Terbit *online* pada laman web jurnal: http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI DALAM PENYANDIAN PESAN WHATSAPP

Krisma Budi Ziliwu[1], Andi Maslan[2], Hendri Kremer

[1]Mahasiswa Program Studi Teknik Informatika, Unirversitas Putera Batam
[2]Dosen Program Studi Teknik Informatika, Universitas Putera Batam
[3]Dosen Program Studi Data Komunikasi Visual, Institut Teknologi Batam

Email: pb18021011@upbatam.ac.id

ABSTRACT

Caesar cipher adalah satu salah metode pengamanan pesan dalam ilmu kriptografi. Dalam pengamanan pesan menggunakan caesar cipher setiap karakter akan ditukarkan posisinya sehingga makna dari isi pesan susah untuk dimengerti. Tujuan menggunakan caesar cipher untuk mencegah pihak yang tidak berkepentingan mencuri informasi yang bersifat rahasia dalam pesan. Cara mengaplikasi pengamanan pesan pada penelitian ini dengan merancang aplikasi berbasis desktop menggunakan bahasa pemgrograman vb.net. Pengamanan pesan dengan menggunakan algoritma caesar cipher yaitu dengan menukarkan setiap karakter pada pesan asli menjadi cipherteks. Karakter pada plainteks akan disubstitusikan berdasarkan penjumlahan urutan abjad pada plainteks dengan kunci yang telah ditentukan. Proses pengamanan pada caesar cipher disebut enkripsi sedangkan proses mengubah kembali pesan tersandi menjadi plainteks disebut deskripsi. Kegiatan deskripsi dilakukan dengan cara mengurangkan urutan setiap abjad dengan kunci yang digunakan saat melakukan enkripsi. Pengamanan pesan menggunakan caesar cipher mampu mengamankan isi pesan dengan cara menyamarkan isi pesan atau mengubah bentuk isi pesan asli dengan bentuk yang lain sehingga susah untuk dimengerti oleh pihak yang tidak bertanggung jawab. Keamanan yang bisa didapatkan berupa kerahasiaan, keaslian isi pesan dan juga anti penyangkalan.

Keywords: *Cryptography; message; symmetric key; subtitution, caesar cipher.*

PENDAHULUAN

Akhir-akhir ini, kemajuan teknologi dan pengetahuan semakin berkembang ditandai dengan banyaknya perubahan dari hari ke hari, khususnya pada aspek penyampaian pesan. Penyampaian pesan bisa dilakukan dengan berbagai cara, bisa dengan menyampaikan secara langsung dan juga dengan menggunakan internet. Banyak informasi yang bisa peroleh dari internet dan kadang-kadang informasi rasial bisa juga ditemukan. Dengan mudahnya mengakses internet banyak pihak yang merasa dirugikan dan juga diuntungkan. Hal ini bisa terjadi disebabkan

Terbit *online* pada laman web jurnal: http://ejournal.upbatam.ac.id/index.php/comasiejournal
Jurnal Comasie
ISSN (Online) 2715-6265

ada pihak yang ingin mencuri informasi dan sengaja memodifikasi isi pesan. Modifikasi adalah serangan yang ditujukan pada aspek privasi dan otentikasi, ini dilakukan oleh pihak yang tidak berwenang untuk mengakses dan mengubah informasi (Novenzo Ihsana and Maslan 2020)

Kerahasian dan keutuhan sebuah pesan yang akan disampaikan menjadi satu aspek yang diharapkan setiap individu dalam melakukan kegiatan pertukaran informasi. Hal ini menjadi tuntutan yang sangat dibutuhkan dalam pekerjaan atau dalam berkehidupan sosial. Untuk menjaga kerahasiaan sebuah informasi, pesan teks di sandikan atau diubah bentuk aslinya dengan menggunakan kriptografi.

Kriptografi juga disebut sebagai ilmu atau seni untuk menjaga keamanan pesan. Pengaplikasian penyandian pesan menggunakan kriptografi bertujuan untuk menghindari isi pesan dimanipulasi oleh orang yang tidak memiliki wewenang selama proses pengiriman pesan. Teknik yang bisa dilakukan untuk melindungi kerahasiaan isi pesan yaitu dengan melakukan perubahan teks asli kebentuk yang lain atau sering disebut enkripsi. Pada kriptografi ada banyak metode yang bisa digunakan dalam penyandian pesan dengan tujuan pesan diubah bentuk artinya serumit mungkin. Pengelompokkan penggunaan kunci saat enkripsi dan deskripsi dibedakan menjadi dua algoritma, pertama pada saat enkripsi dan deskripsi menggunakan kode yang sama dan yang kedua, saat enkripsi dan deskripsi menggunakan kunci yang beda.

Caesar cipher adalah algoritma tertua dalam perkembangan ilmu penyandian pesan, caesar cipher juga dikenal sebagai penyandian yang paling sederahana dalam penanganan keamanan pesan (Hermansa, Umar, and Yudhana 2020). Menyandikan isi pesan dengan teknik subtitusi, dimana setiap karakter pada pesan asli akan digeser posisi masing-masing karaker sehingga menghasilkan bentuk lain yang disebut chiperteks.

KAJIAN TEORI

2.1 Teori Dasar

Kriptografi merupakan salah satu cabang ilmu yang mempelajari tentang teknik perhitungan yang berkaitan dengan masalah keamanan sebuah informasi seperti kerahasiaan, integritas data serta otentikasi (Munir 2019).

Kriptografi merupakan bidang ilmu yang mempelajari tentang bagaimana untuk mengamankan proses pengiriman pesan dengan cara menyandikan karakter-karakter tertentu, penyandian bertujuan agar isi pesan tidak disalahgunakan oleh orang yang tidak berkepentingan (Permana 2018).

Ilmu kriptografi bertujuan memberikan layanan mendasar untuk keamanan pesan bagi pengguna sebagai berikut (Nasution 2019).

1. Kerahasiaan
   Fasilitas yang bertujuan untuk memastikan bahwa isi pesan tidak diketahui oleh orang lain selama proses pengiriman.
2. Integritas data
   Keuntungan yang didapatkan dalam menggunakan teknik kriptografi yaitu menjamin bahwa pesan akan diterima dalam keadaan masih utuh dan belom mengalamai perubahan selama proses pengiriman.
3. Otentikasi

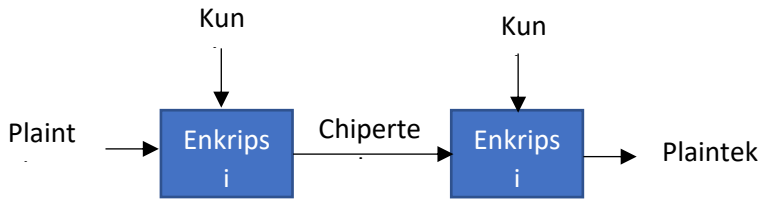
Terbit *online* pada laman web jurnal: http://ejournal.upbatam.ac.id/index.php/comasiejournal
Jurnal Comasie
ISSN (Online) 2715-6265

Fasilitas yang berkaitan untuk melakukan identifikasi terlebih dahulu antara pengirim dan penerima pesan.

4. Anti penyangkalan
   Layanan yang bertujuan menghindari pihak yang berkomunikasi melakukan peyangkalan, yang mana pengirim pesan akan menyangkal telah mengirimkan pesan dan juga sebaliknya penerima pesan tidak mengakui bahwa telah menerima pesan.

4.2Teori Khusus

1. Caesar Chiper
   Caesar cipher dalam ilmu kriptografi adalah metode enkripsi dan deskripsi yang sangat sederhana dan umum. Didalam caesar cipher tiap huruf disubstitusi dengan huruf berikutnya dari susunan alpabet (Munir 2019). Jumlah pergeseran suatu karakter ke karakter lain berdasarkan pada berapa nilai kunci yang dipilih.
2. Pesan teks
   Pesan adalah informasi atau data yang maknanya mudah dimengerti oleh penerima pesan. Dengan kata lain pesan merupakan *clear text* yang belum mengalami penyandian(Mira, Purnomo, and Sembiring 2022).
3. Enkripsi
   Enkripsi adalah proses menggunakan algoritma tertentu untuk mengubah data atau informasi menjadi format yang hampir tidak dapat diidentifikasi sebagai informasi asli. *Plain text* atau teks biasa adalah informasi atau pesan yang dikirim dalam format yang mudah dibaca atau asli (Angriani and Saharaeni 2019).
4. Deskripsi
   Dekripsi adalah kebalikan dari kegiatan enkripsi karena tujuan dari deskripsi mengembalikan pesan yang tersandi atau informasi palsu ke pesan asli. Pada proses mengembalikan isi pesan tersamar harus menggunakan kode yang telah disiapkan sebelumnya. Kegiatan perubahan isi pesan dari *plaintext* ke *ciphertext* disebut enkripsi, dan prosedur mengembalikan teks dari *ciphertext* ke *plaintext* disebut dekripsi (Feraldi et al. 2021)



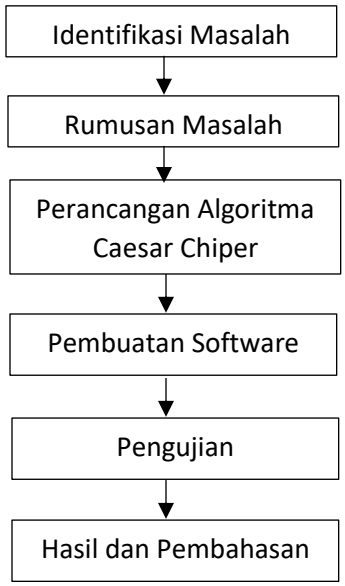
Gambar 1. Diagram enkripsi dan deskripsi

Terbit *online* pada laman web jurnal: http://ejournal.upbatam.ac.id/index.php/comasiejournal
Jurnal Comasie
ISSN (Online) 2715-6265

METODE PENELITIAN

3.1 Desain Penelitian

Desain penelitian adalah keseluruhan kerangka kerja atau pegangan yang digunakan dalam perencanaan dan pelaksanaan penelitian agar penelitian dilakukan secara terstruktur (Mulyadi 2013)



Gambar 2. Desain Penelitian
(Sumber: Data penelitian 2022)

1. Identifikasi Masalah
   Pada tahap identifikasi masalah, penulis ingin mengenali apa yang menjadi permasalah saat ini dalam proses pengiriman pesan. Banyak pihak yang sengaja mencari tahu isi pesan untuk mencuri informasi dan juga untuk mengubah isi yang sesungguhnya. Sangat sedikit pengirim dan penerima pesan menyandikan isi pesan terlebih dahulu.
2. Rumusan Masalah
   Pada tahap perumusan masalah, penulis ingin menggambarkan cara mengamankan pesan dengan menggunakan algoritma caesar chiper. Pesan yang terkirim berupa hasil enkripsi dimana seorang penerima akan melakukan deskripsi dengan kunci yang sama setelah menerima pesan.
3. Perancangan Algoritma Caesar Cipher
   Metode yang digunakan dalam penelitian ini adalah metode substitusi dengan algoritma caesar cipher. Penyandian menggunakan caesar cipher dengan mensubtitusi karatker-karakter pada pesan asli menjadi pesan tersandi dengan menggunakan kunci.
4. Pembuatan Software
   Aplikasi akan dirancang berbasis desktop dengan tampilan yang mudah dimengerti oleh pengguna. Pada perancagan ini akan ada menu seperti *log in*, *log out*, enkripsi dan deskripsi. Pembuatan software menggunakan bahasa pemrograman visual basic.
5. Pengujian
   Pada tahap pengujian penulis akan melakukan pegujian perangkat lunak menggunakan teknik *blackbox testing. Blackbox testing* merupakan cara pengujian yang dilakukan dengan berfokus hasil *input* dan *output* tanpa mengamati struktur kode dari perangkat lunak (Snadhika 2018).
6. Hasil dan Pembahasan
   Pada hasil pembahasan penulis akan melampirkan menu-menu yang ada diaplikasi serta melakukan pengujian yang membuktikan aplikasi penyandian pesan bisa digunakan. Penyandian yang dilakukan hanya untuk pesan teks yang berisikan abjad dar a-z.

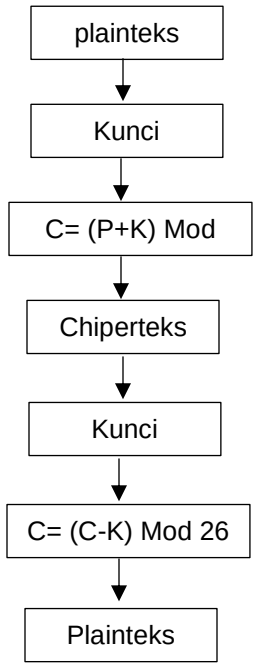
Terbit *online* pada laman web jurnal: http://ejournal.upbatam.ac.id/index.php/comasiejournal
Jurnal Comasie
ISSN (Online) 2715-6265

3.2 Rancang jaringan yang dibangun/ Diusulkan.

Pada perancangan jaringan yang akan diusulkan, penulis menjelaskan tentang flowchart kriptografi caesar chiper, diagram usecase, diagram activity, serta software yang digunakan dalam menjalankan program.

1. Flowchart caesar chiper

   Flowchart enkripsi dan deskripsi bertujuan untuk menggambarkan urutan kegiatan dalam mengamankan isi pesan.

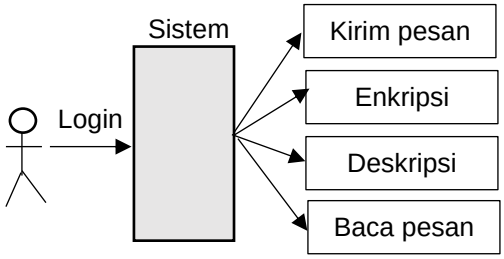


Gambar 3. Flowchart caesar cipher
(Sumber: Data penelitian 2022)

Urutan kegiatan yang dilakukan dalam penyandian isi pesan dengan menggunakan algoritma caesar cipher dimulai dengan menyiapkan pesan asli serta kunci atau kode dalam penyandian. Setiap karatker pada pesan asli akan digeserkan posisi dengan cara menjumlahkan urutan karakter yang akan digeser dengan nilai kunci yang telah disiapkan. Setelah semua karakter digeserkan maka akan menghasilkan cipherteks yang maknanya susah dipahami oleh pihak yang tidak memiliki kunci. Untuk mengembalikan isi pesan asli, penerima pesan harus memiliki kunci yang sama saat melakukan enkripsi. Proses deskripsi yaitu menggeserkan posisi setiap karakter pada cipherteks dengan mengurangi urutan karakter pada abjad dengan nilai kunci yang ada. Setelah setiap karakter pada cipherteks digeserkan maka akan menghasilkan *plaintext.*

2. Diagram usecase

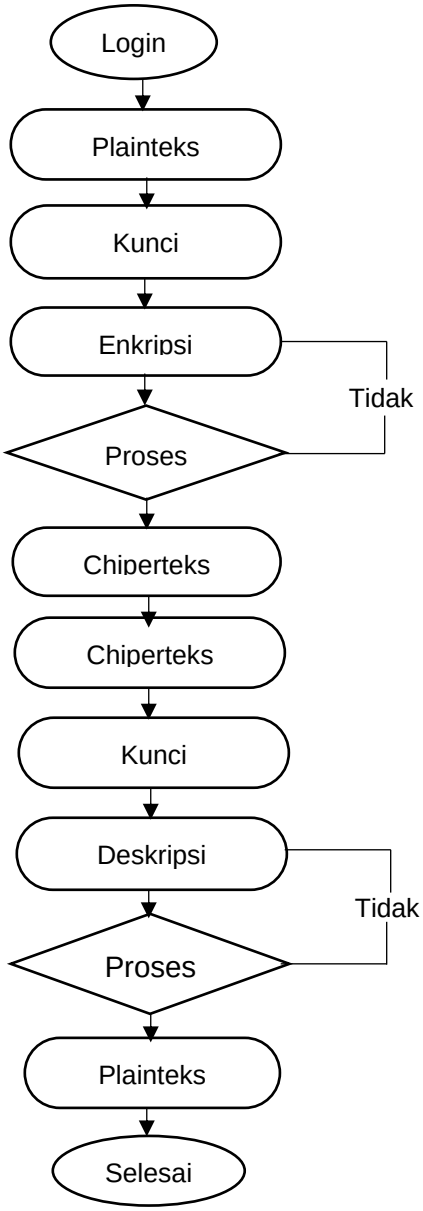
   Use case merupakan sebuah konstruksi untuk menggambarkan hubungan yang terjadi antara aktor dan kegiatan yang terdapat dalam sistem. Kasus penggunaan pemodelan target adalah untuk menentukan kebutuhan fungsional dan operasional sistem dengan menentukan skenario penggunaan sistem yang akan dibangun. Pada diagram use case terdapat beberapa kegiatan yang bisa dilakukan seorang user yaitu melakukan login, kirim pesan, enkripsi, deskripsi dan baca pesan.



Gambar 4. Diagram Usecase

Terbit *online* pada laman web jurnal: http://ejournal.upbatam.ac.id/index.php/comasiejournal
Jurnal Comasie
ISSN (Online) 2715-6265

3. Diagram activity
   Pada diagram activity akan digambarkan proses penggunaan caesar cipher dimulai dari seorang user melakukan otentikasi pada aplikasi penyandian pesan dengan cara melakukan login terlebih dahulu. Selanjutnya akan melakukan enkripsi pesan menjadi cipherteks untuk dikirimkan ke pengguna lain. Seorang penerima pesan harus memiliki kunci yang sama untuk bisa membuka isi dari pesan yang telah diterima. Diagram activity dibagi menjadi dua proses, yaitu kegiatan saat melakukan proses enkripsi dan proses melakukan deskripsi. Tahap awal melakukan enkripsi pengguna melakukan login terlebih dahulu kemudian mempersiapkan plainteks lalu menyandikan dengan menggunakan kunci yang telah disiapkan sehingga menghasilkan cipherteks. Tahap berikutnya saat melakukan deskripsi seorang pengguna harus memiliki kunci atau kode, dimana pesan tersandi diubah kembali menjadi planteks. Setelah pesan tersandi menjadi plainteks maka kegiatan caesar cipher selesai.



Gambar 5. Diagram activity
(Sumber: Data penelitian 2022)

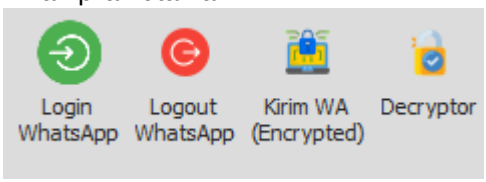
Terbit *online* pada laman web jurnal: http://ejournal.upbatam.ac.id/index.php/comasiejournal
Jurnal Comasie
ISSN (Online) 2715-6265

HASIL DAN PEMBAHASAN

4.1 Hasil

Hasil penelitian yang akan dibahas adalah hasil enkripsi dan deskripsi menggunakan aplikasi penyandian pesan yang telah dibuat. Pada halaman utama ada beberapa menu antara lain: Login, log out, kirim wa (Encrypted) dan descryptor.

1. Tampilan utama

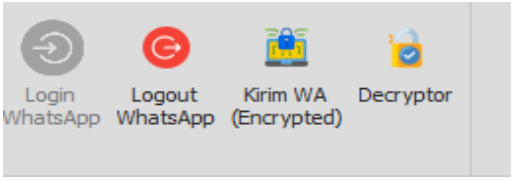


Gambar 6. Halaman utama
(Sumber: Data penelitian 2022)

2. Tampilan login
   Saat memilih login, seorang user akan diarahkan untuk melakukan scan qrcode.

Gambar 7. Halaman utama
(Sumber: Data penelitian 2022)

3. Tampilan log out
   Setelah masuk, menu login tidak aktif, jika seorang ingin keluar dari aplikasi pilih menu log out.

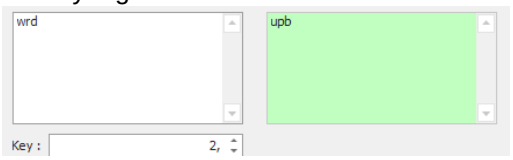


Gambar 8. Halaman utama
(Sumber: Data penelitian 2022)

4. Tampilan Kirim pesan
   Pada tampilan kirim pesan, seorang user akan mempersipkan kunci enkrispi dan juga kepada siapa pesan akan dikirim.

Gambar 9. Halaman utama
(Sumber: Data penelitian 2022)

5. Tampilan Deskripsi
   Untuk membaca isi pesan, seorang pengguna harus mengembalikan isi pesan tersandi dengan menggunakan kunci yang sama.



Gambar 10. Halaman utama
(Sumber: Data penelitian 2022)

4.2 Pengujian Perangkat lunak

1. Pengujian caesar chiper
   Pengujian caesar chiper dilakukan dengan cara mengitung manual dan

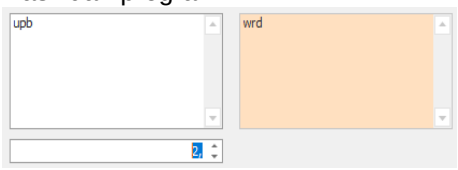
Terbit *online* pada laman web jurnal: http://ejournal.upbatam.ac.id/index.php/comasiejournal
Jurnal Comasie
ISSN (Online) 2715-6265

juga menggunaka aplikasi yang telah dirancang.

Perhitungan manual enkripsi, dengan cara menjumlahkan posisi karakter plainteks dengan kata kunci.

Plainteks: upb
Kunci: 2
Chiperteks: wrd
Mencari (u)
C=(P+K) Mod 26
C= (21+2) Mod 26
C= 23
C= w
Mencari (p)
C=(P+K) Mod 26
C= (16+2) Mod 26
C= 28
C= r
Mencari (b)
C=(P+K) Mod 26
C= (2+2) Mod 26
C= 4
C= d

Hasil dari program

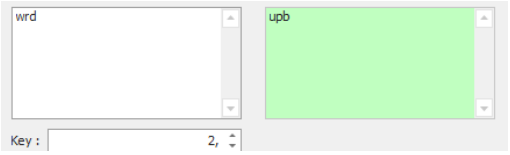


Gambar 11. Halaman utama
(Sumber: Data penelitian 2022)

Untuk melakukan deskripsi menggeserkan posisi karakter dengan mengurangi karakter chiperteks dengan kunci yang sama.

Chiperteks: wrd
Kunci: 2
Plainteks: wrd
Mencari (w)
P=(C-K) Mod 26
P= (23-2) Mod 26
P= 21
P= u
Mencari (r)
P=(C-K) Mod 26
P= (182+2) Mod 26
P= 16
P= p
Mencari (d)
P=(P+K) Mod 26
P= (4+2) Mod 26
P= 2
P= b

Hasil dari program



Gambar 12. Halaman utama
(Sumber: Data penelitian 2022)

Pengujian aplikasi dengan menggunakan metode blackbox testing.

Hasil pengujian

No	Pengujian	Aktivitas	Status
1	Login	Scan qrcode	Sukses
2	Kirim pesan	Pilih menu kirim	Sukses
3	Enkripsi	Pilih menu enkripsi	Sukses
4	Deskripsi	Pilih menu deskripsi	Sukses
5	Logout	Pilih menu Log out	Sukses

Tabel 1. Black box testing
(Sumber: Data penelitian 2022)

KESIMPULAN

Proses enkripsi dan deskripsi teks pesan dengan menggunakan algoritma teknik chiper berhasil dilakukan. Sehingga dapat diasumsikan bahwa penyandian pesan dengan algoritma caesar chiper dapat menjaga kerahasiaan isi pesan.

Terbit *online* pada laman web jurnal: http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

DAFTAR PUSTAKA

Angriani, Husni, and Yeni Saharaeni. 2019. "Implementasi Algoritma Caesar Cipher Pada Keamanan Data Sistem E-Voting Pemilihan Ketua Organisasi Kemahasiswaan." *Inspiration: Jurnal Teknologi Informasi Dan Komunikasi* 9(2):123. doi: 10.35585/inspir.v9i2.2499.

Feraldi, Riyan, Aida Khairuna, Mhd Arief Hasan, Rafael Rezky, Hardiansyah Ramadhan, Program Studi, Teknik Informatika, Fakultas Ilmu, Komputer Universitas, and Lancang Kuning. 2021. "Kombinasi Algoritma Kriftografi Caesar Cipher Dan." *Riau Journal of Empowerment* 7(01):76–86.

Hermansa, Rusydi Umar, and Anton Yudhana. 2020. "Pangamanan Pesan

Menggunakan Kriptografi." *Jurnal Sains Komputer & Matematika* Vol 4:1–13.

Mira, Hindriyanto Dwi Purnomo, and Irwan Sembiring. 2022. "Modifikasi Algoritma Caesar Cipher Pada Kode ASCII Dalam Meningkatkan Keamanan Pesan Teks." *Journal of Information Technology* 2(1):16–22. doi: 10.46229/jifotech.v2i1.293.

Mulyadi, Mohammad. 2013. "Riset Desain Dalam Metodologi Penelitian." *Jurnal Studi Komunikasi Dan Media* 16(1):71. doi: 10.31445/jskm.2012.160106.Munir, Rinaldi. 2019. *Kriptografi*. Kedua. edited by R. Munir. Bandung: Informatika Bandung.

Nasution, Adnan Buyung. 2019. "Implementasi Pengamanan Data Dengan Menggunakan." 3(1):1–6.

Novenzo Ihsana, Angga, and Andi Maslan. 2020. "Analisis Keamanan Jaringan Dari Serangan Paket Data Sniffing Di Pt Raden Syaid Kantor Pos Piayu Kota Batam." *Jurnal Comasie* 05.

Permana, Angga Aditya. 2018. "Penerapan Kriptografi Pada Teks Pesan Dengan Menggunakan Metode Vigenere Cipher Berbasis Android." *JURNAL AI-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI* 4(3):110. doi: 10.36722/sst.v4i3.280.

Snadhika, Tri Jaya. 2018. "Pengujian Aplikasi Dengan Metode Blackbox Testing Boundary Value Analysis (Studi Kasus: Kantor Digital Politeknik Negeri Lampung)." *Jurnal Informatika: Jurnal Pengembangan IT (JPIT)* 03(02):45–48. doi: 10.30591/jpit.v3i1.647.

Biodata Penulis

	Biodata[1] Penulis pertama, Krisma Budi Ziliwu merupakan mahasiswa prodi teknik informatika Universitas Putera Batam
	Biodata[2] Penulis kedua, Andi Maslan, S.T., M.SI merupakan Dosen Prodi Teknik Informatika Universitas Putera Batam
	Biodata[3] Hendri Kremer, merupakan dosen di Program Studi Data Kumunikasi Visual ITEBA Batam, dan juga sebagai wartawan di Media Indonesia.