>   | <b>xiv</b>  |
| <b>DAFTAR TABEL .....</b>   | <b>xvi</b>  |
| <b>BAB I PENDAHULUAN.....</b>   | <b>1</b>    |
| <b>1.1.Latar Belakang .....</b>   | <b>1</b>    |
| <b>1.2.Rumusan Masalah.....</b>   | <b>2</b>    |
| <b>1.3.Batasan Penelitian .....</b>   | <b>3</b>    |
| <b>1.4.Tujuan Peneltian .....</b>   | <b>3</b>    |
| <b>1.5 Manfaat Penelitian .....</b>   | <b>4</b>    |
| <b>1.6.Luaran yang Diharapkan .....</b>   | <b>4</b>    |
| <b>1.7.Sistematika Penulisan .....</b>  | <b>4</b>    |
| <b>BAB II LANDASAN TEORI.....</b>   | <b>6</b>    |
| <b>2.1 Keamanan Data .....</b>  | <b>6</b>    |
| <b>2.1.1 Pengertian Keamanan Data.....</b>  | <b>6</b>    |
| <b>2.1.2 Ancaman Keamanan Data .....</b>  | <b>7</b>    |
| <b>2.2 Kriptografi.....</b>   | <b>8</b>    |
| <b>2.2.1 Pengertian Kriptografi.....</b>  | <b>8</b>    |
| <b>2.2.2 Algoritma Kriptografi.....</b>   | <b>9</b>    |
| <b>2.2.3 Kriptografi kunci simetris .....</b>   | <b>10</b>   |

|  |    |
|--|----|
| 2.2.4 Kriptografi kunci asimetris .....                          | 10 |
| 2.3 Plainteks .....  | 11 |
| 2.4 Chiperteks .....   | 11 |
| 2.5 <i>International Data Encryption Algorithm (IDEA)</i> .....  | 11 |
| 2.5.1 Pembentukan Kunci IDEA .....                               | 12 |
| 2.5.2 Enkripsi IDEA .....  | 13 |
| 2.5.3 Dekripsi IDEA .....  | 15 |
| 2.6 <i>Rivest Shamir Adleman (RSA)</i> .....                     | 16 |
| 2.6.1 Pembentukan Kunci <i>Rivest Shamir Adleman (RSA)</i> ..... | 17 |
| 2.6.2 Enkripsi <i>Rivest Shamir Adleman (RSA)</i> .....          | 17 |
| 2.6.3 Dekripsi Kunci <i>Rivest Shamir Adleman (RSA)</i> .....    | 17 |
| 2.7 Pengujian <i>Black Box</i> .....                             | 18 |
| 2.8 Pengujian Wireshark .....                                    | 18 |
| 2.9 Penelitian Terkait .....                                     | 18 |
| <b>BAB III METODOLOGI PENELITIAN</b> .....                       | 24 |
| 3.1 Tahapan Penelitian .....                                     | 24 |
| 3.1.1 Identifikasi Masalah .....                                 | 25 |
| 3.1.2 Studi Literatur .....                                      | 25 |
| 3.1.3 Analisis Perancangan Perangkat Lunak .....                 | 25 |
| 3.1.4 Perancangan Perangkat Lunak .....                          | 26 |
| 3.1.5 Implementasi Perangkat lunak .....                         | 31 |
| 3.1.6 Pengujian .....  | 32 |
| 3.1.7 Analisis Hasil .....                                       | 32 |
| 3.1.8 Kesimpulan .....   | 32 |
| 3.1.8 Dokumentasi .....  | 33 |
| 3.2 Alat Bantu Penelitian .....                                  | 33 |
| 3.3 Jadwal Penelitian .....                                      | 33 |
| <b>BAB IV HASIL DAN PEMBAHASAN</b> .....                         | 36 |
| 4.1 Data .....   | 36 |

|  |  |            |
|--|--|------------|
| 4.2                                    | Kebutuhan Perancangan Perangkat .....                                      | 36         |
| 4.3                                    | Analisis Perancangan Proses Enkripsi dan Dekripsi Perangkat Lunak.....     | 37         |
| 4.3.1                                  | Analisis Perancangan Cara Kerja Proses Enkripsi.....                       | 37         |
| 4.3.2                                  | Analisis Perancangan Cara Kerja Proses Dekripsi.....                       | 41         |
| 4.3.3                                  | Analisis Proses Pembangkitan Kunci IDEA dan RSA.....                       | 43         |
| 4.3.4                                  | Analisis Proses Perhitungan Enkripsi Algoritma IDEA dan RSA .....          | 53         |
| 4.3.5                                  | Analisis Proses Perhitungan Dekripsi Algoritma IDEA dan RSA.....           | 137        |
| 4.4                                    | Perancangan Perangkat Lunak Enkripsi dan Dekripsi IDEA dan RSA.....        | 221        |
| 4.4.1                                  | Flowchart Enkripsi dan Dekripsi.....                                       | 222        |
| 4.4.2                                  | Use Case Enkripsi dan Dekripsi .....                                       | 227        |
| 4.5                                    | Implementasi Enkripsi dan Dekripsi IDEA dan RSA .....                      | 229        |
| 4.5.1                                  | Implementasi Proses Enkripsi .....   | 229        |
| 4.5.2                                  | Implementasi Proses Dekripsi .....   | 231        |
| 4.6                                    | Pengujian.....   | 232        |
| 4.6.1                                  | Pengujian Fungsionalitas Perangkat Lunak Menggunakan <i>BlackBox</i> ..... | 232        |
| 4.6.2                                  | Pengujian Waktu Proses .....   | 235        |
| 4.6.3                                  | Pengujian menggunakan Wireshark .....                                      | 236        |
| 4.7                                    | Analisis Hasil Luaran Perangkat Lunak .....                                | 240        |
| <b>BAB V KESIMPULAN DAN SARAN.....</b> |  | <b>245</b> |
| 5.1                                    | Kesimpulan .....   | 245        |
| 5.2                                    | Saran.....   | 247        |
| <b>DAFTAR PUSTAKA.....</b>             |  | <b>248</b> |
| <b>DAFTAR RIWAYAT HIDUP .....</b>      |  | <b>252</b> |
| <b>LAMPIRAN.....</b>                   |  | <b>253</b> |
| <b>LAMPIRAN 1 .....</b>                |  | <b>253</b> |
| <b>LAMPIRAN 2.....</b>                 |  | <b>255</b> |
| <b>LAMPIRAN 3.....</b>                 |  | <b>257</b> |
| <b>LAMPIRAN 4.....</b>                 |  | <b>259</b> |
| <b>LAMPIRAN 5.....</b>                 |  | <b>261</b> |

|                          |     |
|--------------------------|-----|
| <b>LAMPIRAN 6</b> .....  | 264 |
| <b>LAMPIRAN 7</b> .....  | 292 |
| <b>LAMPIRAN 8</b> .....  | 298 |
| <b>LAMPIRAN 9</b> .....  | 302 |
| <b>LAMPIRAN 10</b> ..... | 307 |
| <b>LAMPIRAN 11</b> ..... | 310 |
| <b>LAMPIRAN 12</b> ..... | 311 |

## DAFTAR GAMBAR

|   |           |
|---|-----------|
| <b>Gambar 2. 1 Proses Enkripsi/Dekripsi Sederhana .....</b>     | <b>9</b>  |
| <b>Gambar 2. 2 Diagram Pembagian Algoritma Kriptografi.....</b> | <b>10</b> |
| <b>Gambar 2. 3 Skema Enkripsi IDEA.....</b>                     | <b>13</b> |
| <b>Gambar 2. 4 Skema Dekripsi IDEA.....</b>                     | <b>15</b> |
| <b>Gambar 3. 1 Diagram Tahapan Penelitian.....</b>              | <b>24</b> |
| <b>Gambar 3. 2 Spesifik Proses Enkripsi.....</b>                | <b>26</b> |
| <b>Gambar 3. 3 Diagram Proses Enkripsi IDEA .....</b>           | <b>27</b> |
| <b>Gambar 3. 4 Diagram Proses Enkripsi RSA .....</b>            | <b>28</b> |
| <b>Gambar 3. 5 Spesifik Proses Dekripsi.....</b>                | <b>29</b> |
| <b>Gambar 3. 6 Diagram Dekripsi IDEA .....</b>                  | <b>30</b> |
| <b>Gambar 3. 7 Diagram Dekripsi RSA .....</b>                   | <b>31</b> |
| <b>Gambar 4. 1 Flowchart Cara Kerja Enkripsi.....</b>           | <b>38</b> |
| <b>Gambar 4. 2 Diagram Cara Kerja Enkripsi IDEA .....</b>       | <b>40</b> |
| <b>Gambar 4. 3 Flowchart Cara Kerja Dekripsi .....</b>          | <b>41</b> |

|   |            |
|---|------------|
| <b>Gambar 4. 4 Diagram Cara Kerja Dekripsi IDEA.....</b>              | <b>42</b>  |
| <b>Gambar 4. 5 Flowchart Perancangan Enrkripsi dan Dekripsi .....</b> | <b>222</b> |
| <b>Gambar 4. 6 Flowchart Perancangan Enkripsi .....</b>               | <b>223</b> |
| <b>Gambar 4. 7 Flowchart Perancangan Proses Dekripsi .....</b>        | <b>226</b> |
| <b>Gambap 4. 8 Use Case Diagram .....</b>                             | <b>228</b> |
| <b>Gambar 4. 9 Implementasi Proses Enkripsi.....</b>                  | <b>230</b> |
| <b>Gambar 4. 10 Implementasi Enkripsi Berhasil.....</b>               | <b>230</b> |
| <b>Gambar 4. 11 Implementasi Proses Dekripsi .....</b>                | <b>231</b> |
| <b>Gambar 4. 12 Hasil Dekripsi.....</b>                               | <b>232</b> |
| <b>Gambar 4. 13 Hasil Pengujian Wireshark tanpa RSA.....</b>          | <b>237</b> |
| <b>Gambar 4. 14 Hasil Pengujian Wireshark dengan RSA .....</b>        | <b>238</b> |

## DAFTAR TABEL

|   |     |
|---|-----|
| <b>Tabel 2. 1 Penelitian Terkait</b> .....  | 20  |
| <b>Tabel 3. 1 Jadwal Penelitian</b> .....   | 34  |
| <b>Tabel 4. 1 Konversi Kunci IDEA</b> ..... | 44  |
| <b>Tabel 4. 2 Konversi Plaintext</b> .....  | 53  |
| <b>Tabel 4. 3 Hasil Enkripsi 1</b> .....    | 75  |
| <b>Tabel 4. 4 Hasil Enkripsi 2</b> .....    | 94  |
| <b>Tabel 4. 5 Hasil Enkripsi 3</b> .....    | 113 |
| <b>Tabel 4. 6 Hasil Enkripsi 4</b> .....    | 133 |
| <b>Tabel 4. 7 Enkripsi Key</b> .....        | 135 |
| <b>Tabel 4. 8 Dekripsi Key</b> .....        | 138 |
| <b>Tabel 4. 9 Konversi Ciphertext</b> ..... | 140 |
| <b>Tabel 4. 10 Hasil Dekripsi 1</b> .....   | 161 |
| <b>Tabel 4. 11 Hasil Dekripsi 2</b> .....   | 181 |
| <b>Tabel 4. 12 Hasil Dekripsi 3</b> .....   | 200 |
| <b>Tabel 4. 13 Hasil Dekripsi 4</b> .....   | 220 |



|   |            |
|---|------------|
| <b>Tabel 4. 14 Hasil Pengujian Black Box .....</b>      | <b>233</b> |
| <b>Tabel 4. 15 Hasil Pengujian Waktu Enkripsi.....</b>  | <b>235</b> |
| <b>Tabel 4. 16 Hasil Pengujian Waktu Dekripsi .....</b> | <b>236</b> |
| <b>Tabel 4. 17 Hasil Wireshark .....</b>                | <b>238</b> |