Jurnal Ilmu Komputer, Teknologi Dan Informasi
Vol. 2, No. 2, Juli 2024, Hal 39 - 47
ISSN: **2963-0169** (Online - Elektronik)
https://journal.grahamitra.id/index.php/jurikti

Modifikasi Pembangkit Kunci Algoritma Berufort Cipher Berdasarkan Pembangkit Kunci CSPRING Berbasis RSA

Santi Simangunsong[1*], Muhammad Syahrizal[2]

[1]Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
[2]Prodi teknologi rekayasa komputer grafis, Politeknik Cendana, Medan, Indonesia
Jl. Sisingamangaraja No. 338, Medan, Sumatera Utara, Indonesia
Email: [2]syahrizal83.budidarma@gmail.com
Email Penulis Korespondensi: [1*]santisimangunsong33@gmail.com

Abstrak−Informasi merupakan kumpulan data yang berupa teks yang telah disatukan yang bersifat publik atau rahasia. Data rahasia merupakan data yang berisi tentang sesutau atau yang tidak untuk dipublikasikan, sebab data tersebut merupakan dat penting. Untuk itu, data tersebut perlu diamankan. Salah satu cara untuk mengamankan data tersebut adalah dengan memanfaatkan kriptografi. Kriptografi merupakan salah satu ilmu yang yang berperan penting dalam bidang pengamanan informasi. Algoritma di dalam kriptografi terbagi menjadi dua, yaitu algoritma kunci simetri dan algoritma kunci asimetri. Salah satu yang termasuk dalam algoritma kunci simetri adalah beaufort cipher. Beaufort cipher merupakan algoritma kunci simetri yang menggunakan subtitusi abjad dengan menggunakan huruf tersebut sebagai plaintext dan huruf kunci yang memiliki posisi sebanding. Namun seiring dengan perkembangan ilmu pengetahuan manusia, tingkat kejahatan dan teknologi yang digunakan oleh penyadap data meningkat, dimana pengaman dengan metode biasa juga mampu diretas. Penelitian ini menguraikan bagaimana prosedur yang dilakukan untuk memodifikasi pembangkitan kunci yang digunakan pada algoritma beaufort cipher. Proses pembangkitan kunci dilakukan berdasarkan pembangkit kunci CSPING berbasis RSA, artinya kunci yang digunakan pada proses enkripsi dan dekripsi adalah kunci yang dibangkitkan berdasarkan pembangkit kunci CSPRING berbasis RSA, sehingga proses modifikasi yang dilakukan dalam pembangkitan kunci tersebut dapat meminimalkan tindakan pemecahan kunci yang dilakukan pihak lain serta algoritma ini dapat lebih optimal dalam mengamankan data.

Kata Kunci: Kriptografi; Algoritma; Beaufort Cipher; Pembangkit Kunci CSPRING; RSA

Abstract-Information is a collection of data in the form of text that has been put together which is public or confidential. Secret data is data that contains something or that is not to be published, because the data is important. For that, the data needs to be secured. One way to secure this data is by utilizing cryptography. Cryptography is one of the sciences that plays an important role in the field of information security. Algorithms in cryptography are divided into two, namely symmetric key algorithms and asymmetric key algorithms. One of the symmetric key algorithms is the Beaufort cipher. Beaufort cipher is a symmetric key algorithm that uses alphabetical substitution by using the letter as plaintext and key letters that have comparable positions. However, along with the development of human science, the level of crime and technology used by data interceptors increases, where security with ordinary methods can also be hacked. This research describes how the procedure is carried out to modify the key generation used in the Beaufort cipher algorithm. The key generation process is carried out based on the RSA-based CSPING key generator, meaning that the key used in the encryption and decryption process is the key generated based on the RSA-based CSPRING key generator, so that the modification process carried out in the key generation can minimize the key breaking action carried out by other parties and this algorithm can be more optimal in securing data.

Keywords: Cryptography; Algorithm; Beaufort Cipher; CSPRING Key Generator; RSA

1. PENDAHULUAN

Penyalahgunaan informasi merupakan salah satu dampak negatif dari perkembangan teknologi yang berkembang pesat saat ini, oleh karena itu perlu dilakukan pengamanan informasi agar tidak dapat diakses oleh orang-orang yang tidak bertanggung jawab[1][2]. Informasi-informasi tersebut dapat berupa data pribadi yang tidak dibuat untuk diplublikasikan, data perusahaan penting dan berbagai informasi lain yang bersifat rahasia[3]. Salah satu cara yang dapat digunakan untuk mengamankan informasi tersebut adalah dengan menggunakan metode kriptografi. Kriptografi merupakan salah satu ilmu yang yang berperan penting dalam bidang pengamanan informasi[4]. Kriptografi memiliki teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi misalnya kerahasiaan dan integritas data, serta otentikasi[5]. Kuat lemahnya metode kriptografi tidak terletak dari hasil enkripsi atau ciphertext, melainkan terletak pada kunci yang digunakan, oleh sebab itu kunci merupakan jantung dari pertahanan data tersebut agar tidak dapat diakses atau dibobol oleh orang-orang yang tidak bertanggung jawab[6]. Algoritma di dalam kriptografi terbagi menjadi dua, yaitu algoritma kunci simetri dan algoritma kunci asimetri. Salah satu yang termasuk dalam algoritma kunci simetri adalah beaufort cipher.

Beaufort cipher merupakan metode kriptografi subtitusi turunan dari vigenere cipher yang menggunakan teknik substraksi[7]. Rumus yang digunakan pada beaufort cipher sangat identik dengan beaufort cipher. Kesamaan dari kedua teknik ini adalah penggunaan fungsi modulo atau sisa hasil bagi maupun jenis kunci yang yang digunakan. Perbedaan dari kedua metode ini adalah peranan kunci, dalam beaufort cipher kunci digunakan sebagai penambah plain teks dan pengurang cipher teks[8]. Sedangkan dalam formula yang digunakan beaufort cipher, kunci digunakan untuk dikurangkan dengan plain teks maupun cipher teks. Kunci (K) pada beaufort cipher adalah urutan karakter-karakter K = k1 ... kd dimana k1 didapat dari banyaknya pergeseran dari alfabet ke-i sama seperti beuafort cipher. Artinya bahwa jumlah kunci yang dibangkitkan harus sama dengan jumlah karakter plaintext yang diamankan. Algoritma ini melakukan proses enkripsi dan dekripsi secara stream (masing-masing karakter plaintext harus memiliki pasangan

kunci. Kelemahan dari algoritma ini adalah, kunci yang digunakan merupakan terdiri dari satu karakter saja berupa huruf a-z. Hal ini dapat dijadikan sebagai kelemahan beaufort cipher[8].

Metode CSPRING berbasis RSA merupakan salah satu pembangkit kunci yang cara kerjanya sederhana, namun paling bagus dan kompleks dalam mengamankan data. cara kerja dari metode ini adalah memilih 2 bilangan prima secara acak yang dijadikan sebagai bilangan rahasia untuk membangkit kan kunci yang akan digunakan untuk mengamankan data rahasia yang akan disimpan atau disampaikan kepada orang lain. artinya kedua bilangan prima yang dipilih secara acak tersebut yang akan dijadikan sebagai dasar untuk membangkitkan kunci dan juga merupakan bilangan pembuka untuk menemukan kunci yang digunakan dalam membangkitkan kunci. untuk itu, kedua bilangan prima tersebut harus benar-benar dirahsiakan agar tidak diketahui.

Berdasarkan penelitian sebelumnya yang dilakukan oleh Mia Diana, dan Taronisokhi Zebua (2018), dalam penelitian yang berjudul optimaslisasi beaufort cipher menggunakan pembangkit kunci RC4 dalam penyandian SMS [9]. Dari hasil penelitian tersebut disimpulkan bahwa algoritma beaufort cipher yang telah dioptimalkan menggunakan RC4 menghasilkan pengamanan yang lebih kuat. Dimana kunci yang dihasilkan lebih sulit untuk diretas.

Selain itu juga, penelitian yang dilakukan oleh Setiadi, De Rosal Ignatius Moses Jatmoko dkk (2018) dalam penelitan yang berjudul kombinasi cipher subtitusi (beaufort dan vigenere) pada citra digital[10]. Kesimpulan dari penelitian tersebut adalah bahwa kedua algoritma tersebut dapat digunakan untuk mengamankan data, sebab kedua metode tersebut hampir sama. Perbedaanya terletak pada kunci yang digunakan. Kunci yang digunakan pada algoritma beaufort cipher lebih panjang dan tidak berulang.

Penelitian selanjutnya yang dilakukan oleh Naniek Widyastuti (2014) dalam penelitian yang berjudul pengembangan metode beaufort cipher menggunakan pembangkit kunci CHAOS[11]. Hasil yang di dapat dari penelitian tersebut adalah visual citra dari hasil enkripsi tidak terlihat, sebab warnanya telah teracak. Pada penelitian yang dilakukan oleh Arief Saputra (2016) dalam penelitian yang berjudul implementasi kriptografi kunci public CSPRING berbasis RSA pada aliplikasi instant messaging, mengatakan bahwa kecepatan proses enkripsi dalam pengamanan data lebih optimal dan menghasilkan kunci yang lebih kuat tidak dapat diretas. Penelitian selanjutnya yang dilakukan oleh Rian Arifin (2013) dalam penelitian yang berjudul optimalisasi algoritma LSB dengan pembangkit kunci CSPRING RSA dalam pengamanan file ke dalam citra digital.kesimpulan yang didapat dari hasil penelitian tersebut adalah pesan rahasia yang diamankan tidak dapat diketahui dan tidak mudah diretas oleh orang lain[12].

Penelitian ini menguraikan bagaimana prosedur yang dilakukan untuk memodifikasi pembangkitan kunci yang digunakan pada algoritma beaufort cipher. Proses pembangkitan kunci dilakukan berdasarkan pembangkit kunci RSA, artinya kunci yang digunakan pada proses enkripsi dan dekripsi adalah kunci yang dibangkitkan berdasarkan pembangkit kunci RSA, sehingga proses modifikasi yang dilakukan dalam pembangkitan kunci tersebut dapat meminimalkan tindakan pemecahan kunci yang dilakukan pihak lain serta algoritma ini dapat lebih optimal dalam mengamankan data.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi (cryptography) berasal dari bahasa yunani yaitu “cryptos” artinya “secret” yang berarti rahasia, sedangkan “graphein” artinya “writing” yang berarti tulisan rahasia[13][14]. Umumnya kriptografi digunakan oleh kalangan militer pada perang dunia II untuk menyampaikan informasi mengenai strategi atau langkah yang harus mereka hadapi untuk melawan musuh. Kriptografi ini digunakan untuk mengamankan pesan tersebut agar pesan rahasia tersebut tidak diketahui oleh pihak musuh. Selain itu pada abad 17, ratu Skolandia mengirim pesan rahasianya dengan menggunakan sistem kriptografi. Namun, hal tersebut telah berhasil dipecahkan oleh seorang pemecah kode sehingga ratu tersebut dihukum dengan cara dipancung. Ada beberapa defenisi kriptografi yang telah dikemukakan. Kriptografi merupakan salah satu bidang ilmu yang mempelajari tentang menjaga keamanan pesan dalam proses pengiriman dengan menggunakan metode penyandian tertentu dengan tujuan agar informasi yang termuat dalam pesan tersebut tidak diambil dan disalahgunakan oleh orang lain[15]. Namun seiring dengan perkembangan zaman, kriptografi terus mengalami perkembangan dimana banyak metode-metode baru yang telah ditemukan dan dibuat untuk mengamankan data rahasia mereka.

Kriptografi memiliki beragam metode untuk menyandikan pesan atau informasi yang ingin kita sembunyikan, seperti Caesar cipher, polyalphabetic, vigenere transposisi, dan masih banyak lagi metode yang ada di dalam kriptografi[16]. Adapun beberapa komponen dalam kriptografi, yaitu[17]:

a. Plaintext, yaitu pesan yang dibaca
b. Ciphertext yaitu pesan kunci atau pesan acak yang tidak bisa dibaca
c. Key, yaitu kunci untuk melakukan teknik kriptografi
d. Algoritma yaitu metode yang dilakukan untuk melakukan enkripsi dan dekripsi.

2.2 Algoritma Beaufort Cipher

Beaufort cipher merupakan salah satu algoritma dalam teknik keamanan kriptografi klasik. Kunci (K) pada beaufort cipher adalah urutan karakter-karakter K = k1 ... kd dimana k1 didapat dari banyaknya pergeseran dari alfabet ke-i sama seperti viginere cipher[17]. Artinya bahwa jumlah kunci yang dibangkitkan harus sama dengan jumlah karakter

plaintext yang diamankan. Algoritma ini melakukan proses enkripsi dan dekripsi secara stream (masing-masing karakter plaintext harus memiliki pasangan kunci). Hal ini yang menyebabkan algoritma ini sama hampir sama dengan algoritma vigeneere cipher. Adapun formulasi yang digunakan dalam proses enkripsi dan dekripsi adalah[7]:
Formula proses enkripsi:

$$Ci = Ek(Mi) = (Ki - Mi)\ Mod\ 26 \quad (1)$$

Formula proses deskripsi:

$$Mi = Dk(Ci) = (Ki - Ci)\ Mod\ 26 \quad (2)$$

Keterangan dari rumus di atas adalah Mi = Pesan yang akan dienkripsi (*Plain*), Ci = Sandi (*Cipher*), Ki = Kunci, Ek = Fungsi Enkripsi dan Dk = Fungsi Dekripsi. Nilai mod 26 di atas tergantung dari jumlah kebutuhan karakter yang digunakan, pada awalnya beaufort cipher hanya menggunakan 26 karakter, namun seiring dengan perkembangan teknologi komputer saat ini, maka dapat menggunakan mod 256 (mengguakan seluruh tabel ASCII).

2.3 Pembangkit CSPRING Berbasis RSA

Pembangkit kunci CSPRING berbasis Rivest Shamir Adleman (RSA) merupakan teknik kriptografi dengan memanfaatkan 2 bilangan prima. Algoritma RSA diperkenalkan oleh tiga peneliti dari MIT (Masschussets Institute of Technology), yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976. Pada algoritma RSA terdapat tiga proses yaitu, pembangkitan kunci, proses enkripsi dan proses dekripsi. Letak kesulitan algoritma ini adalah bagaimana menemukan dua faktor bilangan prima yang besar yang akan digunakan sebagai kunci publik dan kunci privat. Dua bilangan prima besar tersebut p dan q dimana $p \neq q$[18].

Algoritma RSA didasarkan pada proses enkripsi dan dekripsinya matematika khususnya pada konsep bilangan prima dan aritmatika modulo[19]. Proses matematika tersebut dilakukan untuk menghasilkan kunci rahasia yang dapat digunakan untuk proses dekripsi hanya oleh pengirim dan penerima pesan. Dasar dari algoritma ini memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Jika semakin besar bilangan yang difaktorkan, maka semakin lama waktu yang dibutuhkan. Jadi semakin besar bilangan yang difaktorkan, semakin sulit pemfaktorannya, semkin kuat pula algoritma RSA. Berikut adalah langkah-langkah penggunaan algoritma RSA[20]:

a. Menentukan p dan q. p dan q adalah bilangan prima
b. Menghitung nilai n yang merupakan modulus dengan rumus

$$n = p * q \quad (3)$$

Dimana, n = Bilangan Integer, p = Bilangan Prima Pertama, dan q = Bilangan Prima Kedua.

c. Menentukan nilai e yang bilangan prima dengan syarat.

$$1 < e < n \quad (4)$$

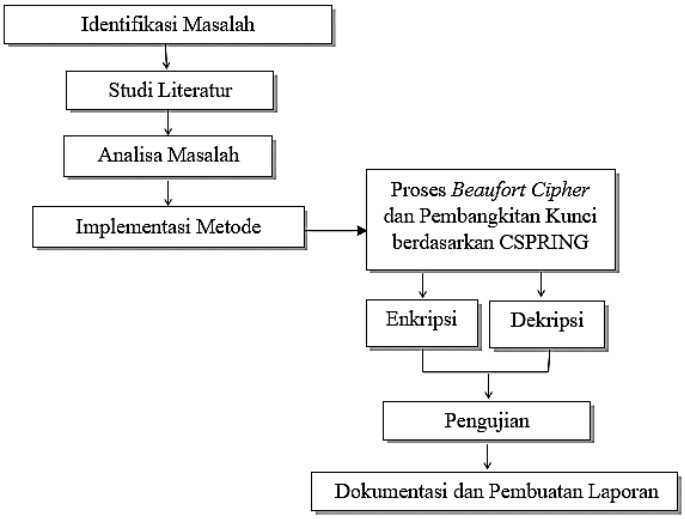
d. Mencari nilai deciphering exponent (d) dengan menggunakan rumus :

$$d = 1 + (k * n)/e \quad (5)$$

Dimana, d = deciphering exponent, k = Sembarang Angka, n = Bilangan Integer, dan e = bilangan prima.

2.4 Tahapan Penelitian

Secara Umum, Kerangka yang dilakukan dalam penelitian ini digambarkan pada bagan diagram di bawah ini:



Gambar 1. Kerangka Kerja Penelitian

Dari gambar 1 tersebut dapat dijelaskan sebagai berikut:

a. Identifikasi Masalah
   Pada tahap ini merupakan cara penulis untuk mengetahui sumber permasalahan yang dihadapi dalam proses modifkasi pembentukan kunci beaufort cipher dengan pemabngkit kunci CSPRING berbasis RSA.
b. Studi Literatur
   Pada tahapan ini dilakukan pemahaman terhadap objek yang akan diteliti dengan pengambilan data dari sumber referensi seperti buku, e-jurnal, dan sumber-sumber lain yang berhubungan dengan metode dan permasalahan yang akan diteliti.
c. Analisa Masalah
   Setelah tahapan studi literatur, maka tahapan selanjutnya adalah menganalisa masalah, yang dimana dianalisis kelemahan algortima beaufort cipher. Setelah diketahui kelemahannya, maka tahapan selanjutny adalah mencari solusi untuk menyelesaikan permasalah tersebut
d. Implementasi Metode
   Setelah melakukan analisa masalah, maka tahapan selanjutnya yaitu tahapan implementasi metode yang merupakan tahapan penerapan metode yang digunakan dalam penelitian. Tahapan awal yang dilakukan adalah melakukan proses pembangkitan kunci menggunakan CSPRING berbasis RSA kemudian melakukan proses enkripsi dan dekripsi.
   1. Tahapan pembangkitan kunci dimulai dengan menentukan nilai p dan q yang merupakan bilangan prima. Kedua bilangan prima ini yang akan dijadikan sebagai bilangan awal dalam proses pembentukan kunci. kemudian setelah ditentukan nilai p dan q, maka tahapan selanjutnya adalah mengalikan kedua bilangan tersebut.
   2. Tahapan selanjutnya adalah tahapan enkripsi dan dekripsi teks yang akan diamankan dimana kunci yang digunakan pada proses enkripsi dan dekripsi merupakan kunci yang dibangkitkan berdasarkan CSPRING berbasis RSA. Proses enkripsi dan dekripsi dilakukan berdasarkan formula beaufort cipher.
e. Pengujian
   Pada tahapan selanjutnya penulis akan melakukan pengujian terhadap sistem yang telah dirancang untuk memastikan apakah setelah dimodifikasi, kunci yang dihasilkan lebih kuat atau sebaliknya. Dalam tahapan ini akan dilakukan perhitungan manual dan kemudian dicocokan dengan sistem yang dibuat, kemudian memastikan apakah hasil enkripsi dan dekripsi sama. Hal ini juga berlaku untuk pembangkitan kunci yang dihitung secara manual, yang dimana jua dicocokkan dengan sistem.
f. Dokumentasi dan Pembuatan Laporan
   Tahapan ini akan menampilkan hasil dari modifikasi pembentukan kunci beaufort cipher dengan pembangkit kunci CSPRING berbasis RSA yang akan dibangun dan hasil pembuatan laporan penelitian. Kemudian Tahapan akhir akan dilakukan proses penulisan laporan. Tahapan ini akan menjabarkan proses dan masalah-masalah yang dihadapi dalam penelitian ke dalam bentuk laporan. Penulisan laporan penelitian juga dilakukan sebagai bentuk tanggung jawab dari hasil penelitian yang dilakukan.

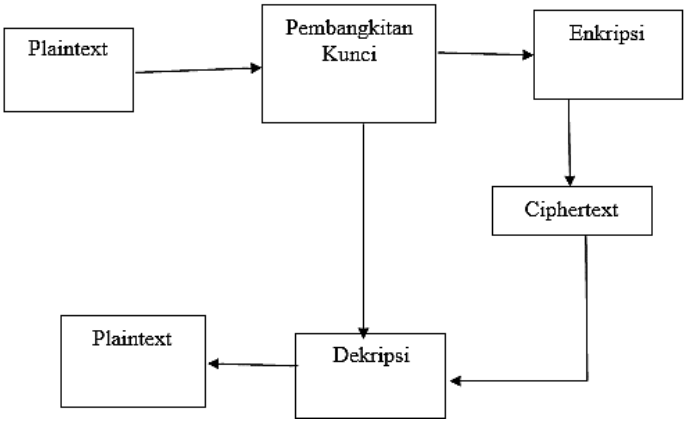
3. HASIL DAN PEMBAHASAN

3.1 Analisa Penerapan Metode

Kriptografi merupakan salah satu ilmu yang yang berperan penting dalam bidang pengamanan informasi. Kriptografi memiliki teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi misalnya kerahasiaan dan integritas data, serta otentikasi. Kuat lemahnya metode kriptografi tidak terletak dari hasil enkripsi atau dekripsi, melainkan terletak pada kunci yang digunakan. Setiap metode yang ada dalam algoritma kriptografi memiliki kelemahan masing-masing yang salah satu kelemahan tersebut terletak pada kuncinya. Kunci merupakan jantung pertahanan pengamanan data dalam teknik kriptografi. Semakin bagus kunci yang digunakan, maka semakin kuat pengamanan data yang dihasilkan. Namun seiring dengan perkembangan teknologi, banyak metode baru yang telah ditemukan dan dibuat untuk digunakan dalam upaya penyalahgunaan informasi. Metode-metode tersebut memanfaatkan kelemahan kunci yang digunakan. Mulai dari menebak panjang kuncinya, dan lain sebagainya. Bila hal ini dibiarkan, maka akan mengancam keamanan data.

Metode ini mulai tidak digunakan oleh banyak orang untuk mengamankan infomasi atau data rahasia, karena tidak cukup kuat. Salah satu solusi keamanan kunci adalah melakukan pembangkitan kunci yang lebih acak sehingga kunci yang digunakan dalam beaufort cipher lebih tahan terhadap tindakan pemecahan. Berikut adalah bagan hasil analisa terhadap keamanan kunci.

Jurnal Ilmu Komputer, Teknologi Dan Informasi
Vol. 2, No. 2, Juli 2024, Hal 39 - 47
ISSN: **2963-0169** (Online - Elektronik)
https://journal.grahamitra.id/index.php/jurikti

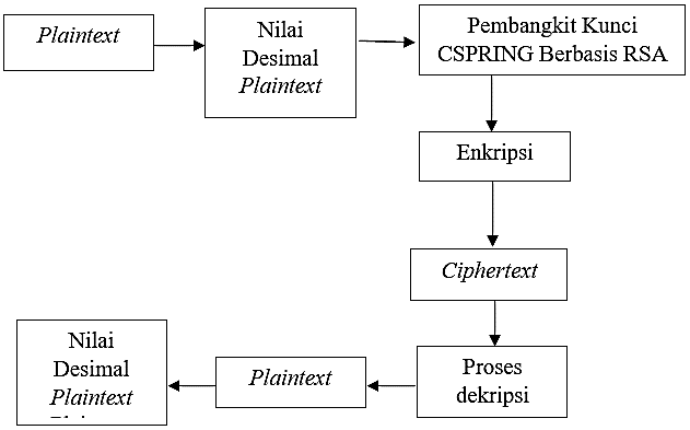


Gambar 2. Analisa Keamanan Kunci

Tahapan pertama yang dilakukan dalam proses modifikasi pembentukan kunci beaufort cipher, yaitu menginputkan teks yang akan diamankan, kemudian mengubah teks tersebut ke dalam bentuk desimal ASCII. Setelah mengubah pesan asli tersebut, kemudian dilakukan proses pembangkitan kunci berdasarkan pembangkit kunci CSPRING berbasis RSA. Hasil dari pembangkitan kunci inilah yang akan dijadikan kunci dan yang akan dienkripsikan. Berikut adalah prosedur yang dilakukan dalam mengamankan data berdasarkan algoritma beaufort cipher yang kunci telah dimodifikasi:

a. Proses enkripsi
b. Rubah plaintext menjadi nilai desimal.
c. Bangkitkan kunci berdasarkan pembangkit kunci CSPRING berbasis RSA
d. Lakukan proses enkripsi berdasarkan algoritma beaufort cipher dengan menggunakan kunci hasil tahap ke 2
e. Hasil proses tahap ke 2 adalah ciphertext

Proses dari modifikasi kunci algoritma beaufort cipher berdasarkan pembangkit kunci CSPRING berbasis RSA, dapat dilihat pada gambar di bawah ini:



Gambar 3. Diagram Proses Modifikasi Kunci Algoritma Beaufort Cipher Berdasarkan Pembangkit Kunci CSPRING Berbasis RSA

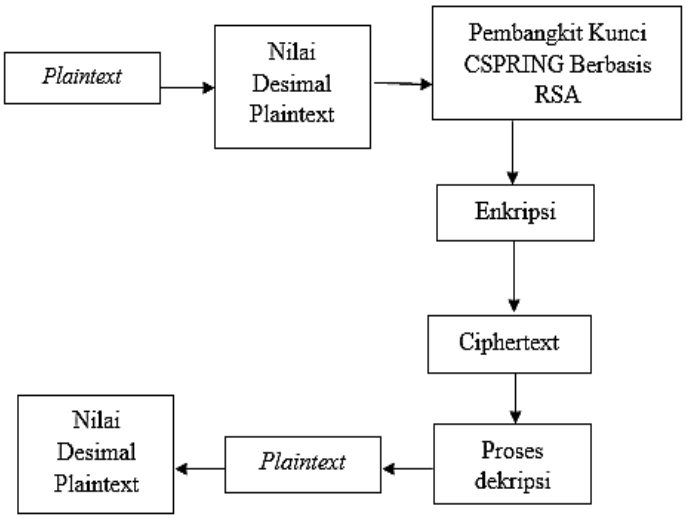
3.2 Penerapan Modifikasi Kunci Algoritma Beaufort Cipher Berdasarkan Pembangkit Kunci CSPRING Berbasis RSA

Tahapan pertama yang dilakukan dalam proses modifikasi beaufort cipher, yaitu menginputkan teks yang akan diamankan, kemudian mengubah teks tersebut ke dalam bentuk desimal ASCII. Setelah mengubah pesan asli tersebut, kemudian dilakukan proses pembangkitan kunci berdasarkan pembangkit kunci CSPRING berbasis RSA. Hasil dari pembangkitan kunci inilah yang akan dijadikan kunci dan yang akan dienkripsikan. Berikut adalah prosedur yang dilakukan dalam mengamankan data berdasarkan algortma beaufort cipher yang dimodifikasi :

a. Proses enkripsi
b. Rubah plaintext menjadi nilai desimal.
c. Bangkitkan kunci berdasarkan pembangkit kunci CSPRING berbasis RSA
d. Lakukan proses enkripsi berdasarkan algoritma beaufort cipher dengan menggunakan kunci hasil tahap ke 2
e. Hasil proses tahap ke 2 adalah ciphertext

Proses dari modifikasi pembentukan kunci algoritma beauforte cipher berdasarkan pembangkit kunci berbasis RSA, dapat dilihat pada gambar di bawah ini:

Jurnal Ilmu Komputer, Teknologi Dan Informasi
Vol. 2, No. 2, Juli 2024, Hal 39 - 47
ISSN: **2963-0169** (Online - Elektronik)
https://journal.grahamitra.id/index.php/jurikti



Gambar 4. Diagram Proses Modifikasi Beaufort Cipher dengan Pembangkit Kunci CSPRING berbasis RSA

Data teks yang digunakan sebagai sample untuk diamankan adalah password akun E-mail penulis seperti pada tabel 1:

Tabel 1. Sampel Data

Karakter	Nilai ASCII
D	68
U	85
A	65
O	79
K	75
T	84
O	79
B	66
E	69
R	82

a. Proses pembentukan kunci
   1. Menentukan nilai p dan q yang merupakan bilangan prima. Bilangan tersebut adalah sebagai berikut:

      $P = 47\ dan\ q = 71$

   2. Kemudian menghitung nilai n dengan rumus n = p*q

      $n = 47 * 71 = 3337$

   3. Kemudian menentukan nilai d dan c sebagai kunci privat
      d = 79
      c = 1019
   4. Kemudian menentukan karakter yang dibutuhkan dalam proses pembangkitan kunci. karakter tersebut adalah:

Tabel 2. Karakteristik Pembentuk Kunci

Teks	Desimal ASCII
R	82
A	65
H	72
A	65
S	83
I	73
A	65

Setelah dikonversi, memecah hasil nilai konversi tersebut menjadi blok-blok. Pesan yang telah dikonversi di atas dapat dipecah menjadi 5 blok yang terdiri dari 3 digit setiap blok. Blok-blok tersebut adalah 826 572 658 373

065. Kemudian melakukan proses pembangkitan kunci menggunakan formula pembangkitan kunci CSPRING berbasis RSA.

$K1 = 826^{79}\ mod\ 3337 = 1670$

$K2 = 572^{79}\ mod\ 3337 = 3136$

$K3 = 658^{79}\ mod\ 3337 = 1833$

$K4 = 373^{79}\ mod\ 3337 = 1773$

$K5 = 065^{79}\ mod\ 3337 = 1579$

Dari hasil perhitungan di atas, didapatkan nilai blok baru yaitu 1670 3136 1833 1773 1579. Kemudian nilai-nilai di atas dibagi dalam beberapa blok, dimana setiap blok terdiri dari 2 digit. Nilai-nilai tersebut adalah 16 70 31 36 18 33 17 73 15 79. Nilai-nilai tersebut adalah kunci yang akan digunakan pada proses enkripsi dan dekripsi.

b. Proses enkripsi

Proses enkripsi merupakan tahapan pengacakan pesan dari pesan awal atau plaintext menjadi pesan acak atau ciphertext. Berikut adalah perhitungannya :

$Ci\ =\ (Ki - Pi)\ mod\ 256$

$C1\ =\ (16 - D)\ mod\ 256\ =\ (16 - 68)\ mod\ 256\ =\ (-52)\ mod\ 256\ =\ 204\ =$ Ï

$C2\ =\ (70 - U)\ mod\ 256\ =\ (70 - 85)\ mod\ 256\ =\ (-15)\ mod\ 256\ =\ 241\ =$ Ò

$C3\ =\ (31 - A)\ mod\ 256\ =\ (31 - 65)\ mod\ 256\ =\ (-34)\ mod\ 256\ =\ 222\ =\ fi$

$C4\ =\ (36 - O)\ mod\ 256\ =\ (36 - 79)\ mod\ 256\ =\ (-43)\ mod\ 256\ =\ 213\ =\ '$

$C5\ =\ (18 - K)\ mod\ 256\ =\ (18 - 75)\ mod\ 256\ =\ (-57)\ mod\ 256\ =\ 199\ =<<$

$C6\ =\ (33 - T)\ mod\ 256\ =\ (33 - 84)\ mod\ 256\ =\ (-51)\ mod\ 256\ =\ 205\ =$ Õ

$C7\ =\ (17 - O)\ mod\ 256\ =\ (17 - 79)\ mod\ 256\ =\ (-62)\ mod\ 256\ =\ 194\ =$ ¯

$C8\ =\ (73 - B)\ mod\ 256\ =\ (73 - 66)\ mod\ 256\ =\ 7\ mod\ 256\ =\ 7\ =< BEL >$

$C9\ =\ (15 - E)\ mod\ 256\ =\ (15 - 69)\ mod\ 256\ =\ (-54)\ mod\ 256\ =\ 202\ =$ ┘

$C10\ =\ (79 - R)\ mod\ 256\ =\ (79 - 82)\ mod\ 256\ =\ (-3)\ mod\ 256\ =\ 253\ =$ "

Dari hasil enkripsi di atas, maka didapatkan pesan acak atau ciphertext yaitu Ï Òfi′ << Õ¯ < BEL > ┘"

c. Proses dekripsi

Proses dekripsi merupakan proses mengembalikan pesan acak ke pesan awal atau plaintext. Berikut adalah proses perhitungan dekripsi :

$Pi\ =\ (Ki - Pi)\ mod\ 256$

$C1\ =\ (16 -$ Ï$)\ mod\ 256\ =\ (16 - 204)\ mod\ 256\ =\ (-188)\ mod\ 256\ =\ 68\ =\ D$

$C2\ =\ (70 -$ Ò$)\ mod\ 256\ =\ (70 - 241)\ mod\ 256\ =\ (-171)\ mod\ 256\ =\ 85\ =\ U$

$C3\ =\ (31 - fi)\ mod\ 256\ =\ (31 - 222)\ mod\ 256\ =\ (-191)\ mod\ 256\ =\ 65\ =\ A$

$C4\ =\ (36 - ')\ mod\ 256\ =\ (36 - 213)\ mod\ 256\ =\ (-177)\ mod\ 256\ =\ 79\ =\ O$

$C5\ =\ (18 - <<)\ mod\ 256\ =\ (18 - 199)\ mod\ 256\ =\ (-181)\ mod\ 256\ =\ 75\ =\ K$

$C6\ =\ (33 -$ Õ$)\ mod\ 256\ =\ (33 - 205)\ mod\ 256\ =\ (-172)\ mod\ 256\ =\ 84\ =\ T$

$C7\ =\ (17 -$ ¯$)\ mod\ 256\ =\ (17 - 194)\ mod\ 256\ =\ (-177)\ mod\ 256\ =\ 79\ =\ O$

$C8\ =\ (73 - < BEL >)\ mod\ 256\ =\ (73 - 7)\ mod\ 256\ =\ 66\ mod\ 256\ =\ 66\ =\ B$

$C9\ =\ (15 -$ ┘$)\ mod\ 256\ =\ (15 - 202)\ mod\ 256\ =\ (-187)\ mod\ 256\ =\ 69\ =\ E$

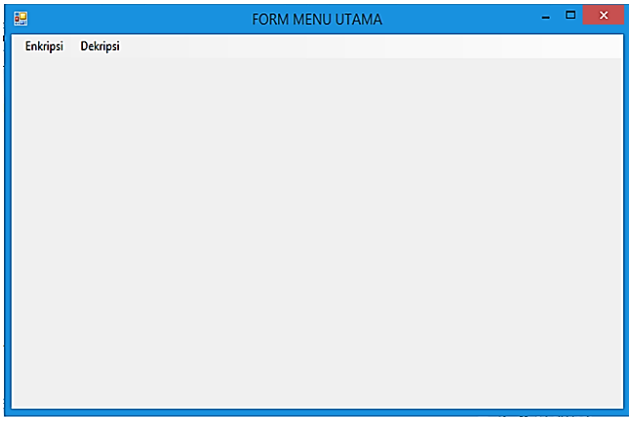
$C10\ =\ (79 -$ "$)\ mod\ 256\ =\ (79 - 253)\ mod\ 256\ =\ (-174)\ mod\ 256\ =\ 82\ =\ R$

Maka *plaintext* dari proses dekripsi adalah DUAOKTOBER.

3.3 Tampilan Program

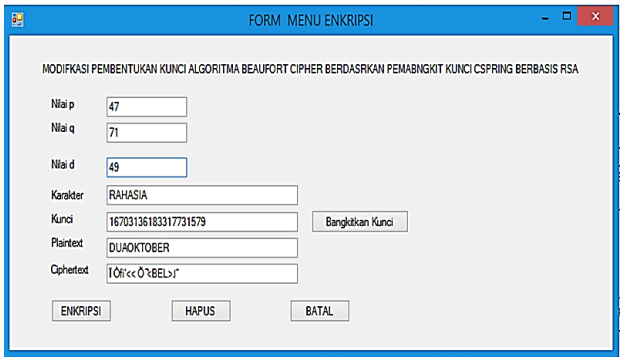
Tampilan program merupakan bentuk tampilan grafis yang berhubungan langsung dengan pengguna. Tampilan program berguna untuk menghubungkan antara pengguna dengan sistem operasi sehingga aplikasi tersebut dapat digunakan.

a. Tampilan menu utama



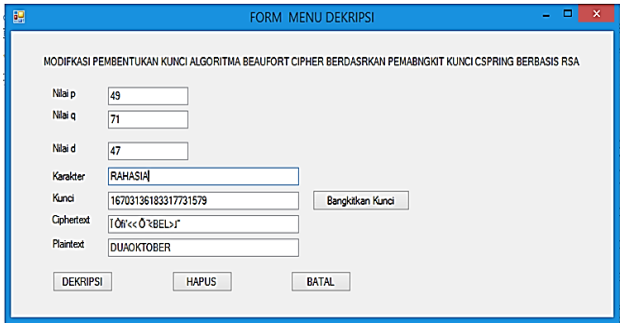
Gambar 5. Tampilan Menu Utama

b. Tampilan Menu Enkripsi



Gambar 6. Tampilan Menu Enkripsi

c. Tampilan Menu Deskripsi



Gambar 7. Tampilan Menu Deskripsi

3.4 Hasil Pengujian

Pengujan merupakan salah satu proses penelitian yang dilakukan untuk mendapatkan informasi mengenai kualitas suatu layanan yang diuji. Proses pengujian aplikasi yang telah dibuat ini dilakukan berdasarkan hasil yang telah diperoleh dari *input* yang telah diproses. Berikut adalah hasil pengujian aplikasi pengamanan data menggunakan modifikasi pembangkitan kunci algoritma *beaufort cipher* dengan pembangkit kunci CSPRING RSA :

Tabel 3. Hasil Pengujian

P	Q	D	Karakter	Kunci	Plaintext	Ciphertext
47	71	79	RAHASIA	16703136183317731579	DUAOKTOBER	Ï Òfï'<< Õ˜<BEL>Ì“
59	83	53	KAMPUNG	378929509308502840813	HATINURANI	ÏεÕìç̃@¥©
31	61	91	DARKNESS	58920691704972648291	BALON MERAH	©°À⅋ÆjŨ˜Ⅎ
51	87	59	JENDELA	5627948590164739294	WAKTUKELAM	ċÕĭÇẔŐŠŮ
57	73	79	GLOWING	54692845620194750274	KEHIDUPAN	ňŕÕżᵛᵻˢ:Fȝ

4. KESIMPULAN

Kesimpulan dari penelitian modifikasi pembentukan kunci algoritma Beaufort Cipher berdasarkan pembangkit kunci CSPRING berbasis RSA adalah sebagai berikut: Pertama, prosedur pengamanan data dengan menggunakan algoritma Beaufort Cipher melibatkan penyandian alfabet melalui deretan sandi yang berkaitan dengan huruf-huruf dalam kata kunci, yang pada dasarnya merupakan metode yang sangat kuat dalam mengamankan data, dikenal luas, dan digunakan secara luas. Kedua, modifikasi dalam pembentukan kunci algoritma Beaufort Cipher menggunakan pembangkit kunci CSPRING berbasis RSA melibatkan konversi plaintext menjadi desimal ASCII dan penggunaan kunci yang dihasilkan dari proses pembangkitan kunci CSPRING berbasis RSA untuk enkripsi dan dekripsi. Ketiga, proses pengembangan aplikasi pengamanan data yang merupakan modifikasi dari pembentukan kunci algoritma Beaufort Cipher berdasarkan pembangkit kunci CSPRING berbasis RSA dilakukan menggunakan Microsoft Visual Studio 2008, yang menghasilkan aplikasi yang dapat mempermudah proses pengamanan data, terutama data yang bersifat rahasia.

REFERENCES

[1] S. Nurul, S. Anggrainy, and S. Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)," *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, 2022.
[2] N. S. Hafizhah and F. S. Akbar, "Pengaruh Motivasi Belajar, Integritas Mahasiswa, dan Penyalahgunaan Teknologi Informasi Terhadap Perilaku Kecurangan Akademik," *Eqien-Jurnal Ekon. Dan Bisnis*, vol. 10, no. 2, pp. 195–200, 2022.
[3] M. B. Yel and M. K. M. Nasution, "Keamanan informasi data pribadi pada media sosial," *J. Inform. Kaputama*, vol. 6, no. 1, pp. 92–101, 2022.
[4] R. Maulana and R. M. Simanjorang, "Implementasi Kriptografi Untuk Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 6, pp. 377–383, 2021.
[5] A. Setiawan and T. Fatimah, "Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada PT. Trans Intra Asia," *SKANIKA Sist. Komput. dan Tek. Inform.*, vol. 4, no. 1, pp. 66–71, 2021.
[6] F. Telaumbanua and T. Zebua, "Modifikasi Vigenere Cipher Dengan Pembangkit Kunci Blum Blum Shub," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 4, no. 1, 2020.
[7] E. Ndruru and T. Zebua, "Pembangkitan Kunci Beaufort Cipher Dengan Teknik Blum-blum Shub pada Pengamanan Citra Digital," *Bull. Inf. Technol.*, vol. 3, no. 2, pp. 149–154, 2022.
[8] A. Abiyuda and L. Nababan, "Rancang Bangun Aplikasi Chatting Dengan Wireless LAN Menggunakan Metode Beaufort Cipher," *Inf. Syst. Data Sci.*, vol. 1, no. 2, pp. 97–106, 2023.
[9] M. Diana and T. Zebua, "Optimalisasi Beaufort Cipher Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, p. 12, 2018, doi: 10.30645/j-sakti.v2i1.52.
[10] D. R. I. M. Setiadi, C. Jatmoko, E. H. Rachmawanto, and C. A. Sari, "Kombinasi Cipher Subtitusi (Beaufort Dan Vigenere) Pada Citra Digital," *Proceeding SENDI_U*, pp. 52–57, 2018.
[11] N. Widyastuti, "Pengembangan Metode Beaufort Cipher Menggunakan Pembangkit Kunci Chaos," *J. Teknol.*, vol. 7, no. 1, pp. 73–82, 2014.
[12] R. Arifin, "optimalisasi algoritma LSB dengan pembangkit kunci CSPRING RSA," *UNM J.*, vol. 1, 2013.
[13] I. Riadi, A. Fadlil, and F. A. Tsani, "Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 33–45, 2022.
[14] O. Dakhi, M. Masril, R. Novalinda, J. Jufrinaldi, and A. Ambiyar, "Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Chiper," *J. Inov. Vokasional dan Teknol.*, vol. 20, no. 1, pp. 27–36, 2020.
[15] A. T. F. Alhamdi and R. F. Siahaan, "Penerapan Kriptografi Dalam Pengamanan Pesan Text Berbasis Android Dengan Menggunakan Metode Rijndael," *J. Mahajana Inf.*, vol. 6, no. 2, pp. 69–74, 2021.
[16] A. Amrulloh and E. I. H. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 5, no. 2, pp. 71–77, 2019.
[17] A. Z. F. Rangkuti and H. Fahmi, "Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5," *J. Nas. Komputasi Dan Teknol. Inf.*, vol. 3, no. 2, 2020.
[18] C. F. Sianturi, "Modifikasi Pembangkit Kunci Algoritma RSA Dengan Menerapkan Algoritma Blum Blum Shub (BBS)," *Build. Informatics, Technol. Sci.*, vol. 2, no. 1, pp. 39–43, 2020.
[19] N. B. N. Putra, F. A. Raihana, W. M. A. Mondong, and A. R. Kardian, "Analisis Enkripsi Kriptografi Asimetris Algoritma RSA Berbasis Pemrograman Batch pada Media Flashdisk," *Jurasik (Jurnal Ris. Sist. Inf. dan Tek. Inform.*, vol. 8, no. 1, pp. 142–154, 2023.
[20] N. C. H. Wibowo, K. Umam, A. M. I. Khaq, and F. A. Rizki, "Komparasi Waktu Algoritma RSA dengan RSA-CRT Base On Computer," *Walisongo J. Inf. Technol.*, vol. 2, no. 1, pp. 13–26, 2020.