

Aplikasi Keamanan Sistem Pengiriman Tagihan Pembayaran *Online* (Invoice) Berbasis Website dengan algoritma RSA-CRT

Muhammad Fikhri Rafli¹, Zaimah Panjaitan², Wahyu Riansah³

^{1,2,3} Sistem Informasi, STMIK Triguna Dharma, Medan, Indonesia

Email: ¹fikhri.rafli@gmail.com, ²zaimahp09@gmail.com, ³wahyuriansah2@gmail.com

Email Penulis Korespondensi: zaimahp09@gmail.com

Article History:

Received Dec 10th, 2023

Revised Dec 22th, 2023

Accepted Jan 15th, 2024

Abstrak

Pemanfaatan teknologi saat ini harus bisa dilakukan oleh semua bidang. Kemudahan komunikasi dapat mempercepat pihak instansi dalam proses pengiriman dokumen invoice secara online berbasis website. Invoice berisikan detail transaksi yang bersifat rahasia. Aspek keamanan data yang dikirimkan merupakan hal yang harus dijaga, karena manipulasi data di tengah pengiriman dapat merugikan kedua belah pihak. Salah satu tindakan dalam pencegahan dari manipulasi data yaitu dengan memanfaatkan ilmu kriptografi yang mengubah pesan menjadi kode rahasia yang sulit dipahami. Sehingga keaslian dan keamanan data dapat terjamin. RSA - CRT merupakan modifikasi dari dua buah algoritma RSA (Rivest Shamir Adleman) merupakan salah satu jenis kriptografi yang bersifat asimetris. Penerapan algoritma RSA akan mengubah isi dari invoice menjadi kode rahasia. Sedangkan CRT (Chinese Remainder Theorem) teori matematika yang akan menambah keamanan sistem dengan adanya perhitungan tambahan untuk proses dekripsi.

Kata Kunci : Kriptografi, RSA (Rivest Shamir Adleman), CRT (Chinese Remainder Theorem), Asimetris, Invoice.

Abstract

The utilization of technology nowadays should be accessible across all fields. The ease of communication can accelerate institutional parties in the process of sending invoice documents online via a website-based platform. Invoices contain transaction details that are confidential. The security aspect of the transmitted data must be safeguarded, as data manipulation during transmission can be detrimental to both parties. One preventive measure against data manipulation is by utilizing the science of cryptography, which converts messages into secret codes that are difficult to decipher. Thus, the authenticity and security of the data can be ensured. RSA - CRT is a modification of two RSA (Rivest Shamir Adleman) algorithms, which is one type of asymmetric cryptography. The implementation of the RSA algorithm will transform the content of the invoice into a secret code. Meanwhile, CRT (Chinese Remainder Theorem) is a mathematical theory that enhances system security by incorporating additional calculations for the decryption process.

Keyword : Cryptography, RSA (Rivest Shamir Adleman), CRT (Chinese Remainder Theorem), Asymmetric, Invoice.

1. PENDAHULUAN

Semua bidang usaha atau bisnis memanfaatkan teknologi komputer sebagai media untuk memperoleh informasi yang cepat dan akurat. Teknologi informasi memiliki pengaruh untuk mentransformasikan bagaimana bisnis dijalankan. Manfaat teknologi dalam bisnis salah satunya adalah pengiriman data seperti invoice dapat dilakukan dengan cepat. Invoice atau dikenal juga dengan faktur merupakan sebuah dokumen yang memuat bukti pembelian. Dokumen tersebut berisi tentang detail pembelian barang, seperti harga per item, banyaknya barang, jumlah barang, hingga waktu dilakukannya pembelian tersebut. Selain berupa rincian pembelian, invoice juga dapat digunakan sebagai tagihan penjual kepada pembeli[1]. Informasi pada invoice berupa rincian pembelian yang akan dikirimkan kepada client harus dalam keadaan aman. Rawannya manipulasi data oleh pihak lain dapat mengganggu proses transaksi. Kerahasiaan data sangat diperlukan baik dalam suatu organisasi maupun pribadi, bahkan dalam jaringan internasional yang sering disebut internet. Untuk menjaga kerahasiaan data, maka diperlukan keamanan data agar data tidak dapat dibaca dan dimengerti.

Permasalahan yang terjadi adalah bagaimana cara pengamanan yang dapat dilakukan saat invoice sebagai nota tagihan dikirim kepada customer, menggunakan teknologi yang mempermudah pengiriman secara online, dengan aplikasi yang ramah bagi user namun memiliki keamanan yang membuat user merasa aman dalam bertransaksi. Pada penelitian ini,

permasalahan ini akan diselesaikan dengan cara membuat aplikasi yang mengandung teknologi kriptografi berupa autentikasi pesan yang meyakinkan bahwa pengirim dan data yang dikirim adalah benar dan penerima juga benar sesuai dengan kebutuhan pembayaran. Cara yang digunakan dalam penelitian ini adalah dengan pemanfaatan kunci private yang dibangkitkan dengan algoritma RSA.

Kriptografi merupakan ilmu untuk menjaga kerahasiaan pesan dengan cara mengubahnya ke dalam bentuk yang tidak dapat dimengerti isinya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan Enkripsi dan Dekripsi[2]. Kriptografi berdasarkan jenis kuncinya dibedakan menjadi dua, yaitu asimetris dan simetris. Salah satu algoritma dalam Kriptografi asimetris adalah Algoritma RSA. RSA (Rivest Shamir Adleman) merupakan salah satu algoritma kriptografi asimetris yang menggunakan sepasang kunci yaitu publik dan privat. Panjang kunci dapat disesuaikan, semakin panjang bit dalam pembentukan kunci, maka akan rumit untuk dipecahkan, karena harus memfaktorkan dua bilangan yang sangat besar[3].

Kelebihan RSA terletak pada sepasang kunci yang digunakan untuk mengenkripsi dan mendekripsi pesan. Kelebihan lain algoritma RSA ada pada ketahanannya terhadap serangan, Hal ini disebabkan kompleksitas dekripsinya yang dinamis dengan cara menentukan nilai p dan q pada saat proses pembangkitan pasangan kunci, sehingga dihasilkan sebuah key space yang cukup besar, sehingga tahan terhadap serangan. Perhitungan pada RSA yang sangat besar akan sangat sulit untuk diimplementasikan pada program. Untuk itu perlu adanya algoritma tambahan yang dapat memperkecil perhitungan RSA. CRT (Chinese Remainder Theorem) adalah salah satu algoritma yang dapat digunakan dalam implementasi RSA. CRT (Chinese Remainder Theorem) adalah suatu algoritma yang dapat mengurangi perhitungan aritmatika modular dengan modulus besar untuk perhitungan yang sama untuk masing-masing faktor dari modulus [4]. Kombinasi RSA-CRT menjadi lebih maksimal dalam pengamanan data.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Penelitian ini dilakukan dengan beberapa tahapan yaitu pertama adalah identifikasi permasalahan. Dalam hal ini dilakukan observasi mengenai permasalahan yang dihadapi oleh sebuah perusahaan yang memiliki urgensi pengiriman tagihan invoice secara online kepada customer [5]. Observasi dan pengumpulan data dengan melakukan tinjauan dan pengamatan secara langsung ke CV. ARD Pro. Kegiatan ini bertujuan untuk menganalisis masalah yang dihadapi terkait Invoice pada CV. ARD Pro. Setelah pengumpulan data, maka didapat bahwasannya invoice yang akan dikirimkan ke client CV. ARD Pro masih tidak aman atau mudah untuk dimanipulasi. Keterangan pada invoice CV. ARD Pro. Yaitu Nomor Faktur, Nama Client, Jumlah Uang dan Detail Pembayaran haruslah bersifat rahasia karena merupakan data yang sensitif. Diperlukan teknik kriptografi untuk memastikan integritas, kerahasiaan, keasliannya.

Kemudian, dari identifikasi tersebut maka diambil keputusan pemanfaatan metode yang digunakan untuk masalah keamanan pengiriman invoice. Tahapan ketiga adalah mengidentifikasi algoritma kriptografi yang akan dipakai pada aplikasi pengiriman invoice, sejauh mana algoritma tersebut secara matematis mampu untuk mengamankan data. Dalam tahapan ini dilakukan juga observasi mengenai kelebihan dan kelemahan algoritma. Tahapan keempat adalah merancang sistem yang dilanjutkan dengan tahapan kelima yaitu membangun sistem sesuai dengan rancangan serta memasukkan algoritma yang telah dicanangkan ke dalam sistem yang di bangun. Setelah sistem selesai dibangun, maka dilakukan pengujian sistem. Pada akhirnya, diambil kesimpulan apakah sistem ini layak dan dapat menjadi solusi dari permasalahan yang ada atau tidak.

2.2 Algoritma RSA

RSA ditemukan oleh 3 orang penemu Ron Rivest, Adi Shamir, dan Leonard Adleman[6]. Penemu pertama algoritma kriptografi asimetris adalah Shifford Cocks, James H. Ellis dan Malcolm Williamson (sekelompok ahli matematika yang bekerja untuk United Kindom's Government Communication Head Quarters, agen rahasia Inggris) pada awal tahun 1970. Pada tahun 1976 algoritma kunci asimetris untuk pertama kalinya dipublikasikan oleh Whitfield Diffie dan Martin Hellman. Ide Clifford Cocks ditemukan kembali oleh Ron Rivest, Adi Shamir dan Leonard Adleman dari Massachussets Intitute of Technology pada tahun 1977 dan dipublikasikan pada tahun 1978[7].

RSA mempunyai dua kunci yaitu kunci publik (Public Key) dan kunci privat (Private Key) yang menyebabkan masuk dalam kategori asimetris[8]. Algoritma ini memanfaatkan bilangan prima (bilangan yang hanya habis dibagi oleh bilangan itu sendiri) untuk menghasilkan sepasang kunci yang akan digunakan pada prose enkripsi dan dekripsi. Meskipun algoritma RSA ini merupakan standard dunia, tapi algoritma RSA ini masih memiliki kelebihan dan kekurangan[9].

Adapun kelebihan RSA adalah sebagai berikut[10][11] :

1. Tingkat keamanan berlapis dan menjadi lebih terjamin karena memakai dua kunci yang berbeda pada proses enkripsi dan dekripsi.
2. RSA dapat digunakan sebagai tanda tangan digital (digital signature), sehingga penyengkalan dapat dicegah.
3. Distribusi kunci menjadi lebih mudah karena jalur aman untuk distribusi kunci tidak lagi diperlukan.
4. Sulitnya memfaktorkan bilangan non prima menjadi faktor prima.
5. Manajemen kunci menjadi lebih mudah karena memiliki 2 buah kunci.

Adapun kelemahan algoritma RSA meliputi[12] :

1. Jika pesan akan di enkripsi dan dekripsi memiliki teks yang panjang, proses enkripsi dan dekripsi membutuhkan waktu yang sangat lambat.
2. Ukuran cipher menjadi sekitar 2 kali lipat ukuran semula.

2.3 Implementasi Algoritma RSA-CRT

CRT (Chinese Remainder Theorem) adalah suatu teori matematis yang digunakan untuk mengkonversi eksponensiasi modular yang berukuran besar menjadi eksponensiasi modular yang relatif lebih kecil[13]. CRT misalkan $m = m_1, m_2, \dots, m_n$, dan setiap pasang m_i, m_j coprime (bilangan bulat positif sedemikian hingga $PBB(m_i, m_j) = 1$ untuk $i \neq j$).

CRT pada dasarnya digunakan untuk menyempurnakan kekuarangan pada algoritma RSA yang pada saat dekripsi sulit untuk dilakukan karena besarnya nilai pemangkatan. CRT berfungsi untuk menguraikan pangkat pada RSA sehingga teknik matematis pada CRT mampu mempercepat proses yang ada pada pemangkatan saat dekripsi di algoritma RSA.

1. Proses pembangkitan kunci algoritma RSA

- a. Menentukan bilangan prima untuk p dan q , dimana $p = 43$ dan $q = 47$
- b. Melakukan perkalian nilai p dengan q untuk mendapatkan nilai modulus (n):
$$n = p \times q$$
$$= 43 \times 47 = 2021$$
 (1)

- c. Menghitung nilai totient n (ϕn)
$$\phi n = (p - 1)(q - 1)$$
$$= (43 - 1)(47 - 1) = 1932$$
 (2)

- d. Menentukan nilai e , dengan syarat GCD (Greater Common Divisor), dimana $\text{gcd}(e, \phi n) = 1$ Nilai e didapat dengan mencoba bilangan yang memenuhi $\text{gcd}(e, \phi n) = 1$. Untuk menentukan nilai e ini, diperlukan persamaan dengan Rumus Algoritma Euclidean sebagai berikut :
$$r^0 = q^1 r^1 + r^2, 0 < r^2 < r^1, r^1 = q^2 r^2 + r^3, 0 < r^3 < r^2, r^n = \dots$$
 (3)

Nilai e yang diambil adalah 5, karena $\text{gcd}(5, 1932) = 1$ maka $e = 5$

- e. Menentukan kunci private (d) dengan persamaan $d = (1 + (k \times \phi n)) / e$. Nilai d yang dihasilkan dari persamaan tersebut harus berupa bilangan bulat. Nilai k merupakan nilai acak $k = 1, 2, 3 \dots$ dst hingga menghasilkan bilangan bulat. $k = 2$
$$d = (1 + (k \times \phi n)) / e$$
$$= (1 + (2 \times 1932)) / 5$$
$$= (1 + 3864) / 5$$
$$= 3865 / 5 = 773$$

sehingga diperoleh pasangan kunci sebagai berikut:

- Kunci publik (e, n) => (5, 2021) (5)
Kunci rahasia (d, n) => (773, 2021)

2. Proses enkripsi Algoritma RSA

- a. Proses enkripsi menggunakan kunci public (e, n) = 5, 2021. Pesan (plaintext) yang akan dienkripsi yaitu 15DES2021. Kemudian pesan dipisah per karakter (M_n) kemudian dikonversi kedalam kode ASCII menjadi : 49 53 68 69 83 50 48 50 49.

- b. Selanjutnya adalah menghitung proses enkripsi sesuai dengan kode ASCII dengan berikut :
$$C = M^e \text{ mod } n$$
$$C^1 = M1^e \text{ mod } n$$
$$= 49^5 \text{ mod } 2021$$
$$= 282475249 \text{ mod } 2021 = 79$$

Begitu selanjutnya dilakukan untuk seluruh plaintexts sehingga didapatkan hasil enkripsi atau ciphertexts sebagai berikut : 79 68 1916 1680 488 854 330 854 79

3. Proses dekripsi algoritma RSA dengan CRT

Proses Dekripsi menggunakan kunci private (d, n) = 773, 2021.

Kemudian dihitung dengan rumus $M = C^d \text{ mod } n$.

$$M1 = C^d \text{ mod } n$$
$$= 79^{773} \text{ mod } 2021$$

Namun besarnya nilai untuk perhitungan C^d , akan sulit dihitung secara manual ataupun dengan bantuan kalkulator, sehingga perlu adanya algoritma tambahan yaitu CRT untuk memperkecil nilai d .

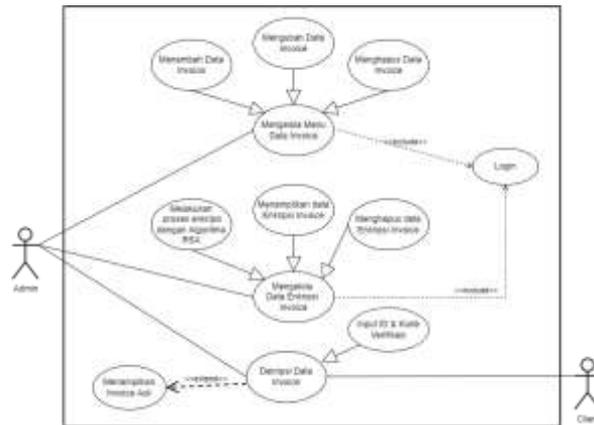
- a. Menentukan nilai dP
$$dP = e^{-1} \text{ mod } (p - 1) \Rightarrow d \text{ mod } (p - 1)$$
$$= 773 \text{ mod } (43 - 1)$$
$$= 773 \text{ mod } 42 = 17$$
 (7)

- b. Menentukan nilai dQ
$$dQ = e^{-1} \text{ mod } (q - 1) \Rightarrow d \text{ mod } (q - 1)$$
 (8)

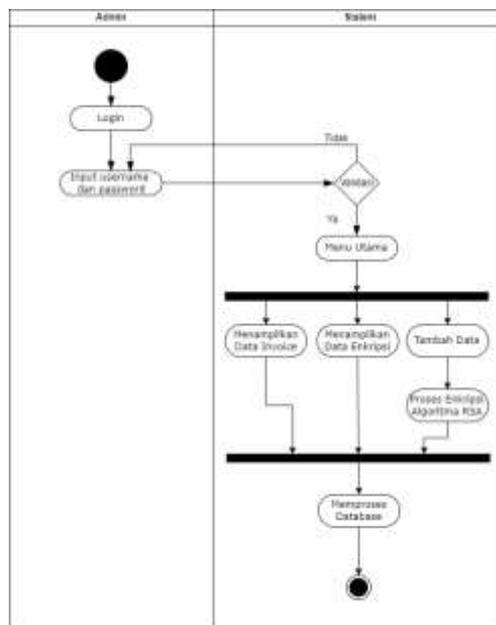
- $= 773 \bmod (47 - 1)$
 $= 773 \bmod 46 = 37$
- c. Menentukan nilai $qInv$ (9)
 $qInv = q^{-1} \bmod p$
 $= 47^{-1} \bmod 43 = 11$
artinya $11 \times 47 \equiv 1 \bmod 43$,
sama dengan $11 \times 47 \bmod 43 = 1$
Sehingga didapat $(dP, dQ, qInv) = 17, 37, 11$.
- d. Menentukan nilai $m1$ (10)
 $m1 = C^{dP} \bmod p$
 $= 79^{17} \bmod 43$
Jika dilihat, nilai pemangkatan masih terlihat besar. Untuk mencari nilai $m1$ ini maka dibuat proses sebagai berikut :
 $79 \bmod 43 = 36$
 $79^{17} \equiv 36^{17} \pmod{43}$
Faktorkan nilai pangkatnya untuk mempermudah perhitungan $36^{17} \bmod 43 = 36^{4+4+4+4+1} \bmod 43$
 $= ((36^4 \bmod 43)^4) \times (36^1 \bmod 43) \bmod 43$
 $= ((36^4) \times 36) \bmod 43$
 $= (1679616 \times 36) \bmod 43 = 6$
Maka $m1 = 79^{17} \bmod 43 = 6$
- e. Menentukan nilai $m2$ (11)
 $m2 = C^{dQ} \bmod q$
 $= 79^{37} \bmod 47$
Prosesnya sana seperti mencari $m1$
 $79 \bmod 47 = 32$
 $79^{37} \equiv 32^{37} \pmod{47}$
Lalu memfaktorkan nilai pangkat
 $32^{37} \bmod 47 = 32^{8+8+8+8+4+1} \bmod 47$
 $= ((32^8 \bmod 47)^4) \times (32^4 \bmod 47) \times (32^1 \bmod 47)$
 $\bmod 47$
 $= ((36^4) 6 \times 32) \bmod 47$
 $= (1679616 \times 6 \times 32) \bmod 47 = 2$
Maka $m2 = 79^{17} \bmod 47 = 2$
- f. Menentukan nilai h (12)
 $h = qInv (m1 - m2) \bmod p$
 $= 11 (6 - 2) \bmod P$
 $= 11 \times 4 \bmod 43$
 $= 44 \bmod 43 = 1$
- g. Terakhir menentukan Plaintext (M_1) dengan rumus : (13)
 $M = m2 + h \times q$
 $M1 = 2 + 1 \times 47$
 $= 2 + 47 = 49$
- h. Untuk mendapatkan plainteks lainnya, lakukan kembali proses di atas hingga selesai. Setelah selesai, akan didapatkan kembali nilai plainteks ASCII awal : 49 53 68 69 83 50 48 50 49.

2.4 Desain Sistem

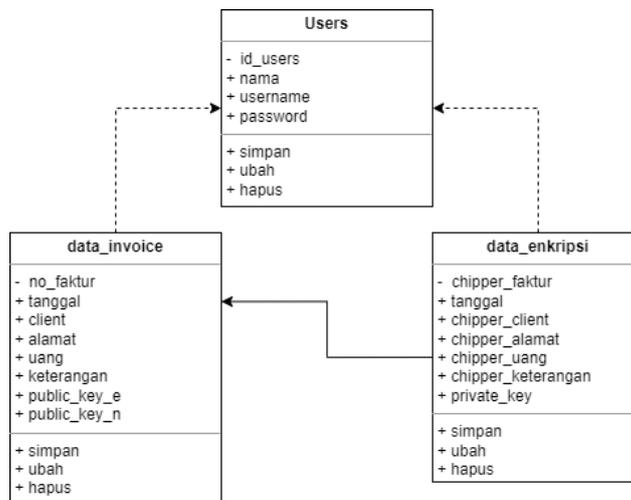
Dalam pembuatan suatu sistem, diperlukan pemodelan yang berorientasi objek dengan menggunakan standar Unified Modelling Language (UML). Diagram yang digunakan dalam pemodelan sistem adalah Use Case Diagram, Activity Diagram dan Class Diagram[14][15].



Gambar 1. Use Case Diagram



Gambar 2. Activity Diagram



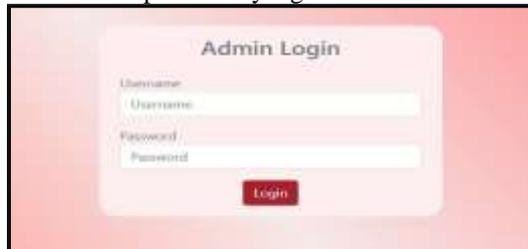
Gambar 3. Class Diagram

3. HASIL DAN PEMBAHASAN

Hasil implementasi kriptografi algoritma RSA – CRT yang digunakan untuk mengamankan data invoice pada CV. Ard Pro dirancang berbasis web. Implementasi berbasis web digunakan untuk mempermudah client dalam mengakses aplikasi[16]. Berikut adalah hasil tampilan antarmuka serta hasil pengujian dari sistem yang telah dibangun[17].

1. Tampilan Form Login

Form Login merupakan halaman yang digunakan oleh admin untuk masuk ke dalam aplikasi. Form login akan melakukan validasi terhadap username dan password yang telah terdaftar di database.



Gambar 4. Form Login

2. Tampilan Form Data Invoice

Form Data Invoice merupakan form untuk menampilkan data invoice yang tersimpan pada database.



Gambar 5. Form Data Invoice

3. Tampilan Form Buat Kunci

Form buat kunci digunakan untuk membuat sepasang kunci, public key dan private key. Pada Form Bangkit Kunci, setelah memasukkan 2 bilangan prima pada textbox dan menekan Button Buat Kunci, maka akan menampilkan public key dan private key. Disini nilai yang diambil adalah 43 dan 47.



Gambar 6. Form Buat Kunci

4. Tampilan Form Tambah Invoice

Form Tambah Invoice berfungsi untuk membuat invoice yang berisikan data client sekaligus mengenkripsi dan menyimpan ke dalam database. Setelah pasangan kunci didapat, selanjutnya membuat data invoice yang berisikan data client. Data invoice yang telah diisi selanjutnya akan dienkripsi dan disimpan kedalam database.

Gambar 7. Form Tambah Invoice

Jika berhasil maka data invoice akan disimpan ke tabel data invoice pada database dan ditampilkan pada form Data Invoice.

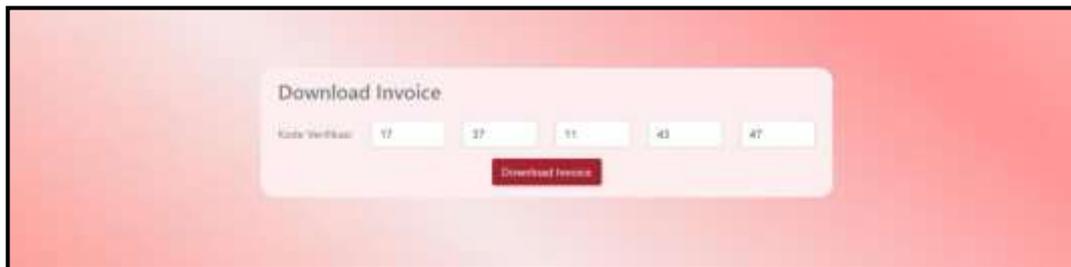
5. Tampilan Form Data Enkripsi

Form Data Enkripsi merupakan form untuk menampilkan data invoice yang telah terenkripsi di database. Form ini juga akan memberikan URL yang akan diberikan ke client untuk mengenkripsi invoice.

Gambar 8. Form Enkripsi

6. Tampilan Form Dekripsi

Saat invoice telah sampai di sisi client, maka client dapat melakukan dekripsi dengan menggunakan URL khusus yang diberikan oleh pihak perusahaan. Client akan dikirimkan URL dan private key (kode verifikasi). Setelah client membuka URL yang diberikan, maka akan langsung diarahkan ke Form Dekripsi dan akan diminta validasi dengan memasukkan private key yang sesuai.

A screenshot of a web form titled "Download Invoice". The form has a light blue background and a white border. It contains five input fields for "Kode Verifikasi" with values 17, 37, 91, 43, and 47. Below the fields is a red button labeled "Download Invoice".

Gambar 9. Form Dekripsi

7. Tampilan Invoice

Jika seluruh proses berhasil maka aplikasi akan menampilkan invoice dalam bentuk PDF yang berisikan data yang asli (plaintext).



Gambar 10. Tampilan Invoice

4. KESIMPULAN

Berdasarkan hasil pengujian sistem, Algoritma RSA – CRT dapat diterapkan untuk mengamankan data invoice pada CV. Ard Pro. dengan cara mengubah isi datanya menjadi sebuah bilangan. Hal ini disebabkan Algoritma RSA-CRT merupakan Algoritma kunci asimetris yang baik digunakan pada sistem yang memiliki dua jenis user karena mempunyai kunci yang berbeda. Selain itu, implementasi sistem berbasis website cocok digunakan pada sistem yang memiliki dua jenis user karena lebih mudah client untuk menjalankan program. Oleh karena sistem ini berhasil menjawab kebutuhan keamanan pada CV. Ard Pro, maka sangat besar kemungkinan aplikasi serupa dapat pula diterapkan di perusahaan lain sesuai kebutuhan penggunaan.

DAFTAR PUSTAKA

- [1] L. Lutfiana, "LKP: Pembuatan Aplikasi Invoice Berbasis Microsoft Access pada PT. Kamajaya Poetra Abadi," 2020, [Online]. Available: <http://repository.dinamika.ac.id/id/eprint/4881/>.
- [2] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan FileDokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016, doi:10.30872/jim.v10i1.23.
- [3] J. K. T. Ivan Wibowo, Budi Susanto, "Penerapan Algoritma Kriptografi Asimetris Rsa Untuk Keamanan Data Di Oracle," *J. Inform.*, vol. 5, no. 2, pp. 1689–1699, 2019, [Online]. Available: <http://labti.ukdw.ac.id/ojs/index.php/informatika/article/viewFile/68/32%0> Ahttp://e-jurnal.pelitanusantara.ac.id/index.php/mantik/article/view/253.
- [4] A. Arief and R. Saputra, "Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging," *Sci. J. Informatics*, vol. 3, no. 1, pp. 46–54, 2016, doi: 10.15294/sji.v3i1.6115.
- [5] E. Malays and S. Sakti, "Pengembangan Fitur Invoice Pada Aplikasi Jasa Titip Berbasis Android," vol. 22, no. 2, pp. 35–39, 2021.
- [6] E. Cahyo Prabowo and I. Afrianto, "Penerapan Digital Signature Dan Kriptografi Pada Otentikasi Sertifikat Tanah

- Digital - Teknik Informatika Universitas Komputer Indonesia,” J. Ilm. Komput. dan Inform., vol. 6, no. 2, 2017.
- [7] M. Y. Simargolang, “Implementasi Kriptografi RSA Dengan PHP,” vol. 1, pp. 1–10, 2017.
- [8] N. Zaatsiyah and U. N. Semarang, “Implementing Digital Signature With RSA And MD5 In Securing E-Invoice Document,” vol. 5, pp. 129–140, 2021.
- [9] J. Simarmata, Sriadhi, and R. Rahim, Kriptografi Teknik Keamanan Data & Informasi, 1st ed. Yogyakarta: Andi, 2019.
- [10] R. Munir, “Kriptografi,” Informatika, 2019.
- [11] M. K. Harahap, “Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad,” InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan), vol. 1, no. 1, pp. 61–64, 2016, doi: 10.30743/infotekjar.v1i1.43.
- [12] Sumandri, “Studi Model Algoritma Kriptografi Klasik dan Modern,” Semin. Mat. dan Pendidik. Mat. UNY, pp. 265–272, 2017
- [13] Z. Panjaitan, K. Ibnutama, and M. G. Suryanata, “Penggunaan Chinese Remainder Theorem (CRT) pada Algoritma RSA,” J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer), vol. 18, no. 1, p. 41, 2019, doi: 10.53513/jis.v18i1.102.
- [14] A. Suprianto and A. A. F. Matsea, “Rancang Bangun Aplikasi Pendaftaran Pasien Online Dan Pemeriksaan Dokter Di Klinik Pengobatan Berbasis Web,” J. Rekayasa Inf., vol. 7, no. 1, pp. 48–58, 2018.
- [15] P. Informatika, B. Darma, G. L. Ginting, and L. Teori, “Perancangan Aplikasi Pembelajaran Cascading Style Sheets Dengan Metode Computer Based Intruction,” vol. III, no. May, pp. 15–22, 2013
- [16] F. A. Prabowo, “Sistem Informasi Pengolahan Sertifikat Berbasis Web Di Divisi Training SEAMOLEC,” J. Masy. Inform. Indones., vol. 2, no. 1, pp. 82–91, 2017.
- [17] M. K. Taryana Suryana, “Fungsi Web Browser Memilih Aplikasi Editor HTML Text Editor Notepad ++,” Repository.Unikom.Ac.Id, pp. 1–9, 2020, [Online]. Available: [https://repository.unikom.ac.id/68227/1/Materi 1 Pengenalan HTML.pdf](https://repository.unikom.ac.id/68227/1/Materi%201%20Pengenalan%20HTML.pdf).