P-ISSN : 2580-4316
E-ISSN : 2654-8054
https://doi.org/10.37817/ikraith-informatika.v11i2

# Perangkat Lunak Pembelajaran Enkripsi Identity-Based Encryption (IBE)

Yamina Hulu[1] , Swingly Purba[2] , Melva E Pangaribuan[3]
Program Studi Teknik Informatika
Institut Sains dan Teknologi T.D. Pardede, Medan
*E-mail:* yaminahuulu@gmail.com[1] , swingly.purba61@gmail.com[2] , melpangrib@gmail.com[3]

**ABSTRAK**

Identity-Based Encryption (IBE) merupakan teknik kriptografi kunci publik yang menggunakan identitas pengguna sebagai dasar kunci publik sehingga tidak bergantung pada sertifikat seperti pada mekanisme kunci publik konvensional. Penelitian ini merancang dan mengimplementasikan perangkat lunak pembelajaran IBE yang menampilkan proses pembentukan kunci, enkripsi, dan dekripsi secara bertahap. Perangkat lunak dibangun menggunakan Microsoft Visual Basic .NET dengan dukungan SHA-1 dan menyediakan dua model komunikasi, yaitu dua pengguna dan tiga pengguna. Identitas tujuan dapat berupa e-mail, nomor telepon, phone number, address, atau ID card number sesuai batasan sistem. Hasil implementasi menunjukkan bahwa perangkat lunak dapat memvisualisasikan tahapan Setup dan Extract pada pembentukan kunci, kemudian proses enkripsi dan dekripsi, menampilkan setiap langkah perhitungan, mengatur kecepatan visualisasi, serta menyimpan hasil proses dalam berkas teks. Skenario contoh dengan pesan "ISTP" menunjukkan bahwa pesan dapat dikembalikan ke bentuk plaintext setelah proses dekripsi. Dengan demikian, perangkat lunak dapat digunakan sebagai alat bantu untuk memahami alur kerja IBE secara lebih terstruktur.

**Kata kunci:** *Identity-Based Encryption, kriptografi, pembentukan kunci, enkripsi, dekripsi, SHA-1*

**ABSTRACT**

Identity-Based Encryption (IBE) is a public-key cryptographic technique that uses a user identity as the basis of a public key, reducing dependence on certificates used in conventional public-key mechanisms. This study designs and implements an IBE learning software that visualizes key generation, encryption, and decryption step by step. The software is developed using Microsoft Visual Basic .NET with SHA-1 support and provides two communication models: two-user and three-user communication. The destination identity can be represented by an e-mail, mobile number, phone number, address, or identity card number according to the system requirements. The implementation shows that the software can visualize the Setup and Extract stages of key generation, followed by encryption and decryption, display each computational step, control visualization speed, and save process results as text files. The example scenario using the message "ISTP" demonstrates that the original plaintext can be recovered after decryption. Therefore, the software provides a structured learning aid for understanding the operational flow of IBE.

**Keywords:** *Identity-Based Encryption, cryptography, key generation, encryption, decryption, SHA-1*

## 1. PENDAHULUAN

Perlindungan informasi digital membutuhkan mekanisme yang dapat menjaga kerahasiaan data sekaligus memungkinkan pengguna yang berhak memperoleh kembali informasi tersebut. Kriptografi menyediakan pendekatan matematis untuk mengubah plaintext menjadi ciphertext melalui proses enkripsi dan mengembalikannya melalui dekripsi. Pada kriptografi kunci publik, kebutuhan pengelolaan kunci dapat menjadi lebih kompleks karena kunci publik harus dikaitkan dengan identitas pemiliknya. Skripsi yang menjadi dasar artikel ini mengangkat Identity-Based Encryption (IBE) sebagai pendekatan yang memungkinkan suatu identitas yang telah diketahui, seperti alamat e-mail atau nomor telepon, digunakan sebagai public key. Dengan pendekatan tersebut, proses komunikasi dapat dilakukan tanpa terlebih dahulu mencari sertifikat public key penerima.

IBE diperkenalkan oleh Adi Shamir pada tahun 1984 untuk mengatasi persoalan autentikasi kunci publik. Pada sistem ini, public key ditentukan dari identitas pengguna, sedangkan private key dibangkitkan oleh Private Key Generator (PKG) menggunakan master key. Skripsi menjelaskan bahwa konsep tersebut kemudian berkembang, antara lain melalui teknik Boneh-Franklin yang memanfaatkan bilinear pairing. Keunggulan IBE yang menjadi dasar pengembangan perangkat lunak adalah kesederhanaannya dalam menggunakan identitas sebagai public key, sedangkan salah satu persoalan yang tetap harus diperhatikan adalah distribusi private key dari PKG melalui kanal yang aman.

Permasalahan penelitian dirumuskan menjadi dua hal, yaitu bagaimana menampilkan proses pembentukan kunci,

P-ISSN : 2580-4316
E-ISSN : 2654-8054 https://doi.org/10.37817/ikraith-informatika.v11i2

enkripsi, dan dekripsi pada IBE serta bagaimana mempermudah pembelajaran IBE. Tujuan perancangan adalah menghasilkan perangkat lunak yang dapat membantu pembelajaran kriptosistem IBE dan memberikan gambaran cara kerja setiap tahap. Perangkat lunak dibatasi pada plaintext maksimum 48 karakter, beberapa jenis identitas dengan aturan format tertentu, penyimpanan hasil dalam berkas .txt, dua model pengguna dan tiga pengguna, serta tiga tahap utama berupa pembentukan kunci, enkripsi, dan dekripsi.

## 2. LANDASAN TEORI

### 2.1 Kriptografi dan kriptografi kunci publik

Kriptografi merupakan bidang yang mempelajari teknik untuk menjaga informasi agar tidak dapat dibaca oleh pihak yang tidak berhak. Skripsi membahas empat tujuan utama, yaitu kerahasiaan, integritas data, autentikasi, dan non-repudiation. Algoritma kriptografi menggunakan kunci sebagai bagian penting dari keamanan. Berdasarkan bentuk kunci, kriptografi modern dibedakan menjadi kriptografi simetris dan asimetris. Pada kriptografi simetris, kunci enkripsi dan dekripsi sama, sedangkan pada kriptografi asimetris digunakan pasangan public key dan private key.

Pada mekanisme kunci publik, pengirim dapat mengenkripsi pesan menggunakan public key penerima, sementara proses dekripsi dilakukan menggunakan private key. Skripsi mencatat bahwa pendekatan ini membantu mengatasi persoalan distribusi kunci simetris, tetapi mempunyai konsekuensi berupa komputasi yang relatif lebih kompleks. IBE mengambil konsep kunci publik tersebut lebih lanjut dengan menggunakan identitas pengguna sebagai dasar public key.

### 2.2 Identity-Based Encryption

Secara umum, IBE melibatkan Public Key Generator atau Private Key Generator (PKG), master key, parameter sistem, identitas pengguna, public key berbasis identitas, dan private key. Skripsi membagi proses IBE menjadi tiga tahap utama, yaitu pembentukan kunci, enkripsi, dan dekripsi. Pembentukan kunci terdiri atas Setup dan Extract. Pada Setup, PKG membangkitkan parameter sistem dan master key. Pada Extract, identitas pengguna diproses untuk menghasilkan private key. Tahap enkripsi menggunakan parameter sistem, identitas penerima, pesan, dan bilangan acak, sedangkan dekripsi menggunakan ciphertext, identitas, dan private key penerima.

### 2.3 SHA-1 dan landasan matematis

Perangkat lunak juga menyediakan materi pendukung SHA-1. Dalam skripsi, SHA-1 dijelaskan sebagai algoritma hash yang menghasilkan message digest 160 bit dan digunakan dalam pemrosesan identitas pada tahapan IBE yang diimplementasikan. Landasan matematis yang digunakan mencakup Greatest Common Divisor, bilangan prima, grup, randomize, kurva elips, serta operasi modular. Konsep-konsep tersebut mendukung penjelasan perhitungan pada proses pembentukan kunci dan enkripsi.

### 2.4 Tahapan IBE dalam perangkat lunak

Tahap pembentukan kunci menjadi bagian penting karena private key tidak dibuat langsung oleh pengguna. Pada Setup, PKG menghasilkan nilai yang menjadi parameter sistem dan master key. Parameter tersebut kemudian digunakan pada tahap Extract untuk memproses identitas penerima. Dalam perangkat lunak, proses ini tidak disembunyikan di balik satu tombol yang hanya menghasilkan keluaran akhir. Sebaliknya, sistem menampilkan perhitungan antara sehingga pengguna dapat melihat hubungan antara identitas, fungsi hash, parameter sistem, dan private key. Pendekatan visualisasi tersebut sesuai dengan tujuan perangkat lunak sebagai media pembelajaran.

Tahap enkripsi menggunakan identitas penerima sebagai dasar pembentukan komponen yang berhubungan dengan ciphertext. Pesan yang dimasukkan pengguna terlebih dahulu diubah ke bentuk yang dapat diproses oleh algoritma. Bilangan acak r digunakan pada perhitungan komponen U, sedangkan komponen V dibentuk dengan operasi XOR antara plaintext dan hasil hash H2. Hasil akhir kedua komponen digabungkan menjadi ciphertext. Pada tahap dekripsi, penerima menggunakan private key dan ciphertext untuk membentuk kembali nilai H2 yang sesuai. Operasi XOR selanjutnya memulihkan plaintext. Urutan tersebut memberikan gambaran sebab-akibat antara setiap tahap proses.

P-ISSN : 2580-4316
E-ISSN : 2654-8054
https://doi.org/10.37817/ikraith-informatika.v11i2

**2.5 Model komunikasi dua dan tiga pengguna**

Model dua pengguna merupakan bentuk paling sederhana yang digunakan perangkat lunak. Alice berperan sebagai pengirim dan Bob sebagai penerima. Pembentukan private key dilakukan untuk Bob, kemudian Alice melakukan enkripsi menggunakan identitas Bob. Setelah ciphertext diterima, Bob melakukan dekripsi menggunakan private key yang diperoleh dari PKG. Model ini digunakan untuk memperlihatkan alur dasar dari pembentukan kunci sampai pemulihan pesan.

Model tiga pengguna memperluas alur tersebut dengan menambahkan Charlie. Bob tidak hanya menjadi penerima, tetapi juga menjadi pihak yang meneruskan pesan kepada Charlie setelah melakukan proses dekripsi. Karena setiap penerima memiliki identitas yang berbeda, perangkat lunak mensyaratkan ID tujuan antarpengguna tidak sama. Model ini membantu memperlihatkan bahwa proses IBE dapat digunakan pada alur komunikasi lebih dari dua pihak dan setiap penerima mempunyai private key yang berkaitan dengan identitasnya masing-masing.

**2.6 Perangkat lunak sebagai media pembelajaran**

Nilai pembelajaran pada perangkat lunak terletak pada kemampuan sistem untuk memperlihatkan proses internal algoritma. Pengguna dapat melihat perubahan data dari plaintext menjadi representasi heksadesimal, proses hash SHA-1, pembentukan parameter, operasi XOR, pembentukan U dan V, penggabungan ciphertext, sampai pemulihan plaintext. Selain itu, kecepatan visualisasi dapat diatur sehingga pengguna mempunyai kesempatan untuk mengikuti tahapan perhitungan. Fasilitas teori dan sejarah juga menghubungkan implementasi dengan konsep kriptografi yang mendasarinya.

**2.7 Komponen pendukung implementasi**

Selain algoritma utama IBE, implementasi memanfaatkan beberapa komponen pendukung agar proses dapat ditampilkan secara interaktif. Command button digunakan untuk menjalankan aksi seperti proses, clear, cancel, save, start, resume, dan exit. Label digunakan untuk memberikan keterangan terhadap data yang sedang ditampilkan. Textbox menjadi media untuk memasukkan message, identitas tujuan, ciphertext, dan plaintext. Common dialog control digunakan pada fasilitas penyimpanan, sedangkan image menampilkan ilustrasi hubungan antarpengguna. Timer mengatur interval setiap langkah visualisasi, combo box menyediakan pilihan kecepatan, dan listbox menampilkan urutan tahapan perhitungan.

Pembagian komponen tersebut memperlihatkan bahwa rancangan antarmuka disusun mengikuti kebutuhan proses algoritma. Form input memusatkan perhatian pada data yang dibutuhkan sebelum proses dimulai, sedangkan form proses memusatkan perhatian pada perubahan nilai selama algoritma berjalan. Pemisahan ini penting untuk perangkat lunak pembelajaran karena pengguna dapat membedakan antara data masukan, proses matematis, dan keluaran tanpa harus membaca kode program.

## 3. METODOLOGI

Metodologi artikel ini mengikuti tahapan perancangan dan implementasi yang terdokumentasi dalam skripsi. Tahapan dimulai dari identifikasi kebutuhan perangkat lunak, perumusan alur IBE, perancangan antarmuka, implementasi algoritma, kemudian pengujian menggunakan skenario komunikasi dua pengguna dan tiga pengguna. Fokus pengujian adalah memastikan bahwa setiap tahap dapat ditampilkan secara berurutan dan bahwa hasil enkripsi dapat diproses kembali hingga plaintext diperoleh.

**3.1 Analisis kebutuhan**

| No | Kebutuhan sistem | Implementasi |
|---|---|---|
| 1 | Input plaintext maksimum 48 karakter | Textbox message |
| 2 | Identitas tujuan | E-mail, Hp Number, Phone Number, Address, Id Card Number |
| 3 | Tahap pembentukan kunci | Setup dan Extract |
| 4 | Tahap enkripsi dan dekripsi | Form proses dengan visualisasi langkah |
| 5 | Model komunikasi | 2 user dan 3 user |
| 6 | Kontrol pembelajaran | Pengaturan kecepatan proses |
| 7 | Dokumentasi hasil | Fasilitas Save ke file .txt |

*Tabel 1. Kebutuhan utama perangkat lunak pembelajaran IBE*

**3.2 Alur algoritma IBE**

Pada tahap Setup, sistem menghasilkan titik pada kurva elips dan master key, kemudian menghitung parameter publik. Pada tahap Extract, identitas penerima dikonversi ke bentuk yang diperlukan dan diproses

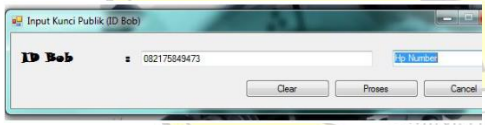
P-ISSN : 2580-4316
E-ISSN : 2654-8054 https://doi.org/10.37817/ikraith-informatika.v11i2

menggunakan SHA-1 untuk memperoleh nilai yang digunakan dalam pembentukan private key. Pada tahap enkripsi, pesan dikonversi ke bentuk heksadesimal, bilangan acak r ditentukan, kemudian sistem menghitung komponen ciphertext U dan V. Komponen V diperoleh melalui operasi XOR antara plaintext dan nilai hash H2. Ciphertext merupakan gabungan komponen U dan V. Pada tahap dekripsi, penerima memasukkan ciphertext dan private key; sistem menghitung kembali nilai H2 dan melakukan XOR terhadap komponen V sehingga plaintext dapat diperoleh kembali.

### 3.3 Perancangan perangkat lunak

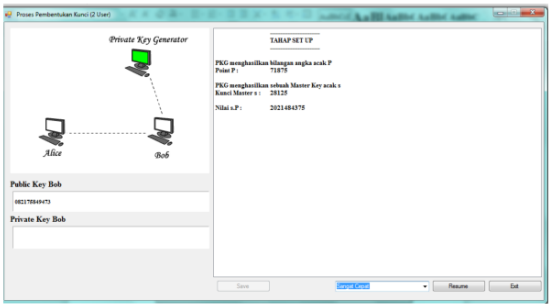
Perangkat lunak dirancang menggunakan Microsoft Visual Basic .NET. Objek antarmuka yang digunakan meliputi command button, label, textbox, common dialog control, image, timer, combo box, dan listbox. Form utama berfungsi sebagai penghubung ke proses pembentukan kunci, enkripsi, dekripsi, sejarah, teori, SHA-1, dan team. Untuk model dua pengguna, alur mencakup Alice sebagai pengirim dan Bob sebagai penerima. Model tiga pengguna menambahkan Charlie sebagai penerima berikutnya sehingga pesan dapat diproses kembali dari Bob menuju Charlie.

Contoh implementasi awal memperlihatkan input identitas Bob sebelum proses pembentukan kunci. Identitas pada contoh skripsi adalah 082175849473 dengan tipe Hp Number. Tampilan tersebut ditunjukkan pada Gambar 1.




*Gambar 1. Tampilan input kunci publik ID Bob*

Setelah input identitas diproses, sistem menampilkan proses Setup dan pembentukan private key. Antarmuka proses menyediakan area visualisasi tahapan, informasi public/private key, kontrol kecepatan, dan tombol penyimpanan hasil. Contoh rancangan proses pembentukan kunci ditunjukkan pada Gambar 2.




*Gambar 2. Tampilan proses pembentukan kunci dua pengguna*

### 3.4 Prosedur pengujian

Pengujian pada artikel dilakukan dengan menelusuri skenario yang memang didokumentasikan dalam bab implementasi skripsi. Pengujian tidak diarahkan untuk mengukur keamanan kriptografis secara formal, tetapi untuk memeriksa kesesuaian fungsi perangkat lunak dengan kebutuhan yang telah ditetapkan. Setiap skenario dimulai dari input identitas atau pesan, menjalankan proses melalui antarmuka, mengamati tahapan perhitungan, dan memeriksa keluaran proses. Skenario dua pengguna digunakan untuk memeriksa alur dasar, sedangkan skenario tiga pengguna digunakan untuk memeriksa pembentukan kunci bagi dua penerima dan pengiriman pesan berantai.

| No | Skenario | Input utama | Keluaran yang diperiksa |
|---|---|---|---|
| 1 | Input identitas | ID Bob 082175849473 | ID diterima dan tipe identitas dipilih |
| 2 | Setup | P dan master key acak | Parameter sistem ditampilkan |
| 3 | Extract | Identitas Bob | Private key Bob ditampilkan |
| 4 | Enkripsi 2 user | ISTP + ID Bob | Ciphertext terbentuk |
| 5 | Dekripsi 2 user | Ciphertext + private key Bob | Plaintext ISTP |
| 6 | Setup/Extract 3 user | ID Bob + ID Charlie | Kunci kedua penerima diproses |
| 7 | Enkripsi Alice-Bob | ISTP + ID Bob | Ciphertext Alice-Bob |
| 8 | Dekripsi Bob | Ciphertext + private key | Pesan dipulihkan |
| 9 | Enkripsi Bob-Charlie | Pesan + ID Charlie | Ciphertext berikutnya |
| 10 | Dekripsi Charlie | Ciphertext + private key | Plaintext Charlie |

*Tabel 3. Skenario pengujian fungsional berdasarkan implementasi skripsi*

P-ISSN : 2580-4316
E-ISSN : 2654-8054
https://doi.org/10.37817/ikraith-informatika.v11i2

### 3.5 Urutan pelaksanaan penelitian

Urutan pelaksanaan dapat diringkas menjadi lima kegiatan. Pertama, dilakukan identifikasi permasalahan pembelajaran IBE dan penentuan batasan sistem. Kedua, dilakukan pemahaman terhadap konsep kriptografi kunci publik, IBE, SHA-1, kurva elips, dan operasi matematis yang digunakan. Ketiga, dilakukan perancangan alur Setup, Extract, Encrypt, dan Decrypt serta rancangan form yang dibutuhkan untuk dua dan tiga pengguna. Keempat, rancangan diterapkan menggunakan Microsoft Visual Basic .NET dengan objek antarmuka yang telah ditentukan. Kelima, sistem dijalankan menggunakan contoh input yang tercantum dalam bab implementasi dan hasil setiap tahap diamati untuk memastikan alurnya sesuai dengan rancangan.

Tahapan tersebut menempatkan kebutuhan pembelajaran sebagai dasar perancangan. Karena target perangkat lunak adalah memberikan gambaran proses, maka setiap tahapan algoritma perlu mempunyai representasi pada antarmuka. Misalnya, Setup tidak hanya menghasilkan public parameter, tetapi juga menampilkan nilai yang dihasilkan PKG. Extract tidak hanya menghasilkan private key, tetapi juga memperlihatkan proses pemrosesan identitas. Demikian pula Encrypt dan Decrypt menampilkan transformasi data dan operasi yang dilakukan.

## 4. HASIL DAN PEMBAHASAN

### 4.1 Implementasi pembentukan kunci

Hasil implementasi menunjukkan bahwa menu Pembentukan Kunci menampilkan form input identitas penerima. Setelah tombol proses dijalankan, sistem masuk ke tahap Setup. Pada contoh dua pengguna dalam skripsi, PKG menghasilkan bilangan acak P sebesar 71875 dan master key s sebesar 28125, kemudian menghitung s.P sebesar 2021484375. Selanjutnya proses Extract memproses identitas Bob melalui SHA-1 dan perhitungan berikutnya untuk memperoleh private key. Nilai-nilai tersebut ditampilkan bertahap pada area proses sehingga pengguna pembelajaran tidak hanya melihat hasil akhir, tetapi juga dapat mengikuti urutan perhitungannya.

### 4.2 Implementasi enkripsi dan dekripsi dua pengguna

Pada skenario dua pengguna, Alice memasukkan pesan “ISTP” dan ID Bob 082175849473. Pesan diubah ke bentuk heksadesimal, kemudian sistem menentukan bilangan acak r dan menghitung komponen ciphertext. Nilai V dibentuk melalui XOR plaintext dengan H2. Setelah U dan V digabungkan, ciphertext ditampilkan dan dapat disimpan. Pada tahap dekripsi, Bob memasukkan ciphertext, identitas, dan private key. Sistem menghitung H2(dID,U), melakukan XOR dengan V, kemudian mengubah hasil kembali ke karakter sehingga pesan “ISTP” diperoleh sebagai plaintext. Rangkaian tersebut memperlihatkan keterkaitan langsung antara tahap enkripsi dan dekripsi.

### 4.3 Implementasi komunikasi tiga pengguna

Model tiga pengguna menggunakan Alice, Bob, dan Charlie. Pada tahap pembentukan kunci, sistem memproses identitas Bob dan Charlie. Skripsi menggunakan contoh ID Bob 082175849473 dan ID Charlie 085270456013. Alice mengenkripsi pesan untuk Bob, Bob melakukan dekripsi, kemudian pesan diproses kembali untuk dikirimkan kepada Charlie. Pada model ini identitas tujuan antarpengguna tidak boleh sama. Perangkat lunak menampilkan setiap tahapan sehingga model komunikasi berantai dapat dipelajari secara visual.

### 4.4 Visualisasi dan fasilitas pembelajaran

Salah satu hasil utama perangkat lunak adalah penyajian proses secara bertahap. Setiap form proses menyediakan area hasil perhitungan, tombol Start/Resume atau proses, kontrol Speed, dan fasilitas Save pada proses tertentu. Dengan demikian, perangkat lunak tidak berhenti pada fungsi enkripsi dan dekripsi, tetapi juga menempatkan perhitungan sebagai materi pembelajaran. Menu Sejarah dan Teori memberikan materi terkait IBE, sedangkan menu SHA-1 menyediakan teori pendukung yang berkaitan dengan pemrosesan identitas.

| Aspek yang diuji | Skenario pada skripsi | Hasil yang didokumentasikan |
|---|---|---|
| Pembentukan kunci | ID Bob pada model 2 user | Setup, Extract dan private key ditampilkan |
| Enkripsi 2 user | Pesan ISTP ke Bob | Ciphertext U dan V ditampilkan |
| Dekripsi 2 user | Bob menggunakan private key | Plaintext ISTP diperoleh kembali |
| Pembentukan kunci 3 user | ID Bob dan ID Charlie | Private key untuk kedua identitas diproses |

P-ISSN : 2580-4316
E-ISSN : 2654-8054 https://doi.org/10.37817/ikraith-informatika.v11i2

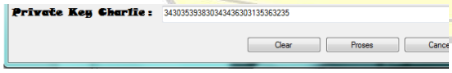
| | | |
|---|---|---|
| Enkripsi 3 user | Alice ke Bob | Ciphertext ditampilkan dan dikirim ke Bob |
| Dekripsi 3 user | Bob menerima ciphertext | Pesan dipulihkan sebelum diproses kembali |
| Enkripsi ulang | Bob ke Charlie | Pesan diproses kembali menggunakan alur IBE |
| Penyimpanan | Tombol Save | Hasil proses dapat disimpan sebagai .txt |

*Tabel 2. Ringkasan hasil implementasi berdasarkan skenario pada skripsi*

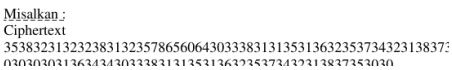
### 4.5 Pembahasan

Hasil implementasi selaras dengan tujuan awal penelitian, yaitu menampilkan proses kerja IBE secara terperinci dan membantu pemahaman algoritma. Fasilitas pengaturan kecepatan membuat pengguna dapat mengikuti tahapan perhitungan, sedangkan fasilitas Save memungkinkan proses dan hasil perhitungan disimpan. Dari sisi pembelajaran, pemisahan antara Setup, Extract, Encrypt, dan Decrypt membantu memperjelas fungsi masing-masing komponen. Model dua pengguna memberikan alur dasar komunikasi, sedangkan model tiga pengguna memperlihatkan bagaimana pesan dapat diteruskan dan diproses kembali.

Namun, ruang lingkup perangkat lunak tetap mengikuti batasan skripsi. Plaintext dibatasi maksimum 48 karakter, animasi bersifat statis, dan penyimpanan hasil menggunakan berkas teks. Perangkat lunak juga ditujukan sebagai alat bantu pembelajaran, bukan sebagai aplikasi pengamanan file umum. Hal tersebut penting karena hasil penelitian yang dilaporkan adalah keberhasilan visualisasi dan implementasi skenario IBE yang telah dirancang, bukan evaluasi keamanan komersial terhadap sistem kriptografi.




*Gambar 4.16 Tampilan Form Input Data Dekripsi (3 user - Charlie)*




*Gambar 3. Tampilan input data dekripsi tiga pengguna untuk Charlie*

### 4.6 Contoh alur perhitungan pada implementasi

Contoh implementasi dua pengguna menggunakan ID Bob 082175849473 dengan tipe Hp Number dan pesan ISTP. Pada proses Setup, nilai yang ditampilkan dalam skripsi adalah P = 71875, master key s = 28125, dan s.P = 2021484375. Nilai tersebut merupakan bagian dari demonstrasi proses, bukan parameter tetap yang harus digunakan pada setiap eksekusi karena perangkat lunak menggunakan pembangkitan nilai acak. Setelah tahap Setup, sistem melanjutkan tahap Extract dengan memproses ID Bob menggunakan SHA-1.

Pada tahap enkripsi, pesan ISTP diubah menjadi representasi heksadesimal 49535450 dan dilengkapi hingga panjang blok yang digunakan dalam implementasi. Sistem kemudian menentukan bilangan acak r dan menghitung U serta H2. Komponen V diperoleh melalui XOR plaintext dengan H2. Dari dokumentasi implementasi, ciphertext yang dihasilkan kemudian ditampilkan sebagai gabungan dua komponen tersebut. Pada dekripsi, Bob menggunakan private key dan ciphertext untuk menghitung kembali H2(dID,U), kemudian XOR dilakukan antara V dan H2 sehingga nilai plaintext dapat dikembalikan. Hasil akhir dikonversi dari heksadesimal ke karakter dan menghasilkan pesan ISTP.

Untuk tiga pengguna, skripsi mendokumentasikan ID Bob 082175849473 dan ID Charlie 085270456013. Pada proses pembentukan kunci, sistem menjalankan Extract untuk Bob dan Charlie. Selanjutnya Alice mengenkripsi pesan kepada Bob. Setelah Bob memperoleh plaintext, proses dilanjutkan dengan enkripsi kembali menuju Charlie. Tahap dekripsi Charlie menggunakan private key Charlie. Rangkaian ini menunjukkan bahwa setiap tujuan mempunyai identitas dan private key yang berbeda, sementara tahapan dasar enkripsi dan dekripsinya tetap mengikuti alur IBE yang sama.

### 4.7 Tampilan proses dan keterlacakan pembelajaran

Antarmuka proses dibuat untuk menempatkan keluaran perhitungan di area yang dapat dibaca pengguna. Form pembentukan kunci memperlihatkan peran PKG, Alice, dan Bob serta nilai public key dan private key. Form enkripsi menampilkan message, identitas tujuan, bilangan acak, hasil hash, dan ciphertext. Form dekripsi menampilkan ciphertext yang diterima, identitas penerima, private key, proses XOR, dan plaintext. Susunan tersebut membuat

P-ISSN : 2580-4316
E-ISSN : 2654-8054
https://doi.org/10.37817/ikraith-informatika.v11i2

hubungan antara masukan, proses, dan keluaran lebih mudah ditelusuri dibandingkan program yang hanya menampilkan hasil akhir.

Fasilitas Save juga mendukung kegiatan pembelajaran karena pengguna dapat menyimpan hasil eksekusi untuk dibaca kembali. Sementara itu, menu Sejarah dan Teori menyediakan materi yang berhubungan dengan IBE, sedangkan menu SHA-1 memberikan teori pendukung. Kombinasi materi konseptual dan visualisasi perhitungan menjadikan perangkat lunak tidak hanya berfungsi sebagai demonstrasi enkripsi, tetapi juga sebagai media untuk mempelajari urutan algoritma.

### 4.8 Batasan hasil implementasi

Hasil penelitian harus dibaca sesuai ruang lingkup yang ditetapkan pada skripsi. Sistem menerima plaintext maksimum 48 karakter dan membatasi beberapa tipe identitas berdasarkan format tertentu. Penyimpanan hasil dilakukan dalam berkas .txt dan animasi bersifat statis. Selain itu, penelitian tidak mendokumentasikan pengujian penetrasi, analisis ketahanan terhadap serangan, atau perbandingan kinerja dengan algoritma kriptografi lain. Oleh karena itu, kontribusi yang dilaporkan dalam artikel ini adalah perangkat lunak bantu pembelajaran yang memvisualisasikan proses IBE sesuai algoritma dan skenario yang dirancang.

### 4.9 Analisis ketercapaian tujuan

Tujuan pertama penelitian adalah menampilkan proses pembentukan kunci, enkripsi, dan dekripsi pada IBE. Berdasarkan implementasi, ketiga proses tersebut mempunyai form tersendiri dan dapat dijalankan melalui menu Proses. Pembentukan kunci dibagi menjadi Setup dan Extract, sedangkan model tiga pengguna menyediakan pembentukan kunci untuk ID Bob dan ID Charlie. Proses enkripsi menampilkan message, identitas tujuan, bilangan acak, perhitungan U dan V, serta ciphertext. Proses dekripsi menampilkan ciphertext, identitas, private key, perhitungan H2, operasi XOR, dan hasil plaintext.

Tujuan kedua adalah mempermudah pembelajaran IBE. Indikator yang tersedia dalam implementasi adalah adanya visualisasi setiap tahapan, kontrol kecepatan, materi Sejarah dan Teori, materi SHA-1, serta fasilitas Save. Dengan fasilitas tersebut, pengguna dapat mengamati proses pada kecepatan yang dapat disesuaikan dan menyimpan hasilnya untuk dipelajari kembali. Kesimpulan ini mengikuti hasil yang dilaporkan dalam skripsi, yaitu bahwa perangkat lunak dapat digunakan untuk membantu pemahaman algoritma IBE.

### 4.10 Perbandingan alur dua pengguna dan tiga pengguna

| Komponen | Dua pengguna | Tiga pengguna |
|---|---|---|
| Pengirim | Alice | Alice, kemudian Bob |
| Penerima | Bob | Bob dan Charlie |
| Pembentukan kunci | ID Bob | ID Bob dan ID Charlie |
| Enkripsi | Alice ke Bob | Alice ke Bob dan Bob ke Charlie |
| Dekripsi | Bob | Bob dan Charlie |
| Identitas tujuan | Satu identitas tujuan | Dua identitas tujuan berbeda |
| Fokus pembelajaran | Alur dasar IBE | Alur komunikasi berantai |

*Tabel 4. Perbandingan model komunikasi pada perangkat lunak*

Perbandingan pada Tabel 4 menunjukkan bahwa perbedaan utama kedua model terletak pada jumlah pihak dan tahap pengiriman pesan. Prinsip dasar IBE tetap dipertahankan, tetapi model tiga pengguna menambahkan tahap pembentukan kunci untuk Charlie serta proses enkripsi dan dekripsi lanjutan. Dengan demikian, pengguna dapat mempelajari konsep dasar terlebih dahulu melalui model dua pengguna sebelum melihat skenario yang lebih panjang pada model tiga pengguna.

## 5. KESIMPULAN

Perangkat lunak pembelajaran IBE yang dirancang pada skripsi dapat menampilkan proses kerja algoritma kriptografi IBE secara bertahap, mulai dari pembentukan kunci, enkripsi, hingga dekripsi. Sistem juga menyediakan pengaturan kecepatan perhitungan dan animasi proses sehingga dapat digunakan untuk membantu pemahaman algoritma. Selain itu, fasilitas Save memungkinkan proses kerja dan hasil perhitungan disimpan sebagai berkas teks. Implementasi mencakup model dua pengguna dan tiga pengguna, dengan contoh proses yang menunjukkan bahwa pesan dapat dikembalikan ke bentuk plaintext setelah dekripsi. Berdasarkan hasil tersebut, perangkat lunak memenuhi tujuan yang ditetapkan dalam skripsi sebagai alat bantu pembelajaran IBE.

## 6. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak yang telah memberikan dukungan selama proses penyusunan dan penyelesaian penelitian serta pengembangan perangkat lunak pembelajaran IBE.

**DAFTAR PUSTAKA**

1. Ariyus, D. (2020). Kriptografi: Keamanan Data dan Komunikasi. Yogyakarta: Andi Publisher.

2. Enterprise, J. (2021). Keamanan Data dan Jaringan Komputer. Jakarta: Elex Media Komputindo.

3. Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). Modul Literasi Digital: Keamanan Digital. Jakarta: Kominfo.

4. Badan Siber dan Sandi Negara. (2023). Laporan Tahunan Badan Siber dan Sandi Negara 2023. Jakarta: BSSN.

5. Badan Siber dan Sandi Negara. (2021). Pedoman Keamanan Siber Indonesia. Jakarta: BSSN.

6. Suyanto. (2021). Pengantar Keamanan Informasi. Yogyakarta: Penerbit Andi.

7. Rerung, R. R. (2020). Keamanan Informasi dan Jaringan Komputer. Yogyakarta: Deepublish.

8. Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi. (2023). Buku Ajar Keamanan Informasi. Jakarta: Kemendikbudristek.

9. Badan Standardisasi Nasional. (2022). Sistem Manajemen Keamanan Informasi (SNI ISO/IEC 27001:2022). Jakarta: BSN.

10. Raharjo, B. (2021). Keamanan Informasi. Bandung: Informatika.

11. Shamir, A. (1985). Identity-based cryptosystems and signature schemes. Advances in Cryptology—CRYPTO 84, 47–53.

12. Boneh, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairing. Advances in Cryptology—CRYPTO 2001, 213–229.

13. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.

14. National Institute of Standards and Technology. (2015). Secure Hash Standard (SHS), FIPS PUB 180-4. U.S. Department of Commerce.

15. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.