IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN

SKRIPSI

Oleh

Krisma Budi Ziliwu

180210119

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK & KOMPUTER
UNIVERSITAS PUTERA BATAM
2022

IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN

SKRIPSI

Untuk memenuhi salah satu syarat
memperoleh gelar Sarjana

Oleh

Krisma Budi Ziliwu

180210119

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK & KOMPUTER
UNIVERSITAS PUTERA BATAM

2022

SURAT PERYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya:

Nama : Krisma Budi Ziliwu

NPM : 180210119

Fakultas : Teknik dan Komputer

Program Studi : Teknik Informatika

Menyatakan bahwa "**Skripsi**" yang saya buat dengan judul:

IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN

Adalah hasil karya sendiri dan bukan "duplikasi" dari karya orang lain. Sepengetahuan saya, di dalam naskah Skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah Skripsi ini digugurkan dan gelar akademik yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun.

Batam, 08 Agustus 2022

Krisma Budi Ziliwu

180210119

IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN

SKRIPSI

Untuk memenuhi salah satu syarat
memperoleh gelar Sarjana

Oleh

Krisma Budi Ziliwu

180210119

Telah disetujui oleh Pembimbing pada tanggal
seperti tertera di bawah ini

Batam, 08 Agustus 2022

Andi Maslan, S.T., M.SI

Pembimbing

UPB

Universitas Putera Batam

ABSTRAK

Kejahatan *cyber* menjadi hal yang sangat dikhawatirkan oleh pengguna jaringan internet dalam berkomunikasi. Oleh karena itu, setiap pesan yang akan dikirimkan harus diamankan dengan teknik kriptografi. 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.

Kata kunci: Kejahatan *cyber*; Caesar cipher; Kriptografi; Keamanan; Pesan

ABSTRACT

Cyber crime is a matter of great concern for internet network users in communicating. Therefore, every message to be sent must be secured with cryptographic techniques. Caesar cipher is a method of securing messages in cryptography. In securing messages using Caesar cipher, each character will be exchanged in position so that the meaning of the message content is difficult to understand. The purpose of using caesar cipher is to prevent unauthorized parties from stealing confidential information in messages. How to apply message security in this study by designing a desktop-based application using the vb.net programming language. Message security using the Caesar cipher algorithm is by exchanging each character in the original message into ciphertext. The characters in the plaintext will be substituted based on the sum of the alphabetical order in the plaintext with a predetermined key. The process of securing the Caesar cipher is called encryption while the process of converting the encrypted message back into plaintext is called description. The description activity is carried out by subtracting the order of each alphabet with the key used when encrypting. Securing messages using Caesar cipher is able to secure the contents of the message by disguising the content of the message or changing the form of the original message in another form so that it is difficult for irresponsible parties to understand. Security that can be obtained in the form of confidentiality, authenticity of the message content and also anti-denial.

Keywords**:** *Cyber crime*; C*aesar cipher; Criptography; Security, Message*

UPB

Universitas Putera Batam

KATA PENGANTAR

Puji Tuhan kami ucapkan syukur karena telah dengan baik memberikan keberkahan kepada penulis sehingga bisa menyelesaikan tugas akhir yang menjadi syarat utama untuk menyelesaikan progras studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis sadar bahwa penulisan skripsi ini sangat sederhana dan jauh dari kata sempurna. Oleh sebab itu kritik dan saran akan selalu penulis menerimanya dengan senang hati. Dengan segala keterbasan, penulis menyadari bahwa skripsi ini tidak akan terselesaikan tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, segala kerendahan hati, penulis menyampaikan terima kasih kepada:

1. Ibu Dr. Nur Elfi Husda, S.Kom., M.SI. selaku Rektor Universitas Putera Batam;
2. Bapak Welly Sugianto, S.T., M.M. selaku Dekan Fakultas Teknik dan Komputer;
3. Bapak Andi Maslan, S.T., M.SI. selaku Ketua Program Studi Teknik Informatika dan juga selaku pembimbing skripsi penulis;
4. Bapak Koko Handoko, S.Kom., M.Kom. Selaku pembimbing Akademik pada Program Studi Teknik Informatika Universitas Putera Batam;
5. Dosen dan Staff Universitas Putera Batam;
6. Orang tua dan adik kandung penulis yang memberikan dukungan dan doa agar penulis dapat menyelesaikan skripsi ini;
7. Istri tercinta yang selalu memberi dukungan dan doa agar penulis dapat menyelesaikan skripsi ini;
8. Dan teman-teman seperjuangan yang tidak bisa penulis sebutkan semuanya terimakasih untuk saran dan dukungannya;

Kiranya Tuhan saja yang membalas kebaikan setiap orang yang telah membantu penulis dan semoga skripsi ini dapat memberikan manfaat untuk penulis maupun setiap orang membutuhkan.

Batam, 08 September 2022

KRISMA BUDI ZILIWU

Daftar Isi

ABSTRAK i
ABSTRACT ii
KATA PENGANTAR iii
Daftar Gambar vi
Daftar Tabel vii
BAB I PENDAHULUAN 1
1.1 Latar Belakang **1**
1.2 Identifikasi Masalah **3**
1.3 Batasan Masalah **4**
1.4 Rumusan Masalah **4**
1.5 Tujuan Penelitian **4**
1.6 Manfaat Penelitian **4**
BAB 2 TINJAUAN PUSTAKA 5
2.1 Teori Dasar 5
2.1.1 Sejarah Kriptografi 5
2.1.2 Unsur Dalam Kriptografi 7
2.1.3 Tujuan Kriptografi 10
2.1.4 Jenis Jenis Kriptografi 11
2.1.5 Fungsi Hash 13
2.2 Algoritma *Caesar Cipher* 14
2.3 Perancangan Sistem 14
2.3.1 VB.net 15
2.3.2 Node.js 15
2.3.3 Unified modelling language (UML) 16
2.3.4 Flowchart 18
2.4 Pengujian Aplikasi Penyadian Pesan 21
2.5 Penelitian Terdahulu 21
2.6 Kerangka Pemikiran 24
BAB III METODE PENELITIAN 26
3.1 Desain Penelitian 26
3.2 Teknik Pengumpulan Data 28
3.3 Pemodelan Fungsional 28
3.3.1 Flowchart caesar cipher *29*
3.3.2 Diagram Use Case *30*

3.3.3 Diagram Activity ***31***
3.4 Perancangan Interface 33
3.4.1 Halaman Utama *33*
3.4.2 Menu Login *34*
3.4.3 Menu log out *34*
3.4.4 Menu Enkripsi *35*
3.4.5 Menu Deskripsi *35*
3.5 Perancangan algoritma *caesar cipher* 36
3.6 Implementasi 41
3.7 Pengujian 42
3.8 Jadwal Penelitian 42
BAB IV HASIL DAN PEMBAHASAN 43
4.1 Hasil Penelitian 43
4.1.1 Halaman Utama 43
4.1.2 Menu Login 44
4.1.3 Menu Log Out 44
4.1.4 Menu Kirim Wa (Encrypted) 45
4.1.5 Menu Decryptor 45
4.2 Pembahasan 46
4.2.1 Implementasi Pengamanan Pesan dengan Algoritma Caesar Cipher 47
4.2.2 Pengujian Fungsional Sistem Dengan Blackboxs Testing 48
4.2.3 Pengujian enkripsi dan deskripsi 48
BAB V KESIMPULAN 52
5.1 Kesimpulan 52
5.2 Saran 52
Daftar Pustaka 53
Lampiran 56
Lampiran 1. Pendukung Penelitian 56
Lampiran 2. Daftar Riwayat Hidup 58
Lampiran 3. Turnitin Skripsi 59
Lampiran 4. Turnitin Jurnal 60
Lampiran 5. Surat Keterangan Penelitian 61

Daftar Gambar

Gambar 2. 1 Diagaram Enkripsi dan Deskripsi 8
Gambar 2. 2 Sistem Kriptografi Simetri 12
Gambar 2. 3 Sistem kriptografi nirsimetri 13
Gambar 2. 4 Simbol *usecase diagram* 17
Gambar 2. 5 Simbol activity diagram 18
Gambar 2. 6 Bagian penting flowchart 19
Gambar 2. 7 Simbol Flowchart 20
Gambar 2. 8 Kerangka pemikiran 24
Gambar 3. 1 Desain Penelitian 26
Gambar 3. 2 Flowchart Caesar Cipher 29
Gambar 3. 3 Diagram Usecase 30
Gambar 3. 4 Diagaram aktivity Enkripsi pesan 31
Gambar 3. 5 Diagram Activity Enkripsi Pesan 32
Gambar 3. 6 Halaman Utama 33
Gambar 3. 7 Menu Login 34
Gambar 3. 8 Menu Logout 34
Gambar 3. 9 Menu Enkripsi 35
Gambar 3. 10 Menu Deskripsi 35
Gambar 3. 11 Arsitektur Aplikasi 41
Gambar 4. 1 Halaman Utama 43
Gambar 4. 2 QR Code 44
Gambar 4. 3 Menu Log Out 44
Gambar 4. 4 Menu Kirim Wa 45
Gambar 4. 5 Menu Decryptor 46
Gambar 4. 6 Enkripsi kunci 1 49
Gambar 4. 7 Enkripsi Kunci 2 49
Gambar 4. 8 Enkripsi Kunci 3 50
Gambar 4. 9 Deskripsi Kunci 1 50
Gambar 4. 10 Enkrispi Kunci 2 51
Gambar 4. 11 Deskripsi Kunci 3 51

Daftar Tabel

Tabel 3. 1 Plainteks 37
Tabel 3. 2 Cipherteks 38
Tabel 3. 3 Baris plainteks 38
Tabel 3. 4 Baris Cipherteks 38
Tabel 3. 5 Jadwal Penelitian 42
Tabel 4. 1 Pengujian Fungsional 48
Tabel 4. 2 Pengujian Enkripsi 48
Tabel 4. 3 Pengujian Deskripsi 49

UPB

Universitas Putera Batam

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi sekarang ini mengalami peningkatan yang sangat signifikan bagi kehidupan manusia. Perkembangan teknologi informasi memudahkan pengguna untuk menyelesaikan setiap aktifitas dengan cara-cara yang lebih praktis, seperti kegiatan dalam melakukan komunikasi antar satu dengan yang dibatasi oleh jarak dan juga berupa aktifitas untuk mengetahui informasi penting secara real time. Pesatnya perkembangan teknologi informasi diberbagai bidang tak terlepas dari manfaatnya untuk membuat, menyimpan dan menyebarkan informasi. Manfaat teknologi informasi tidak hanya penting dalam dunia telekomunikasi namun bisa dirasakan dari berbagai bidang seperti bidang kesehatan, bidang bisnis, bidang pendidikan dan bidang perbankan.

Penggunaan teknologi informasi memiliki dampak yang positif dan juga negatif bagi manusia, tergantung cara individu dalam memanfaatkan teknologi yang ada. Sisi positif yaitu kemudahan mengakses informasi, memudahkan dalam komunikasi, memperbanyak relasi melalui media sosial dan mampu membantu menyelesaikan permasalahan dengan mudah. Namun penggunaan teknologi informasi yang semakin canggih memiliki dampak negatif seperti bagi kehidupan manusia diantaranya; konten negative sangat mudah diakses serta bisa diakses oleh siapapun dan dimanapun, malas bersosialisasi secara fisik, meningkatkanya penipuan dan munculnya kejahatan *cyber*.

Kemudahan dalam pertukaran informasi dalam sebuah jaringan internet memunculkan berbagai ancaman kejahatan atau *cyber crime* yang membuat informasi bisa diambil dan dimodifikasi tanpa persetujuan dari pihak yang bersangkutan. Ancaman *cyber crime* merupakan sebuah kondisi dan situasi yang dapat dinilai melakukan serangan yang mampu merusak dan merugikan serta mengancam kerahasiaan, integritas dan ketersediaan sistem dan informasi (Rahmawati 2017). Dengan munculnya ancaman kejahatan ini menyebabkan para pengguna internet dalam melakukan komunikasi menjadi lebih waspada untuk mengirimkan informasi yang bersifat rahasia dengan yang lain. Akan tetapi, kebutuhan akan komunikasi memaksa pengguna internet untuk terus menggunakan fasilitas yang ada sehingga memunculkan ide-ide untuk mengamankan pesan agar kerahasiaan pesan yang ingin disampaikan bisa terjaga dan bisa terkirim kepenerima tanpa adanya perubahan isi pesan. Serangan-serangan yang bisa dilakukan dalam pengiriman pesan bisa berupa *interception* yaitu serangan yang ditujukan pada aspek privasi yang mana pihak yang tidak berwenang dapat mengakses informasi dan serangan lain berupa *modification* yaitu serangan di bertujuan untuk memodifikasi isi pesan (Novenzo Ihsana and Maslan 2020).

Kerahasiaan dan keamanan suatu informasi yang akan dikirim sehingga bisa sampai kepenerima yang telah ditentukan merupakan aspek yang sangat penting. Untuk mendukung keamanan data dan kerahasiaanya digunakan teknik kriptografi. Teknik ini dilakukan agar pesan yang akan di kirim tidak diketahui oleh orang lain dan hanya bisa diakses oleh pengguna yang telah ditentukan. Kriptografi adalah ilmu dan seni untuk

menjaga pesan dengan cara menyandikan kedalam bentuk yang tidak dapat dimengerti lagi maknanya (Munir 2019).

Teknik kriptografi yang diaplikasikan dalam keamanan pesan atau informasi pada pembahasan ini adalah menggunakan algoritma *caesar cipher*. *Caesar cipher* adalah teknik enkripsi di mana setiap karakter dalam pesan terenkripsi diganti sebagai kunci dengan menggeser urutannya. Misalnya, setiap huruf diganti dengan huruf ketiga yang paling dekat dengan alfabet. Tujuan kriptografi untuk mendapatkan keutuhan, kerahasiaan dan keaslian dari sumber informasi yang telah disampaikan oleh pengirim pesan. Pada kriptografi dikenal beberapa istilah antara lain kode disebut *ciphers*, pesan yang disembunyikan disebut plain text, pesan yang akan diubah bentuk sehingga orang lain tidak mengerti maknanya disebut *ciphertext*. Proses yang dilakukan dalam mengubah isi dari pesan disebut enkripsi, sementara untuk mengembalikan makna dari pesan yang diterima disebut deskripsi. Untuk menjamin kerahasian dan keutuhan dari pesan yang akan disampaikan maka penulis tertarik untuk mengangkat pembahasan dengan judul "**Implementasi *caesar cipher* pada algoritma kriptografi klasik dalam penyandian pesan**"

1.2 Identifikasi Masalah

Pada penelitian ini, penulis akan mengidentifikasi permasalahan yang menjadi masalah utama yaitu:

1. Isi pesan yang hendak disampaikan bisa disalahgunakan.
2. Bisa diketahui isi pesan oleh pihak yang tidak berkepentingan

3. Isi pesan bisa dimodifikasi sehingga berbeda dengan tujuan pesan yang sesungguhnya.

1.3 Batasan Masalah

Berdasarkan latar belakang diatas, maka perlu dibatasi pembahasan pada skripsi antara lain:

1. Melakukan enkripsi dan deskripsi pada pesan yang berisikan huruf
2. Melakukan enkripsi dan deskripsi menggunakan algoritma *caesar cipher*.

1.4 Rumusan Masalah

Bagaimana cara mengimplementasikan pengamanan pesan menggunakan algoritma *caesar cipher*

1.5 Tujuan Penelitian

Untuk merancang sistem pengamanan pada proses pengiriman pesan menggunakan algoritma *caesar cipher*

1.6 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini adalah:

1. Meningkatkan pengetahuan tentang proses penyandian teks menggunakan *caesar cipher*
2. Meningkatkan pengetahuan dalam mengembalikan isi pesan yang telah disandikan.
3. Dapat menjadi bahan referensi dalam menambah pengetahuan untuk melakukan penelitian pada masa selanjutnya.

UPB

Universitas Putera Batam

BAB 2

TINJAUAN PUSTAKA

2.1 Teori Dasar

Kriptografi merupakan pengetahuan pada suatu bidang ilmu yang mempelajari tentang kaidah-kaidah matematika yang berkaitan tentang bagaimana mengonversi pesan asli ke kebentuk yang lain sehingga maksud dari isi pesan tidak mudah dipahami. Tujuan melakukan penyamaran arti yang sebenarnya dari sebuah pesan untuk mengamankan informasi seperti kerahasiaan, keutuhan serta otentikasi pesan (Munir 2019). Pengamanan pesan dilakukan agar informasi yang bersifat rahasia tidak disalah gunakan oleh orang yang tidak memiliki hak atas pesan tersebut. Pada kriptografi terdapat proses penting dalam pengamanan pesan seperti deskripsi dan deskripsi. Enkripsi adalah proses mengubah pesan asli menjadi pesan tersamar yang tidak mudah dipahami artinya sedangkan deskripsi merupakan sebuah proses mengubah kembali isi pesan yang telah disandikan menjadi pesan asli sehingga mudan dibaca dan dipahami artinya. Dalam kripografi penjagaan isi pesan asli ditujukan pada orang yang memiliki niat buruk seperti penyusup, pengacau, lawan dan juga dari penyerang (Janner, Sriadhi, and Robbi 2019).

2.1.1 Sejarah Kriptografi

Perkembangan ilmu kriptografi memiliki sejarah yang panjang dan menarik, dimulai dari pada tahun sebelum masehi sampai pada zaman modern sekarang ini. Penyamaran isi pesan sudah lama dimanfaatkan oleh bangsa Mesir kuno, Cina, Romawi dan Yunani. Kriptografi yang pertama kali digunakan menggunakan metode kriptografi

klasik dengan melakukan substitusi atau dengan cara mengubah susunan setiap karakter dalam pesan. Teknik-teknik pengubahan isi pesan semakin banyak dikarenakan banyak pihak-pihak yang berkontribusi didalamnya seperti kelompok militer, kelompok diplomat, penulis buku harian dan juga kaum pecinta.

Sejarah kriptografi pada Zaman Mesir kuno dibuktikan dengan temuan tulisan pada sebuah prasasti makam bangsawan dengan menggunakan *hieroglyph* (aksara mesir kuno) yang tidak standard. Untuk perkembangan kriptografi pada zaman Yunani dan Romawi kuno digunakan oleh para tentara Sparta pada permulaan tahun 400 SM bertujuan untuk mengacak pesan yang bernama *scytale. Scytale* terbuat dari sebua kertas panjang yang terbuat dari daun papyrus kemudian dililitkan pada sebuah silider kayu berdiameter tertentu. Penulisan dilakukan dengan cara horizontal dari bari ke baris. Untuk bisa membaca isi pesan penerima harus melilitkan kesebuah silinder yang berdiameter sama saat menulis pesan. Algoritma yang digunakan yaitu dengan substitusi sederhana. Perkembangan kriptografi di India kuno digunakan oleh pecinta (*lovers)* untuk berkomunikasi tanpa diketahui orang, teknik kriptografi yang digunakan yaitu dengan cara substitusi. Perkembagan ilmu kriptografi dari zaman kezaman semakin banyak cara yang bisa dilakukan dalam penyandian pesan seperti trasnposisi, substitusi, penambahan atau reduksi jumlah huruf, penggunaan piranti sandi, penggantian huruf dengan angka dan penggunaan simbol. Perkembangan ini ditemukan pada kriptografi bangsa arab sekitar abad 9 hingga 15 masehi. Penyandian juga ditemukan pada masa perang dunia II, yang mana pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan *Enigma.*

Mesin ini menggunakan beberapa roda berputar yang mampu melakukan enkripsi dengan cara yang sangat rumit (Munir 2019).

2.1.2 Unsur Dalam Kriptografi

Didalam ilmu kriptografi ada beberapa unsur penting antara lain (Munir 2019);

1. Pesan, plainteks dan cipherteks

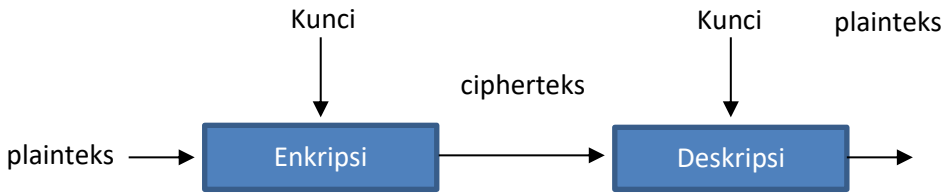
   Pesan (*message*) adalah data atau informasi yang dapat dibaca dan pahami artinya. Pesan dapat berupa teks, citra atau gambar, suara (audio), video atau bentuk-bentuk biner lainnya baik berupa analog maupun digital. Pesan yang menggunakan teks dikenal dengan nama plainteks atau teks yang jelas. Sebuah pesan bisa dikirim dan bisa disimpan, pesan terkirim merupakan informasi yang disampaikan kepenerima dengan media komunikasi sedangkan pesan yang disimpan adalah pesan yang disimpan dalam penyimpan sekunder atau media perekaman. Plainteks merupakan pesan asli yang belum mengalami perubahan makna sedangkan cipherteks merupakan pesan tersandi hasil dari proses penyandian menggunakan enkripsi.

2. Pengirim dan penerima

   Dalam pertukaran informasi untuk menyampaikan pesan akan melibatkan dua entitas. Pengirim (s*ender*) adalah entitas yang mengirim pesan kepada entitas lainnya sedangkan penerima (*receiver*) adalah entitas yang menerima pesan. Dalam hal ini pengirim atau penerima tidak harus berupa manusia, tetapi bisa juga dapat berupa mesin, robot, atau komputer. Dalam pengiriman pesan pihak pengirim dan juga penerima menginginkan isi pesan dalam keadaan aman dan tidak ada perubahan selama proses pengiriman berlangsung.

3. Enkripsi dan deskripsi

Proses menyandikan plainteks menjadi cipherteks disebut enskripsi (encryption) atau enciphering (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan cipherteks menjadi plainteks semula dinamakan deskripsi (descryption) atau deciphering (standard nama menurut ISO 7498 -2). Enkripsi dan juga deskripsi bisa diterapkan pada pesan yang dikirim maupun pada pesan yang tersimpan.



Gambar 2. 1 Diagaram Enkripsi dan Deskripsi

4. *Cipher*, kode dan kunci

Algoritma kriptografi untuk enkripsi dan deskripsi disebut juga *cipher*. *Cipher* dapat diartikan sebagai aturan untuk *enciphering* dan *deciphering*, atau fungsi matematika yang digunakan untuk enskripsi dan deskripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk enciphering atau deciphering. Contoh cipher yang sederhana adalah *caesar cipher* yang aturan enkripsinya dilakukan dengan mengganti sebuah huruf alfabet ke huruf berikutnya. Kunci sering diacu sebagai prosedur yang mengganti setiap plainteks dengan suatu kata kunci. Kunci juga dapat berupa deretan angka dan huruf yang tidak bermakna.

5. Sistem kriptografi

Sistem kriptografi merupakan kumpulan himpunan yang terdiri dari beberapa algoritma seperti enkripsi, algoritma deskripsi, ruang kunci semua plainteks dan cipherteks yang mungkin digunakan. Pada sistem kriptografi dikenal ada dua macam metode penyandian yaitu sistem kriptografi kunci – simetri dan sistem kriptografi kunci publik. Metode penyandian ini digunakan berdasarkan kebutuhan dan dibedakan atas penggunaan kunci yang digunakan dalam penyandian pesan asli.

6. Penyadap

Pengamanan pesan muncul karena adanya penyadap. Penyadap adalah orang yang mencoba menangkap pesan selama proses pengiriman terjadi. Tujuan penyadapan adalah untuk mendapatkan informasi sebanyak-banyaknya yang terdapat dalam sebuah pesan dan juga bisa untuk menipu penerima pesan dengan cara memanipulasi isi pesan yang telah dikirim.

7. Kriptanalisis dan kriptologi

Seiring berkembangnya ilmu kriptografi dalam pengamanan informasi maka melahirkan ilmu baru yang berlawanan dengan tujuan kriptografi yaitu dinamakan kriptanalisis. Kriptanalisis adalah ilmu dan seni untuk memecahkan cipherteks enskripsi-deskripsi. Kriptanalisis berusaha untuk mendapatkan informasi dengan melakukan berbagai teknik sehingga bisa mengembalikan isi pesan dan juga bisa

mengetahui kunci yang digunakan oleh kriptografer saat melakukan proses pengamanan pesan. Orang yang melakukan kriptanalisis disebut kriptanalis. Jika seorang kriptografer mentranformasikan plainteks menjadi cipherteks dengan suatu algoritma dan kunci, maka sebaliknya seorang kriptanalis berusaha memecahkan chipeteks tersebut untuk menemukan plainteks dan kunci.

2.1.3 Tujuan Kriptografi

Ada beberapa tujuan mendasar memanfaatkan ilmu kriptografi dalam pengamanan pesan yaitu (Idayatullah and Insanudin 2016);

1. Kerahasiaan

   Kerahasiaan (*Confiedentiality*), adalah layanan yang bertujuan untuk menjaga isi pesan agar tidak dapat dibaca oleh orang lain selama pengiriman selain dari penerima pesan yang telah ditentukan oleh pengirim yang memiliki kunci atau kode untuk membuka pesan tersandi. Didalam kriptografi layanan ini diimplementsikan dengan cara mengenkripsi pesan menjadi cipherteks.

2. Kelengkapan data

   Kelengkapan (*Data integrity*), adalah layanan berkaitan dengan penjagaan isi pesan agar tidak ada perubahan selama pengiriman berlangsung. Tujuan kriptografi lainnya yaitu menjamin bahwa pesan masih asli/utuh atau belum pernah diubah/manipulasi selama proses pengirimanan. Keutuhan isi pesan selama pengiriman bisa dibuktikan saat peneriman mengubah pesan tersandi dengan cara melakukan deskripsi dengan kunci yang sama sehingga mengembalikan isi pesan yang bisa dimengerti.

3. Otentikasi

Otentikasi (authentication), adalah layanan yang berhubungan dengan identifikasi, yang mengidentifikasikan kebenaran pihak-pihak yang berkomunikasi. Dalam menjaga keaslian data, pihak yang melakukan pertukaran informasi terlebih dahulu melakukan autentikasi terhadap sumber, *server* dan orang yang ingin menggunakan data.

4. Anti penyangkalan

Anti penyangkalan (non-repudiation), adalah layanan untuk mencegah entitas yang berkomunikasi melalukan penyangkalan, yaitu pengirim pesan membantah telah mengirim pesan, atau penerima pesan menyangkal telah menerima pesan.

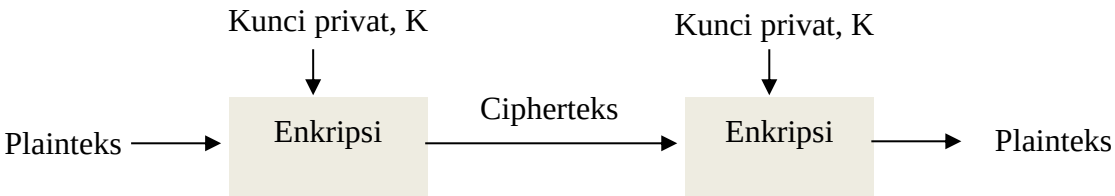
2.1.4 Jenis Jenis Kriptografi

Setiap algoritma kriptografi membutuhkan kunci rahasia untuk melakukan enkripsi dan deskripsi. Kunci rahasia yang digunakan bisa sama dengan kunci saat melakukan enkripsi dengan deskripsi namun ada sebagian yang menggunakan kunci berbeda. Pengelompokan dari penggunaan kunci saat melakukan enskripsi dan deskripsi dapat dikelompokan menjadi kriptografi kunci-simetri dan kriptografi kunci-nirsimeteri. Pada algoritma kriptografi kunci simetri, kunci enkripsi dan deskripsi memiliki kunci rahasia yang sama sedangkan pada algoritma kriptogradi kunci nirsimetri menggunakan kunci yang berbeda saat melakukan enkripsi dan deskripsi pesan.

Didalam kriptografi simetri, keamanan terletak pada kerahasiaan kunci sedangkan algoritmanya sendiri tidak perlu rahasia. Jenis pengamanan pesan seperti ini sudah lama dikenal dalam catatan sejarah hingga tahun 1976. Yang mana semua algoritma kriptografi

klasik termasuk dalam kelompok kriptografi simeteri. Ada juga beberapa algoritma kriptografi modern termasuk kedalam kriptografi simetri seperti: DES (Data encryption standard), blowfish, twofish, triple-des, idea, serpent, mars, rc4, rc5, rc6.

Aplikasi utama kriptografi simetri adalah melindungi kerahasiaan informasi, baik yang ditransmisikan maupun yang tersimpan. Kelemahan dari kriptografi simetri adalah penerima pesan harus memiliki kunci yang sama dengan pengirim pesan, sehingga pengirim pesan harus mencari cara yang aman untuk memberitahu kunci tersebut kepada penerima pesan.

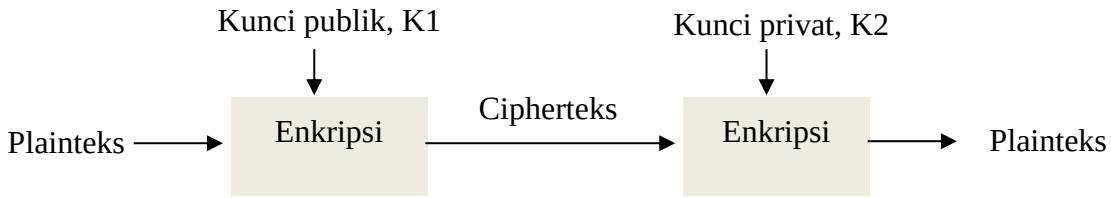


Gambar 2. 2 Sistem Kriptografi Simetri

Pada gambar diatas dijelaskan tentang bagaimana cara melakukan penyandian pesan menggunakan kriptografi simetri atau kunci privat. Dalam penyandian pesan pada saat melakukan enkripsi menggunakan kunci privat ibaratnya K dan untuk mengembalikan isi pesan ke bentuk semula harus menggunakan kunci yang sama yaitu K.

Sedangkan dalam pengamanan pesan menggunakan kunci publik menggunakan cara yang berbeda. Jika kunci enkripsi tidak sama dengan kunci deskripsi maka kriptografinya di sebut kriptografi nirsimetri. Pada kriptografi ini kunci enkripsi tidak rahasia, yaitu diumumkan kepada semua pengguna, sedangkan kunci deskripsi harus dirahasiakan, kegiatan penyandian pesan ini sering disebut sebagai kriptografi kunci

publik. Setiap orang yang berkomunikasi memiliki sepasang kunci, yaitu kunci privat dan kunci publik. Dalam hal ini pengirim melakukan enkripsi dengan kunci publik sipenerima pesan namun untuk melakukan deskripsi hanya penerima yang bisa melakukannya karena cuman dia yang memiliki kunci privatnya (Munir 2019).



Gambar 2. 3 Sistem kriptografi nirsimetri

Pada penyandian menggunakan kriptografi nirsimetri menggunakan dua kunci untuk mengamankan pesan. Untuk kunci enkripsi menggunakan K1 sementara untuk melakukan deskripsi menggunakan kunci K2. Untuk kunci enkripsi semua pengguna boleh mengetahuinya namun untuk kunci deskripsi hanya penerima yang punya otoritas yang memiliki.

2.1.5 Fungsi Hash

Untuk menguji integritas pesan dalam kriptografi disebut dengan fungsi hash. Cara lain untuk mengamankan pesan dalam algoritma kriptografi selain menggunakan kunci simetri dan nirsimetri yaitu dengan menggunakan fungsi hash. Fungsi hash adalah algoritma kriptografi yang mengkompresi pesan yang memiliki ukuran sembarang menjadi pesan yang berukuran tetap. Teknik ini menggunakan fungsi matematika yang menggunakan input biner menjadi biner dengan panjang yang tetap. Algoritma fungsi hash bersifat satu arah, artinya pesan ringkas tidak dapat dikembalikan lagi (deskompresi)

menjadi pesan semula. Umumnya fungsi hash digunakan bila ingin membuat tanda pengenal berupa sidik jari dari pesan. Sidik jari yang digunakan menandakan bahwa pesan yang telah dikirim benar-benar dari orang pengirim yang sebenarnya (Munir 2019)

2.2 Algoritma *Caesar Cipher*

Caesar cipher merupakan salah satu algoritma cipher tertua yang paling diketahui dalam perkembangan ilmu kriptografi. *Caesar cipher* merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada cipherteks. *Caesar cipher* adalah algoritma kriptografi klasik yang dahulu digunakan oleh Julius Caesar untuk mengirimkan pesan rahasia atau taktik militer. Penerapan *caesar cipher* tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan alpabet, pergeseran dilakukan berdasarkan pada kunci yang dimiliki.

2.3 Perancangan Sistem

Pada perancangan sistem ini menggunakan alat bantu untuk bisa mengkomunikasikan tahap-tahap dan instruksi baik berupa visual atau dengan desain. Pada pembuatan sebuah sistem membutuhkan waktu yang cukup baru bisa menghasilkan sebuah aplikasi. Untuk bisa tetap terarah pengerjaan sebuah aplikasi sesuai dengan tujuan sebelumnya diperlukan alat yang bisa dijadikan patokan. Pada penelitian ini untuk menyampaikan dan menggambarkan proses pengerjaan menerapkan *Unified modelling language* dan *flowchart.*

2.3.1 VB.net

Untuk merancang aplikasi penyandia pesan menggunakan bahasa pemrograman Vb.net. VB.NET adalah bahasa pemrograman multi-paradigma yang dikembangkan oleh Microsoft. Diluncurkan pada tahun 2002 sebagai penerus bahasa dasar visual. Visual basic.net merupakan bahasa pemrograman yang berorientas objek dikembangkan dan dirilis oleh Microsoft, dengan tujuan memudahkan para pengguna untuk merancang dan mendesain sebuah program baru. Visual Basic adalah salah satu developement tools untuk membangun aplikasi dalam lingkungan Windows. Dalam pengembangan aplikasi, Visual Basic menggunakan pendekatan Visual untuk merancang *user interface* dalam bentuk *form*, sedangkan untuk kodingnya menggunakan dialek bahasa Basic yang cenderung mudah dipelajari. Dengan menggunakan alat ini, para programmer dapat membangun aplikasi windows forms, aplikasi web berbasis asp.net, dan juga aplikasi command line. alat ini dapat diperoleh secara terpisah dari beberapa produk lainnya (seperti microsoft visual c++, visual c#, atau visual j#), atau juga dapat diperoleh secara terpadu dalam microsoft visual studio.net (Ruli 2017).

2.3.2 Node.js

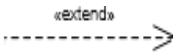
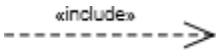
Layanan whatsapp api gateaway yang digunakan dalam mengirim pesan tersandi yaitu menggunakan node.js. Node.JS adalah sistem perangkat lunak atau platform yang digunakan untuk pengembangan aplikasi web. Node.JS dapat juga disebut sebagai runtime environment. Aplikasi ini ditulis dalam campuran Bahasa C++ dan juga JavaScript, mempunyai model event driven (basis event) dan asynchrounous I/O. Tidak seperti

kebanyakan bahasa JavaScript yang dijalankan pada web browser, Node.JS dieksekusi sebagai aplikasi server. Node.JS dapat berjalan di server karena dukungan dari V8 Engine buatan Google dan beberapa modul bawaan yang terintegrasi seperti modul http, modul filesystem, modul security dan beberapa modul penting lainnya (Rachmat 2017). Umumnya javaScript merupakan bahasa pemrograman yang hanya berjalan di sisi klien. Namun dengan aplikasi ini, Anda bisa melengkapi kekurangan tersebut dengan menjalankannya di sisi server sehingga perannya sama dengan PHP, Ruby, Perl, dan sejenisnya.

2.3.3 Unified modelling language (UML)

Unified modeling language merupakan sebuah alat perancangan sistem yang berorientasi pada objek. Pada perancangan sistem hasil analisa dan hasil desain akan didokumentasikan secara visual. Penggunaan *Unified modelling language* bertujuan untuk membantu sebuah kelompok untuk berkomunikasi dalam pengembangan proyek (Haviluddin 2011). Cara menyampaikan informasi yaitu dengan menggunakan simbol-simbol yang mana setiap simbol memiliki nama dan fungsi masing-masing. Tujuan dalam penggunaan *Unified modelling language* untuk memudahkan dalam pengembangan piranti lunak dan juga untuk memudahkan pengguna dalam melakukan proses pengerjaan secara efektif, lengkap dan tepat atau sesuai sasaran.

a. Simbol *usecase diagram*

Simbol	Nama	fungsi
	actor	Orang proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem informasi yang akan dibuat itu sendiri, jadi walaupun simbol dari actor adalah gambar orang, biasanya dinyatakan menggunakan kata benda di awal frase nama *actor*.
	use case	Fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesar antar unit atau actor biasanya dinyatakan dengan menggunakan kata kerja di awal frase nama use case.
	association	Komunikasi antara *actor* dan use case yang berpartisipasi pada use case atau use case memiliki interraksi dengan *actor*.
	*extend*	hubungan use case tambahan ke sebuah use case dimana use case yang ditambahkan dapat berdiri sendiri walau tanpa use case tambahan memiliki nama depan yang sama dengan use case yang di tambahkan.
	generalization	Hubungan generalisasi dan spesialisasi (umum-khusus) antara dua buah use case dimana fungsi yang satu adalah fungsi yang lebih umum dari lainnya.
	*include*	hubungan use case tambahan ke sebuah use case dimana use case yang ditambahkan memerlukan use case ini untuk menjalankan fungsional atau sebagai syarat dijalankan use case ini.

Gambar 2. 4 Simbol *usecase diagram*

b. Simbol *activity diagram*

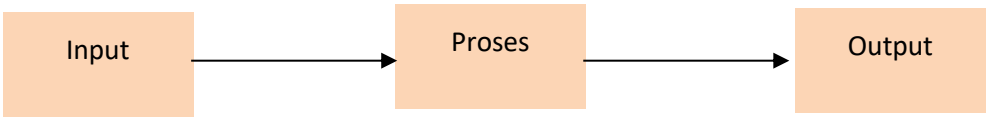
SIMBOL	**NAMA**	**FUNGSI**
	Initial	Status awal aktivitas sistem, sebuah diagram aktivitas memiliki sebuah satutus awal.
	Activity	Aktivitas yang dilakukan sistem, aktivitas biasanya diawali dengan kata kerja.
	Decision	Asosiasi percabangan dimana lebih dari satu aktivitas digabungkan menjadi satu.
	Join	Asosiasi penggabungan dimana lebih dari satu aktivitas lebih dari satu.
	Final	Status akhir yang dilakukan sistem, sebuah diagram aktivitas memiliki sebuah status satu.
	Swimline	Memisahkan organisasi bisnis yang bertanggung jawab terhadap aktivitas yang terjadi.

Gambar 2. 5 Simbol *activity diagram*

2.3.4 Flowchart

Flowchart adalah gambar atau bagan yang menampilkan urutan dan kaitan antar proses yang satu dengan yang lain serta perintah atau instruksinya. Dalam *flowchart* melakukan penggambaran secara grafik dari langkah-langkah dan urutan prosedur suatu program. Umumnya mempengaruhi penyelesaian suatu masalah yang akan

dipelajari dan dievaluasi lebih lanjut (Azkiya, Kurniawan, and Sinurat 2022). Gambaran yang akan dibuat berupa simbol yang mana setiap simbol menggambarkan proses tertentu. Pada pembuatan *flowchart* tidak ada standar yang menjadi patokan yang bersifat mutlak dikarena *flowchart* adalah hasil pemikiran dalam menganalisa suatu masalah. *Flowchart* juga bisa berbeda dengan user lain dalam menggambarkan proses dan instruksi pada program yang dibuat. Secara umum pembuatan *flowchart* akan dibagi menjadi 3 bagian penting yaitu input atau masukkan, proses dan menghasilkan output yang merupakan bahan jadi.



Gambar 2. 6 Bagian penting *flowchart*

Simbol yang umum digunakan dalam flowchart;

Simbol	Nama simbol	Fungsi
	Process	Menyatakan suatu kegiatan proses yang dieksekusi oleh komputer
	Manual	Menyatakan suatu kegiatan proses yang tidak dieksekusi oleh komputer
	Decision	Suatu kondisi dimana menghasilkan dua kemungkinan
	Predefined process	Menyatakan penyediaan tempat penyimpanan suatu pengolahan
	Terminal	Menyatakan mulai dan akhir suatu program
	Input/output	Melakukan proses *input* dan *output*
	Punched card	*Input* berasal dari kartu atau *ouput* ditulis dikartu
	Arus/*flow*	menggambarkan sebuah arus pada suatu proses
	Communication link	*m*enyatakan transmisi data dari satu lokasi ke lokasi lain
	Connector	*M*enyatakan sambungan dari proses ke proses lainnya dalam halaman yang sama
	offline connector	*m*enyatakan sambungan dari proses ke proses lainnya dalam halaman yang berbeda

Gambar 2. 7 Simbol *Flowchart*

2.4 Pengujian Aplikasi Penyadian Pesan

Pengujian yang digunakan dalam merancang aplikasi penyandian pesan dengan algoritma *caesar cipher* yaitu dengan menggunakan *blackbox testing* berfokus pada fungsional perangkat lunak. *Blackbox testing* merupakan cara pengujian yang dilakukan pada perangkat lunak yang hanya berfokus pada hasil masukkan dan keluaran dari aplikasi yang dirancang (Snadhika 2018). Keuntungan dari menggunakan *blackbox testing* adalah penguji tidak perlu mempunyai pengetahuan dengan bahasa pemrograman tertentu, penguji dilakukan dari sudut pandang pengguna bertujuan untuk menjelaskan ketidakteraturan dan ketidaktentuan arah dari sebuah aplikasi.

2.5 Penelitian Terdahulu

Berikut beberapa penelitian terdahulu yang menjadi bahan referensi yang digunakan dalam penelitian ini.

1. (Handayani et al. 2017), STMIK AMIKOM Yogyakarta 4 Februari 2017 yang berjudul "Perancangan Aplikasi Kriptografi Berbasis Web Dengan Algoritma Double *Caesar cipher* Menggunakan Tabel Ascii" membahas tentang implementasi kriptografi berbasis web proses enkripsi dan deskripsi yang tidak terbatas pada 26 alphabet tetapi mencakup semua karakter dan simbol.
2. (Guna 2021), Researchgate 2021 yang berjudul "Implementasi Aplikasi Kriptografi *Caesar cipher* Dengan Php" membahas tentang melakukan penyandian dengan menggunakan teknik *caesar cipher* dengan php berbasis web.
3. (Mesran and Nasution 2021), JURNAL RESTI Vol. 4 No. 6 (2020) 1209 – 1215 yang berjudul "Peningkatan Keamanan Kriptografi *Caesar cipher* dengan Menerapkan Algoritma Kompresi "Stout Codes", membahas tentang cara

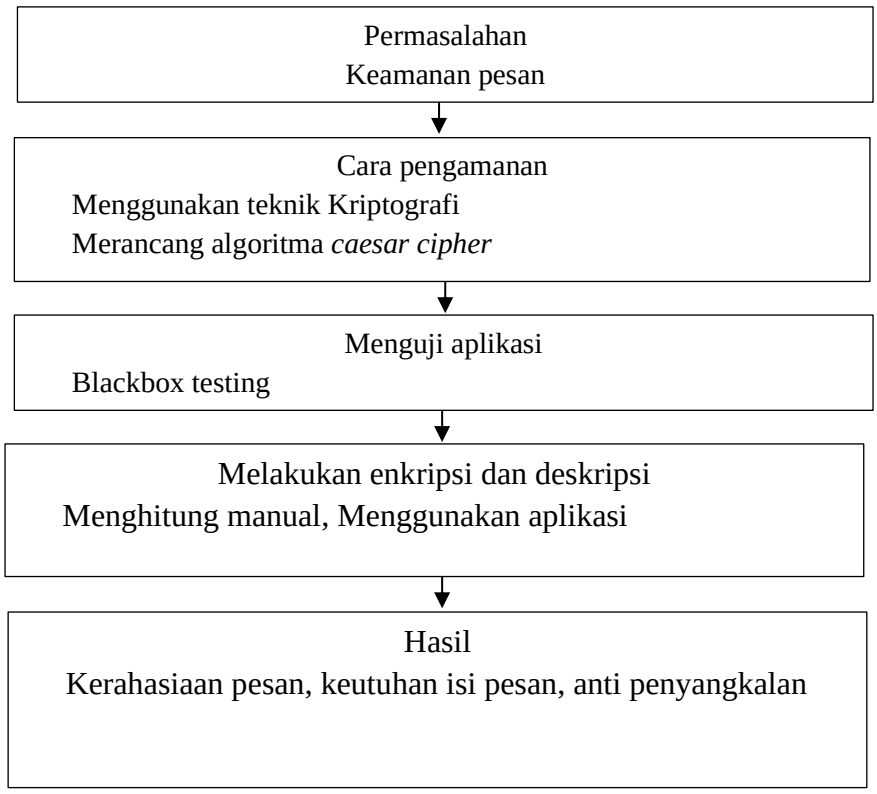
penanganan data dengan menggunakan dua kombinasi algoritma yaitu dengan algoritma *caesar cipher* dan algoritma kompresi stout code.

4. (Febrianingsih, Hafiz, and Informatikan 2019), jurnal Informasi Dan Komputer Vol: 7 No: 2 Thn: 2019 dengan judul "Implementasi Kriptografi Berbasis Caesar Chiper Untuk Keamanan Data" membahas tentang cara matematis dalam melakukan subsitusi pada algoritma *caesar cipher* untuk pengamanan data. Perhitungan subsitusi dapat dilakukan dengan cara subtitusi mulai satu angka kedepannya, dua angka dan selanjutnya.
5. (Angriani and Saharaeni 2019), Jurnal Teknologi Informasi dan Komunikasi P-ISSN: 2088-6705 Volume 9, Nomor 2, Desember 2019: 123 – 126 dengan judul "Implementasi Algoritma *Caesar cipher* Pada Keamanan Data Sistem E-Voting Pemilihan Ketua Organisasi Kemahasiswaan" membahas tentang cara mengamankan data yang dilakukan pada pemilihan ketua organisasi kemahasiswaan. Pengamanan data dilakukan dengan menggunakan algoritma *caesar cipher*. Dalam penelitian yang dilakukan dinyatakan bahwa teknik yang dilakukan cukup aman dalam menjaga kerahasiaan data.
6. (Adriyanto 2019), Jurnal Buffer Informatika Volume 5 Nomor 1, April 2019 dengan judul "Implementasi Algoritma *Caesar cipher* Untuk Keamanan Data Pada Kartu Ujian" membahas tentang cara mengelola data peserta ujian dan juga menjaga kerahasiaan id peserta menggunakan algoritma *caesar cipher*.
7. (Gunawan n.d.), InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan) Vol 2, No 2, Maret 2018 p-ISSN: 2540-759 dengan judul "Kombinasi Algoritma

Caesar cipher Dan Algoritma Rsa Untuk Pengamanan File Dokumen Dan Pesan Teks" membahas tentang cara mengamankan data dengan menggunakan dua kombinasi algoritma yaitu dengan *caesar cipher* dan algoritma Rsa. Dalam penelitian dikatakan bahwa dengan menggunakan dua kombinasi algoritma dalam pengamanan data dapat meningkatkan sistem pengamanan data.

8. (Abraham, Abraham, and Shefiu 2012), *International Journal of Engineering Science & Advanced Technology* dengan judul "*An Improved Caesar cipher (Icc) Algorithm*" membahas tentang cara mengamankan pesan dengan menggunakan algoritma *caesar cipher*.
9. (Mishra n.d.) *International Journal of Research in Engineering and Technology*, dengan judul "Enhancing Security of *Caesar cipher* Using Different Methods" membahas tentang cara peningkatan pengamanan pesan menggunakan *caesar cipher* dengan metode yang berbeda. Menyandikan dengan cara substitusi dan transposisi, dengan teknik ini dianggap kerahasiaan pesan semakin aman.
10. (Limbong 2017) *International Journal of Research in Engineering and Technology* 2 February 2017 dengan judul "*Testing the Classic Caesar cipher Cryptography using of Matlab"* membahas tentang cara merancang penyandian pesan menggunakan matlab, dijelaskan bahwa pengamanan pesan dengan modula yang berjumlah 26 kurang efektif.

2.6 Kerangka Pemikiran



Gambar 2. 8 Kerangka pemikiran

Kerangka pemikiran merupakan model konseptual akan teori yang saling berkaitan satu dengan yang lain terhadap berbagai pengaruh masalah yang penting. Kerangka berpikir adalah model konseptual tentang sebuah teori yang ada kaitannya dengan beberapa pengaruh yang telah diidentifikasikan sebagai masalah penting (sugiyono 2019). Didalam penelitian ini, yang menjadi topik permasalahan yang dibahas adalah keamanan pesan. Keamanan pesan mencakup kerahasaan isi pesan, keutuhan dan juga otentikasi terhadap sistem untuk bisa mengenal antara pengirim dan penerima pesan. Cara pengamanan pesan dengan menggunakan teknik kriptografi dengan algoritma *caesar*

cipher. Pesan yang akan kirimkan akan samarkan terlebih dahulu dengan tujuan memalsukan informasi didalamnya, dengan cara mensubtitusi setiap unit plainteks ke unit cipherteks. Setelah aplikasi penyandian pesan selesai dirancang akan diuji dengan melakukan blakcbox testing, pengujian yang akan dilakukan berupa pengujian fungsional dari aplikasi yang telah dirancang berupa input dan output. Tahap berikutnya akan melakuan pengujian menggunakan rumus matematika untuk memastikan pergeseran karakter sesuai. Hasil perhitungan manual akan dibandingkan dengan hasil menggunakan aplikasi.

UPB

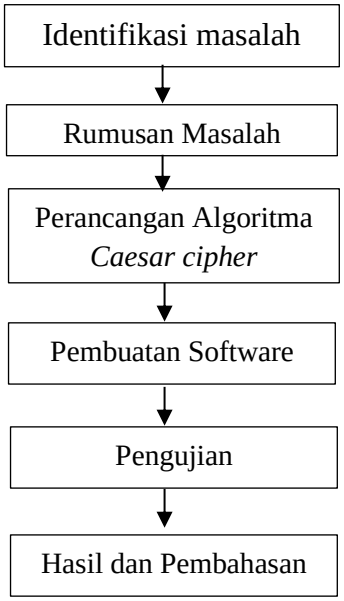
Universitas Putera Batam

BAB III

METODE PENELITIAN

3.1 Desain Penelitian

Berikut tahapan-tahapan desain penelitian untuk merancang aplikasi penyandian pesan.



Gambar 3. 1 Desain Penelitian

Peracangan sistem kriptografi ini dilakukan dengan beberapa tahap yang saling berhubungan antara satu dengan yang lain. Pada pembuatan program pengiriman pesan tersandi yang berbasis desktop, pengirim pesan akan menentukan dengan siapa pesan akan dikirim dengan cara memasukkan nomor tujuan, menginput plain teks yang menjadi cipherteks. Pada proses pengiriman, user akan melalukan log in terlebih dahulu dengan melakukan scan qrcode ke aplikasi desktop yang telah di instal.

1. Identifikasi masalah

   Dalam identifikasi masalah sudah dijelaskan dari atas yaitu memahami cara pengamanan isi pesan sehingga tidak ada perubahan selama proses pengiriman. Dalam komunikasi yang dilakukan banyak pihak diluar sana yang sengaja mencari tahu isi pesan yang akan disampaikan. Selama proses pengiriman pesan banyak kejahatan *cyber* yang bisa terjadi seperti mengubah isi pesan dan mencuri informasi yang ada pada pesan.

2. Rumusan masalah

   Pada bagian ini, penulis akan menggambarkan proses mengamankan isi pesan dengan cara menggunakan teknik kriptografi algoritma caesar cipher. Dengan menggunakan caesar cipher isi pesan tidak mudah dimengerti oleh orang yang bukan penerima sebenarnya. Sebelum pesan dikirimkan teks asli dari pesan akan disandikan terlebih dahulu, mengubah bentuk teks asli menjadi pesan yang tidak bisa dimengerti maknanya.

3. Perancagan algoritma caesar cipher

   Pada perancangan algoritma caesar cipher, penulis akan menjabarkan cara-cara yang harus dilakukan. Tujuan caesar cipher mengubah atau menyamarkan isi pesan dengan cara subtitusi tiap karakter dari teks asli menjadi teks tersandi.

4. Pembuatan software

   Aplikasi penyandian pesan dirancang dan didesain dengan sederhana sehingga mudah dimengerti oleh pengguna. Aplikasi ini berbasis desktop yang dirancang

menggunakan bahasa pemrograman bvb.net. Tampilan utama dari aplikasi penyandian pesan berisikan *log in, log out*, enkripsi (kirim) dan deskripsi.

5. Pengujian

   Pengujian yang dilakukan hanya berfokus pada fungsional dari aplikasi, hasil *input* dan *output.* Pengujian dilakukan dengan metode *blackbox testing* fungsional.

6. Hasil dan pembahasan

   Hasil dan pembahasan merupakan hasil akhir dari pembuatan aplikasi, tampilan dan cara kerja serta menampilkan hasil-hasil dari pengujian yang dilakukan.

3.2 Teknik Pengumpulan Data

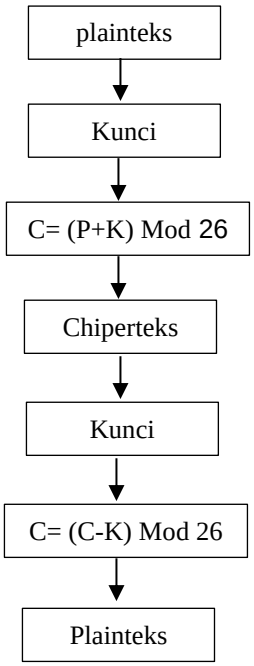
Dalam penelitian ini penulis melakukan pengumpulan data untuk menambah referensi dengan metode studi pustaka. Dalam studi pustaka mencari yang bahan pendukung seperti teori para ahli baik dari buku maupun dari jurnal yang sesuai dengan pembahasan atau topik yang diteliti.

3.3 Pemodelan Fungsional

Dalam perancangan sistem penulis akan menggambarkan tahapan-tahapan yang akan dilakukan dalam merancang desain dan juga intruksi yang digunakan dalam melaksanakan penelitian ini.

3.3.1 Flowchart caesar cipher

Flowchart caesar cipher merupakan diagaram yang menampilkan langklah-langkah atau instruksi untuk melakukan penyandian pesan dengan cara mengganti atau mengubah posisi setiap karakter pada plainteks menjadi cipherteks.



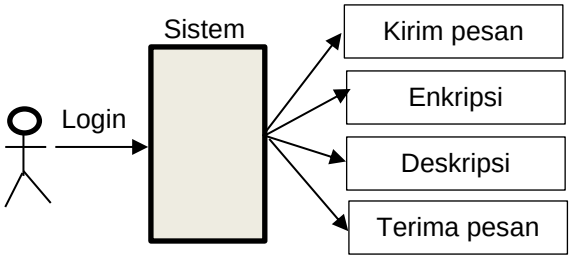
Gambar 3. 2 *Flowchart Caesar Cipher*

Pada *flowchart* ini menggmbarkan proses penyandian pesan dengan algoritma caesar cipher. Algoritma caesar cipher yaitu urutan logis yang sistematis untuk mengamankan pesan dengan teknik subtitusi untuk mengganti setiap urutan huruf yang ada diplainteks dengan huruf-huruf yanga ada diabjad sesuai dengan nilai angka yang dipilih. Urutan instruksi yang dilakukan yaitu dengan menyiapkan teks asli yang akan dikirimkan kepada penerima pesan. Setelah itu menyiapkan kunci yang digunakan dalam pergeseran karakter. Besaran pergeseran karakter tergantung

nilai kunci yang digunakan. Cara penyandiannya urutan plainteks yaitu dengan menambahkan posisi karakter pada plainteks dengan kunci, setelah dapat jumlahnya akan digantikan karakter plainteks sesuai dengan urutan yang didapat dari penjumlahan sehingga karakter plainteks akan menjadi cipherteks. Kegiatan pergeseran karakter akan dilakukan sampai semua isi pesan berubah bentukanya. Pada proses deskripsi pesan tersandi untuk mengubah kebentuk aslinya harus menggunakan kunci yang sama ketika seorang pengguna melakukan enkripsi. Caranya mengurangi setiap karakter pada cipherteks dengan nilai kunci yang ada dan hasil dari pengurangan akan dijadikan patokan untuk melakukan pergeseran sehingga menghasilkan teks asli. Proses ini dilakukan pada setiap karakter cipherteks sampai membentuk plainteks.

3.3.2 Diagram Use Case

Diagram uses case pada aplikasi penyadian pesan ini merupakan urutan interaksi seorang pengguna dengan sistem yang telah dirancang.



Gambar 3. 3 Diagram *Usecase*

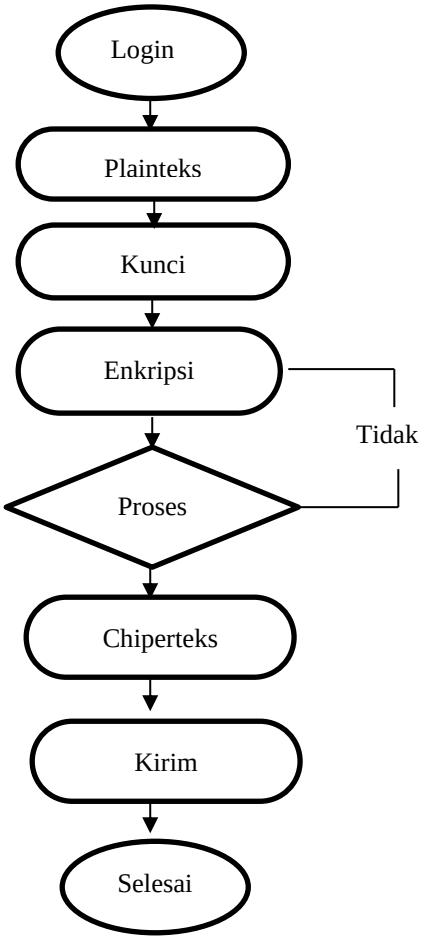
Gambar diatas menjelaskan uraian tentang tahapan urutan yang bisa dilakukan oleh pengguna yaitu memiliki dengan melakukan login terlebih dahulu, dengan bisa masuk ke sistem seorang user bisa mengirimkan pesan tersandi. Melakukan login

bertujuan untuk memperkenalkan diri sebagai pengguna, sehingga teman yang berkomunikasi lainnya mengenal dengan siapa dia mengirim dan menerima pesan. Kegiatan lainnya yang bisa dilakukan adalah melakukan pengiriman pesan, melakukan enkripsi, menerima pesan, melakukan deskripsi.

3.3.3 Diagram Activity

Pada diagram *aktivity* penulis membagi dua kegiatan yang akan dilakukan yaitu proses kirim pesan dan terima pesan.

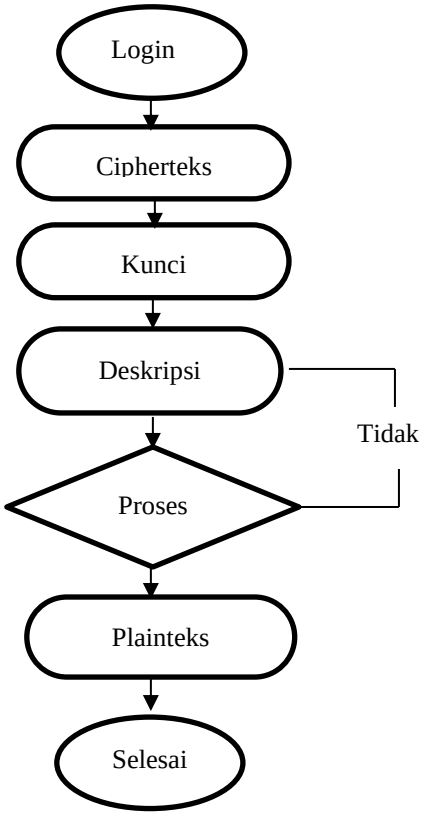
a. Enkripsi Pesan



Gambar 3. 4 *Diagaram aktivity Enkripsi* pesan

Gambar diatas menjelaskan proses pada saat kirim pesan, pengirim akan melakukan log in terlebih dahulu keaplikasi penyandian pesan. Menentukan siapa penerima dengan cara memasukkan nomor whatsapp, membuat plainteks dan menyiapkan kunci. Proses berikutnya yaitu mengubah plainteks menjadi cipherteks. Seteleh mendapatkan cipherteks pengirim melakukan pengiriman pesan kepenerima. Isi pesan yang akan dikirimkan berupa cipherteks hasil enkripsi dengan kunci yang disiapkan pengirim.

b. Deskripsi pesan



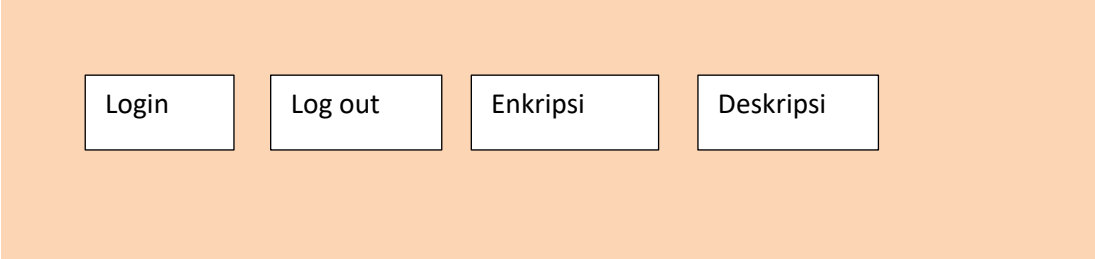
Gambar 3. 5 *Diagram Activity* Enkripsi Pesan

Pada proses penerima pesan, penerima atau seorang pengguna harus melakukan login keaplikasi terlebih dahulu. Setelah menerima pesan, isi pesan harus dideskripsi terlebih dahulu untuk mengetahui arti dari pesan. Kegiatan deskripsi harus menggunakan kunci yang sama sehingga bisa mengembalikkan

3.4 Perancangan Interface

Perancangan *form* antarmuka pada halaman utama terbagi menjadi 4 bagian utama:

3.4.1 Halaman Utama



Gambar 3. 6 Halaman Utama

Gambar diatas yaitu halaman utama dari aplikasi penyandian pesan. Pada tampilan halaman utama ada beberapa pilihan menu antara lain log in, log out, enkripsi dan deskripsi. Pada menu login untuk bisa masuk ke sistem, log out untuk mengakhiri sesi atau keluar dari aplikasi, enkripsi untuk menyandikan pesandan deskripsi untuk mengembalikan kembali makna dari pesan.

3.4.2 Menu *Login*

Gambar 3. 7 *Menu Login*

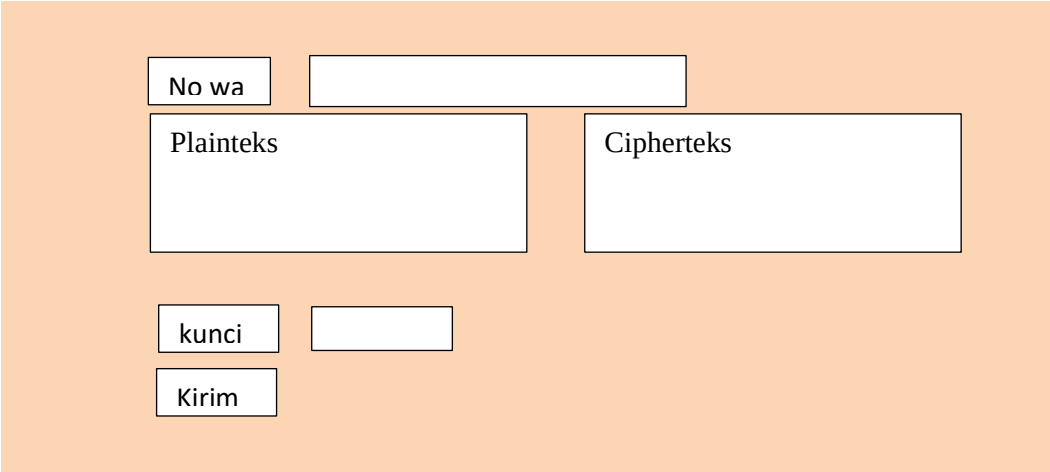
Gambar diatas merupakan desain halaman menu login, seorang pengguna akan diarahkan untuk melakukan scan *qrcode*. Hal ini bertujuan untuk memperkenalkan diri pada sistem sehingga bisa melakukan pengiriman dan penerimaan pesan.

3.4.3 Menu log out

Gambar 3. 8 *Menu Logout*

Desain antar muka menu log out. Untuk mengakhiri sebuah sesi dalam aplikasi, seorang pengguna diarahkan untuk memilih menu log out.

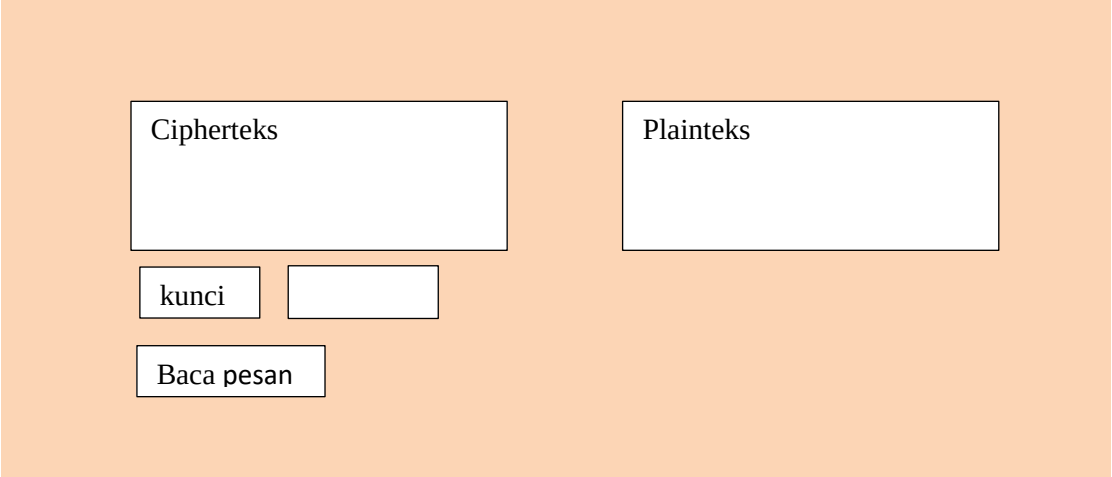
3.4.4 Menu Enkripsi



Gambar 3. 9 Menu Enkripsi

Desain menu enkripsi menampilkan beberapa form, pada menu enkripsi terdapat beberapa tampilan yang bisa dilihat oleh seorang pengguna yaitu, kolom No wa merupakan nomor yang menjadi tujuan dalam pengiriman pesan. Tempat menuliskan plainteks, tempat hasil enkripsi, kunci dan tombol kirim.

3.4.5 Menu Deskripsi



Gambar 3. 10 Menu Deskripsi

Pada menu deskripsi kegiatan pengubahan pesan dari pesan tersandi menjadi teks asli dilakukan. Dengan cara, pesan yang telah dikirm yang masih berbentuk cipherteks akan dikopi dan ditempel dikolom cipherteks pada menu deskripsi.

3.5 Perancangan algoritma *caesar cipher*

Pada perancangan algoritma *caesar cipher* menggunakan teknik penyandian dengan cara substitusi atau pergeseran posisi plainteks berdasarkan kata kunci yang gunakan. Kata kunci yang digunakan merupakan urutan alfabet dalam plainteks. Untuk melakukan pengamanan pesan seorang user akan menggunakan kata kunci yang sama untuk melakukan eskripsi dan deskripsi dengan kunci yang sama. Langkah-langkah yang harus dilakukan untuk membuat teks tersandi dengan teknik *caesar cipher*:

1. Menentukan kata kunci yang digunakan dalam pergeseran karakter
2. Menukarkan karakter pada pesan asli menjadi pesan tersandi yang telah di tentukan sebelumnya.

Sebagai contoh, melakukan pergeseran dengan kata kunci =3, untuk plain teks ABC akan melakukan pergeseran karakter berdasarkan kata kunci yang telah ditentukan sehingga ABC menjadi DEF, yang mana huruf A pada plainteks menjadi huruf D, B menjadi huruf E dan C menjadi huruf F.

Rumus enkripsi caesar cipher

C = E (P) = (P+K) Mod 26

C = Cipher teks

E = Enkripsi

P = Plainteks

K = Kunci

Mod 26 = Total jumlah huruf pada abjad

Rumus deskripsi caesar cipher

P = D (P) = (C-K) Mod 26

P = Plainteks

D = Deskripsi

C = Cipherteks

Mod 26 = Total jumlah huruf dalam karakter

Secara detail berikut tabel pergeseran plain teks menjadi cipher teks dengan kata kunci= 3,

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Tabel 3. 1 Plainteks

Menjadi

D	E	F	G	H	I	J	K	L	M	N	O	P
1	2	3	4	5	6	7	8	9	10	11	12	13
Q	R	S	T	U	V	W	X	Y	Z	A	B	C
14	15	16	17	18	19	20	21	22	23	24	25	26

Tabel 3. 2 Cipherteks

Contoh lain dalam melakukan penyandian pesan menggunakan algoritma *caesar cipher*;

Plainteks : informatika

Kunci : 3

Cipherteks : lqirupdwlnd

Baris plainteks

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Tabel 3. 3 Baris plainteks

Baris Cipherteks

d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Tabel 3. 4 Baris Cipherteks

Cara merancang algoritma caesar cipher dengan menggunakan formulasi matematika. Pertama-tama harus mengkodekan setiap karakter dalam alfabet dengan sebuah angka. Pengkodean dilakukan sesuai dengan urutan setiap huruf dari 1-26. Angka 1 mewakili huruf a dan selanjutnya sampai 26. Pada pengkodean ini tidak mempermasalahkan tentang huruf besar dan huruf kecil semuanya dianggap sama. Perhitungan caesar cipher untuk enkripsi dikenal dengan persamaan C = E(p) = (P+3)

Mod 26 sedangkan pada deskripsi P = D(p) = (C- 3) Mod 26. Huruf C kepanjangan dari cipherteks, D kepanjangan dari deskripsi, E kepanjangan dari Enkripsi, P kepanjangan dari plainteks, angka 3 merupakan kunci dan mod 26 yang merupakan jumlah keseluruhan huruf dalam alfabet. Berikut cara pengerjaan plainteks menjadi cipher teks menggunakan persamaan matematika.

Plainteks : informatika

Kunci : 3

C = E(p) = (P+3) Mod 26

P1 = i = 9 ⟶ c1 = E (9) = (9+3) Mod 26 = 12 = l

P2 = n = 9 ⟶ c2 = E (14) = (14+3) Mod 26 = 17 = q

P3 = f = 9 ⟶ c3 = E (6) = (6+3) Mod 26 = 9 = i

P4 = o = 9 ⟶ c4 = E (15) = (15+3) Mod 26 = 18 = r

P5 = r = 9 ⟶ c5 = E (18) = (18+3) Mod 26 = 21 = u

P6 = m = 9 ⟶ c6 = E (13) = (13+3) Mod 26 = 16 = p

P7 = a = 9 ⟶ c7 = E (1) = (0+3) Mod 26 = 4 = c

P8 = t = 9 ⟶ c8 = E (20) = (20+3) Mod 26 = 23 = w

P9 = i = 9 ⟶ c9 = E (9) = (9+3) Mod 26 = 12 = l

P10 = k = 9 ⟶ c10 = E (9) = (11+3) Mod 26 = 14 = n

P11 = a = 9 ⟶ c11 = E (1) = (0+3) Mod 26 = 4 = d

Dalam perhitungan diatas maka menghasilkan cipherteks yaitu “lqirupdwlnd”

Untuk mengembalikan isi pesan sehingga bisa dimengerti maka dilakukan kegiatan deskripsi. Deskripsi melakukan pergeseran tiap karakter pada cipherteks dengan cara mengurangi urutan karakter pada pesan tersandi dengan angka kunci yang sesuai saat enkripsi. Persamaan matematika dalam melakukan kegiatan deskripsi yaitu dengan menggunakan rumus P = D(p) = (C- 3) Mod 26. Pada contoh deskripsi ini menggunakan pesan hasil enkripsi dari atas dengan kunci yang sama yaitu:

Cipherteks : lqirupdwlnd

Kunci : 3

C1 = l = 12 ⟶ P1 = D (12-3) mod 26 = 9 = i

C2 = q = 17 ⟶ P1 = D (17-3) mod 26 = 14 = n

C3 = i = 9 ⟶ P1 = D (9-3) mod 26 = 6 = f

C4 = r = 18 ⟶ P1 = D (18-3) mod 26 = 15 = o

C5 = u = 21 ⟶ P1 = D (21-3) mod 26 = 28 = r

C6 = p = 16 ⟶ P1 = D (16-3) mod 26 = 13 = m

C7 = d = 4 ⟶ P1 = D (4-3) mod 26 = 1 = a

C8 = w = 23 ⟶ P1 = D (23-3) mod 26 = 20 = t

C9 = l = 12 ⟶ P1 = D (12-3) mod 26 = 9 = i

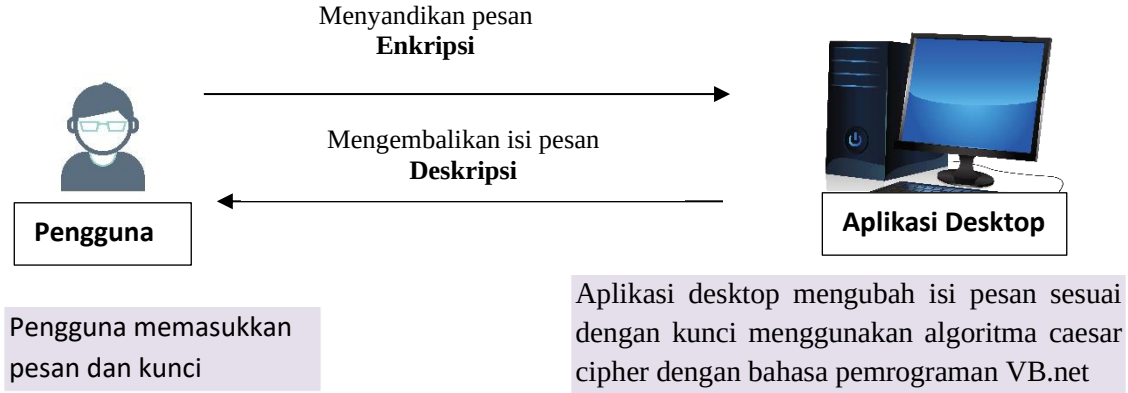
C10 = n = 14 ⟶ P1 = D (14-3) mod 26 = 11 = k

C11 = d = 4 ⟶ P1 = D (4-3) mod 26 = 1 = a

Dari operasi deskripsi diatas menghasil plainteks yaitu “informatika”.

3.6 Implementasi

Pada bagian implementasi menjadi langkah pertama untuk pembangunan sistem yang akan digunakan berdasarkan pada pendekatan dan solusi yang telah dianalisa. Pada tahap implementasi peneliti mengembangkan desain program dengan menggunakan bahasa pemgrograman vb .net 2015 untuk merancang tampilan aplikasi. Bahasa pemrograman vb. net digunakan karena mudah dimengerti dalam mengimplementasikan penyandian pesan menggunakan algoritma caesar cipher. Sedangakan untuk perangkat keras yang digunakan memiliki spesifikasi dengan processor core i5, windows 10 dan ram 8. Tampilan yang dirancang menggrunakan versi desktop untuk dapat digunakan di komputer.



Gambar 3. 11 Arsitektur Aplikasi

Gambar diatas merupakan arsitektur aplikasi penyandian pesan. Pengguna memasukkan pesan dan kunci untuk melakukan pengamanan isi pesan. Hasil enkripsi dan deskripsi akan ditampilkan pada ditampilan aplikasi penyandian pesan berbasis desktop. Teknik pengubahan isi pesan menggunakan algoritma *caesar cipher.*

3.7 Pengujian

Pada bagian pengujian peneliti melakukan pengujian terhadap sistem yang telah dibangun dengan indikator-indikator tertentu. Hal ini dilakukan untuk membuktikan bahwa sistem yang telah dibangun dapat memenuhi kebutuhan dalam penyandian pesan. Fokus pada pengujian yang akan dilakukan yaitu pengujian sistem dan pengujian algoritma caesar cipher. Pengujian sistem mencakup pada pengujian fungsional sebuah sistem sedangkan pengujian algoritma caesar cipher mencakup pada keakuratan penyandian pesan baik dihitung secara manual berdasarkan rumus matematikanya maupun dengan aplikasi yang telah dibuat.

3.8 Jadwal Penelitian

Jadwal penelitian dilakukan pada tahun 2022.

No	Kegiatan	Maret	April	Mei	Juni	Juli
1	Penginputan Judul					
2	Mengumpulkan Data					
3	Merancang Desain					
4	Implementasi					
5	Pengujian Aplikasi					
6	Membuat Laporan					

Tabel 3. 5 Jadwal Penelitian

Berdasarkan pada tabel diatas jadwal penelitian dihitung menggunakan bulan. Dimulai dari menginput judul, mengumpulkan data, merancang desain, mengimplementasikan aplikasi yang ada. Untuk memastikan aplikasi berjalan sesuai dengan tujuan dilakukan pengujian dan langkah terakhir membuat laporan.

UPB

Universitas Putera Batam