PENERAPAN SUPER ENKRIPSI ALGORITMA BEAUFORT DAN VIGENERE CIPHER MEMANFAATKAN PSEUDO KEY GENERATOR BLUM-BLUM SHUB

Putri Awaliyah Rahmah[1)], Achmad Fauzi[2)]

[1,2)]*STMIK Kaputama*
Jl. Veteran No.4A, Tangsi, Kec. Binjai Kota, Kota Binjai, Sumatera Utara 20714
Email: *putriawaliyar@gmail.com*

ABSTRACT

Super encryption is a data security technique that combines multiple cryptographic methods to enhance message security. This study proposes a super encryption method using a combination of Vigenère Cipher and Beaufort Cipher algorithms, strengthened by the Blum Blum Shub pseudo-random key generator. The aim of this method is to secure text data by producing more complex and harder-to-crack encryption. The Vigenère Cipher is known for its polyalphabetic nature, while the Beaufort Cipher offers unique characteristics that distinguish it from other ciphers. The Blum Blum Shub pseudo-key generator ensures a high level of key randomness. The implementation of this method is expected to provide a practical and efficient solution for securing text data. The evaluation focuses on analyzing algorithm complexity, key randomness, and resilience against cryptographic attacks.

Keywords : *Blum_Blum_Shub, Beaufort_Cipher, Super_Encryption, Pseudo_Key_Generator, Vigenère_Cipher.*

1. PENDAHULUAN

Dalam era digital, pesan teks menjadi salah satu bentuk komunikasi paling umum digunakan, baik di sektor pemerintahan, bisnis, maupun pribadi. Sayangnya, pesan teks sering kali menjadi target utama serangan siber, termasuk penyadapan, manipulasi data, dan pencurian informasi. Ancaman ini semakin meningkat seiring dengan maraknya penggunaan layanan pesan instan dan aplikasi berbasis internet. Tanpa pengamanan yang memadai, pesan teks yang mengandung informasi sensitif berpotensi jatuh ke tangan pihak yang tidak berwenang, sehingga membahayakan privasi dan integritas data [1].

Seiring dengan meningkatnya ancaman terhadap keamanan data, inovasi dalam teknik kriptografi terus dilakukan untuk memastikan tingkat perlindungan yang lebih tinggi. Salah satu inovasi tersebut adalah penggunaan metode super enkripsi, yaitu penggabungan lebih dari satu algoritma kriptografi dalam proses enkripsi. Super enkripsi bertujuan untuk meningkatkan kompleksitas sistem keamanan, sehingga memperkecil peluang serangan berhasil menembus sistem [2].

Pengamanan pesan teks biasanya dilakukan dengan teknik enkripsi menggunakan algoritma kriptografi [3]. Namun, algoritma enkripsi tunggal sering kali memiliki kelemahan yang dapat dimanfaatkan oleh penyerang. Sebagai contoh, Vigenère Cipher, meskipun merupakan salah satu algoritma polialfabetik klasik yang dapat mengacak pola dalam pesan, memiliki kelemahan mendasar. Jika panjang kunci

pendek atau kunci berhasil ditebak, algoritma ini masih dapat ditembus melalui serangan seperti analisis frekuensi atau Kasiski Examination [4].

Di sisi lain, Beaufort Cipher, meskipun menggunakan operasi yang berbeda dengan tabel enkripsi yang serupa, juga tidak kebal terhadap serangan jika kunci yang digunakan tidak cukup kuat.Selain penggabungan algoritma, penelitian ini juga mengadopsi generator kunci pseudo Blum Blum Shub (BBS) untuk menghasilkan kunci enkripsi. BBS dipilih karena kemampuannya menghasilkan bilangan acak yang sulit diprediksi, sesuai dengan prinsip dasar kriptografi modern. Dengan menggunakan BBS, kunci yang dihasilkan tidak hanya acak tetapi juga memiliki sifat keacakan yang tinggi, sehingga menambah ketahanan terhadap serangan seperti brute force.

Kelemahan ini mendorong perlunya inovasi metode pengamanan, salah satunya adalah penerapan super enkripsi, yaitu penggabungan dua atau lebih algoritma kriptografi dalam satu proses enkripsi [5]. Super enkripsi bertujuan untuk meningkatkan ketahanan sistem terhadap serangan siber dengan memanfaatkan kelebihan masing-masing algoritma untuk menutupi kelemahannya. Dalam penelitian ini, super enkripsi dilakukan dengan mengombinasikan Vigenère Cipher dan Beaufort Cipher. Kombinasi ini dirancang untuk memberikan tingkat perlindungan lebih tinggi, karena pola operasi kedua algoritma berbeda, sehingga mempersulit analisis pola dan serangan berbasis frekuensi. Dengan demikian, kelemahan pada satu algoritma dapat diminimalkan oleh kekuatan algoritma lainnya.

Selain itu, penelitian ini juga menggunakan generator kunci pseudo Blum Blum Shub (BBS) untuk menghasilkan kunci enkripsi. BBS dipilih karena kemampuannya menghasilkan bilangan acak dengan tingkat keacakan tinggi, sehingga kunci enkripsi menjadi lebih sulit ditebak dan tahan terhadap serangan brute force. Kombinasi super enkripsi dengan BBS diharapkan dapat menghasilkan sistem pengamanan pesan teks yang lebih andal, kompleks, dan sulit ditembus.

Penelitian ini bertujuan untuk mengembangkan metode super enkripsi berbasis kombinasi Vigenère Cipher dan Beaufort Cipher dengan Blum Blum Shub sebagai generator kunci [6]. Selain itu, penelitian ini juga akan mengevaluasi tingkat keacakan kunci, efisiensi algoritma, serta ketahanan sistem terhadap serangan seperti analisis frekuensi dan brute force.
Melalui penggabungan algoritma klasik yang dikombinasikan dengan generator kunci modern, penelitian ini tidak hanya mengusulkan solusi baru dalam pengamanan data tetapi juga memberikan landasan teoritis dan praktis bagi pengembangan sistem kriptografi yang lebih canggih di masa depan [7].

2. METODOLOGI PENELITIAN

2.1 Super Enkripsi

Super enkripsi adalah teknik pengamanan data yang melibatkan penggunaan lebih dari satu algoritma kriptografi secara berlapis untuk memperkuat tingkat keamanan informasi [8]. Dalam metode ini, hasil enkripsi dari satu algoritma dienkripsi kembali menggunakan algoritma lain, menciptakan beberapa lapisan perlindungan yang dirancang untuk mempersulit upaya dekripsi tanpa otorisasi. Super enkripsi merupakan inovasi yang bertujuan untuk mengatasi kelemahan inheren dari algoritma enkripsi tunggal dengan memanfaatkan kelebihan masing-masing algoritma secara sinergis.

Konsep super enkripsi memiliki landasan kuat dalam prinsip keamanan kriptografi, yaitu kerahasiaan (confidentiality), integritas (integrity), dan autentikasi (authentication) [9]. Dengan pendekatan berlapis, super enkripsi tidak hanya menambah kompleksitas dalam analisis serangan, tetapi juga meningkatkan ketahanan terhadap berbagai ancaman, seperti serangan brute force, analisis pola, dan serangan berbasis statistik.

Sistem pengamanan data memiliki beberapa keunggulan utama:

1. Ketahanan yang Lebih Baik terhadap Serangan
   Kombinasi algoritma membuat analisis pola dan serangan brute force menjadi lebih sulit dilakukan.
2. Penguatan Kelemahan Individual
   Kekurangan pada salah satu algoritma dapat ditutupi oleh kekuatan algoritma lainnya.
3. Kompleksitas yang Lebih Tinggi
   Lapisan enkripsi ganda meningkatkan tingkat kesulitan bagi penyerang untuk membongkar sistem tanpa kunci yang valid.

Super enkripsi memberikan solusi yang relevan dalam menghadapi ancaman siber modern, terutama pada pengamanan data yang sensitif seperti pesan teks. Metode ini menjadi landasan penting dalam pengembangan sistem kriptografi yang lebih tangguh dan dapat diandalkan [10].

2.3 Vigenère Cipher

Sandi Vigenère awalnya digambarkan oleh Giovan Battista Bellaso dalam bukunya "Lacifradel Sig Giovan Battista Bellaso" pada tahun 1553 [12], [13]. Ia membangun sandi atas tabula recta Trithemius, tetapi menambahkan sebuah kunci perulangan untuk menukar setiap huruf abjad sandi [13]. Sandi Vigenère sebenarnya merupakan pengembangan dari sandi Caesar [13]. Vigenère Cipher adalah salah satu algoritma kriptografi klasik yang termasuk dalam kategori cipher polialfabetik. Algoritma ini menggunakan tabel Vigenère untuk melakukan enkripsi dengan cara menggeser huruf-huruf pada plaintext berdasarkan nilai kunci yang diberikan [14]. Setiap karakter dalam plaintext dienkripsi menggunakan karakter kunci yang bersesuaian, sehingga menghasilkan ciphertext yang lebih sulit untuk dipecahkan dibandingkan cipher monoalfabetik.

Vigenère Cipher adalah teknik kriptografi klasik yang menggunakan kunci untuk mengubah teks asli menjadi teks yang tidak dapat dibaca (ciphertext) [11]. Teknik ini dapat diterapkan dengan dua cara, yaitu menggunakan angka dan huruf.

1. Penggunaan Angka dalam Vigenère Cipher

Dalam pendekatan berbasis angka, setiap huruf dalam teks asli digantikan dengan angka yang sesuai dengan urutan abjad, yaitu A = 0, B = 1, C = 2, dan seterusnya hingga Z = 25. Kemudian, angka-angka tersebut akan digabungkan dengan kunci yang juga diubah menjadi angka sesuai urutan abjad. Setiap angka dalam teks asli dijumlahkan dengan angka kunci yang bersesuaian, dan hasilnya akan dikurangi 26 untuk memastikan bahwa hasilnya tetap dalam rentang 0 hingga 25 (modulus 26). Setelah itu, angka yang dihasilkan akan diubah kembali menjadi huruf sesuai urutan abjad. Proses ini memungkinkan untuk mengenkripsi dan mendekripsi pesan dengan kunci yang relatif lebih panjang.

Secara matematis dapat dituliskan dengan rumus sebagai berikut :

1. Formula Proses Enkripsi

$$E = Ci = (Pi + Ki) \ mod \ 26 \quad \text{atau} \quad Ci = (Pi + Ki) - 26 \qquad (1)$$

2. Formula Proses Dekripsi

$D = Pi = (Ci - Ki) \ mod\ 26$ atau
$Pi = (Ci - Ki) + 26$ (2)
Di mana :

- E = Enkripsi
- D = Dekripsi
- Ci = Cipherteks
- Pi = Plainteks
- Ki = Kunci

2.4 Beaufort Cipher

Beaufort Cipher adalah algoritma kriptografi klasik yang mirip dengan Vigenère Cipher tetapi memiliki pola operasi yang berbeda [11], [15]. Alih-alih menambahkan nilai kunci ke plaintext, Beaufort Cipher menggunakan operasi pengurangan dengan tabel Beaufort untuk mengenkripsi data.
Secara matematis dapat dituliskan dengan rumus sebagai berikut :
1. Formula Proses Enkripsi
$E = C = (K - P) \ mod\ 26$
2. Formula Proses Dekripsi
$D = P = (K - C) \ mod\ 26$
Di mana :

- E = Enkripsi
- D = Dekripsi
- P = Plainteks (huruf asli)
- K = Kunci
- C = Cipherteks

2.4 Pembangkit Kunci Blum Blum Shub (BBS)

Algoritma ini didasarkan pada prinsip matematika dari teori bilangan, khususnya terkait dengan masalah faktorisasi bilangan besar dan kestabilan masalah integer quadratic residues [16], [20]. Blum Blum Shub adalah algoritma pembangkit bilangan acak yang telah terbukti andal dan memenuhi standar keamanan dalam bidang kriptografi [17].

Pada dasarnya, Blum Blum Shub menggunakan konsep kesulitan dalam faktorisasi bilangan yang merupakan hasil perkalian dua bilangan prima besar. Blum Blum Shub bekerja dengan prinsip dasar sebagai berikut:

1. Pemilihan bilangan prima
   Pilih dua bilangan prima besar yang saling berbeda, p dan q, di mana keduanya kongruen dengan 3 modulo 4 (artinya $p \equiv 3(mod4)$ dan $q \equiv 3(mod4)$).
2. Menghitung modulus
   Hitung $N = p \times q$ yang merupakan bilangan modulus yang digunakan dalam algoritma.
3. Inisialisasi nilai awal
   Pilih nilai awal x_0 yang merupakan bilangan bulat yang tidak memiliki pembagi bersama dengan N (artinya x_0 harus relatif prima terhadap N).
4. Iterasi Algoritma BBS
   Setelah tahap inisialisasi, urutan angka acak dihasilkan dengan iterasi sebagai berikut:
   $$x_{n+1} = {x_n}^2 mod\ N$$
   Nilai x_n diambil secara berkala dari urutan ini, dan angka acak dihasilkan dari bit-bit terakhir dari setiap x_n.
5. Pengambilan bit acak
   Bit acak dihasilkan dengan mengambil beberapa bit terakhir dari nilai x_n misalnya, bit-bit paling kanan dari x_n.
6. Konversi bit Konversi Bit ke Kunci (Key)
   Bit yang dihasilkan dikonversi ke angka desimal, kemudian hasilnya dimodulo $(mod\ 26)$ untuk substitusi kunci (key) ke alfabet.

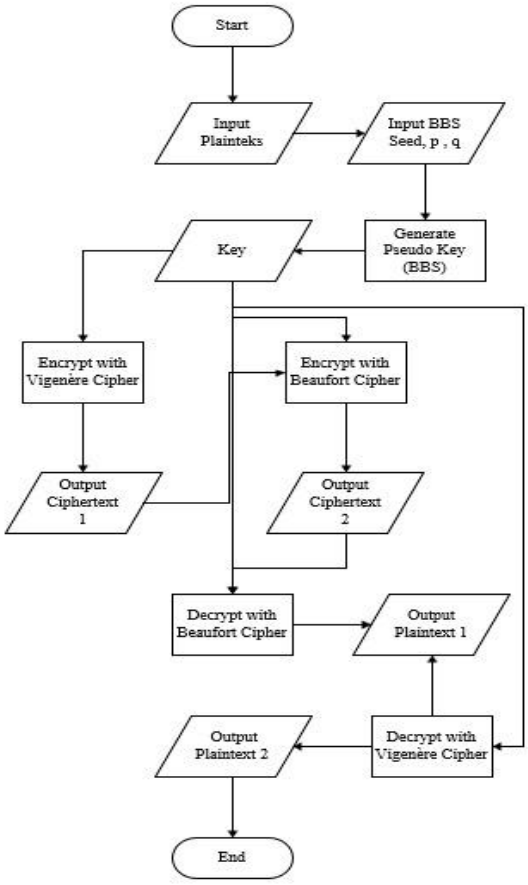
3. HASIL DAN PEMBAHASAN

3.1 Analisis Pembangkitan Kunci Super Enkripsi Vigenère Cipher dan Beaufort Cipher Berdasarkan Teknik Blum-Blum Shub

Pada Kunci yang digunakan dihasilkan oleh algoritma generator bilangan pseudo-acak Blum-Blum Shub (BBS), yang memiliki karakteristik keacakan yang tinggi dan ketahanan terhadap serangan brute force. Dengan

mengintegrasikan teknik BBS dalam pembangkitan kunci, proses super enkripsi diharapkan dapat meningkatkan keamanan pesan teks dari ancaman analisis kriptografi.

Berikut adalah diagram alur proses pembangkitan kunci super enkripsi vigenère cipher dan beaufort cipher berdasarkan teknik blum-blum shub



Gambar 2. Diagram Alur Pembangkitan Kunci Super Enkripsi Vigenère Cipher dan Beaufort Cipher Berdasarkan Teknik Blum-Blum Shub

3.2 Pembangkitan Kunci dengan Teknik Blum Blum Shub Pseudo

Untuk menghasilkan kunci pseudo yang aman dan tidak mudah diprediksi, digunakan algoritma Blum Blum Shub (BBS), yang merupakan salah satu metode pembangkit bilangan acak kriptografi berbasis teori bilangan.

Berikut adalah tahapan proses pembangkitan kunci dengan algoritma Blum Blum Shub.

1. Pemilihan Bilangan Prima
   Dalam algoritma BBS, dua bilangan prima p dan q dipilih, yang memenuhi syarat.
   $p \equiv 3 \; mod \; 4 \; dan \; q \equiv 3 \; mod \; 4$
   - Pada kasus ini, $p = 11$ dan $q = 19$ dipilih.
2. Menghitung modulus
   Hitung $N = p \times q$ yang merupakan bilangan modulus yang digunakan dalam algoritma.
   $$N = p \cdot q = 11 \cdot 19 = 209$$
3. Inisialisai Nilai Awal x_0
   Sebuah bilangan x_0 dipilih sebagai seed awal, dengan syarat $\gcd(x_0, N) = 1$ agar nilai x_0 relatif prima terhadap N.
   - Pada kasus ini, $x_0 = 3$ dipilih.
4. Iterasi Algoritma BBS
   Algoritma Blum Blum Shub menghasilkan bilangan pseudo-random melalui iterasi formulasi berikut:
   $$x_{n+1} = {x_n}^2 \; mod \; N$$

Setiap x_n dihitung dengan cara mengkuadratkan hasil sebelumnya, kemudian mengambil modulus N. Hasil iterasi ini digunakan untuk menghasilkan bit acak dengan mengambil Least Significant Bit (LSB). Berikut adalah hasil perhitungan manual:

- $x_0 = 3$
  $x_1 = 3^2 \; mod \; 209 = 9$
- $x_1 = 9$
  $x_2 = 9^2 \; mod \; 209 = 81$
- $x_2 = 81$
  $x_3 = 81^2 \; mod \; 209 = 121$
- $x_3 = 121$

$x_4 = 121^2 \ mod \ 209 = 144$

- $x_4 = 144$

$x_5 = 144^2 \ mod \ 209 = 16$

5. Pengambilan Bit Acak

Setiap x_n dilakukan ekstraksi ke dalam biner, lalu ambil LSB (Least Significant Bit) dari setiap x_n :

- $x_0 = 9 \rightarrow 1001$
  LSB = 1
- $x_1 = 81 \rightarrow 0101\ 0001$
  LSB = 1
- $x_2 = 121 \rightarrow 0111\ 1001$
  LSB = 1
- $x_3 = 144 \rightarrow 1001\ 0000$
  LSB = 0
- $x_4 = 16 \rightarrow 0001\ 0000$
  LSB = 0

Hasil bit : 11100

6. Konversi Bit ke Kunci (Key)

Bit yang dihasilkan (11100) dikonversi ke angka desimal:

$$11100_2 = 28$$

Karena kunci akan digunakan untuk substitusi alfabet ($mod\ 26$), maka:

$$28 \ mod \ 26 = 2$$

Angka 2 ini dikonversi menjadi huruf alfabet, yaitu **C** (A = 0, B = 1, C = 2). Dengan demikian, kunci (key) pseudo yang dihasilkan adalah huruf **C**, yang dapat digunakan berulang untuk panjang plainteks.

3.3 Enkripsi Menggunakan Vigenère Cipher

Vigenère Cipher bekerja dengan cara menggeser setiap huruf pada plaintext ke depan sejauh nilai kunci yang diberikan. Pada kasus ini, kunci yang digunakan adalah 2, sehingga setiap huruf digeser dua posisi ke depan dalam urutan alfabet.

Plaintext : $KAPUTAMA$

Kunci : 2

Vigenère Cipher menggunakan rumus berikut untuk mengenkripsi huruf

$E = Ci = (Pi + Ki) \ mod \ 26$ atau $Ci = (Pi + Ki) - 26$

Di mana :

a. E = Enkripsi
b. Ci = Cipherteks
c. Pi = Plainteks
d. Ki = Kunci

Langkah-langkah enkripsinya adalah sebagai berikut:

K (posisi 10) dan Kunci (2) dihitung menggunakan rumus:

$$Ci = (10 + 2) \ mod \ 26 = 12$$

1) Huruf ke-12 dalam alfabet adalah M.
   A (posisi 0) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci = (0 + 2) \ mod \ 26 = 2$$

2) Huruf ke-2 dalam alfabet adalah C.
   P (posisi 15) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci = (15 + 2) \ mod \ 26 = 17$$

3) Huruf ke-17 dalam alfabet adalah R.
   U (posisi 20) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci = (20 + 2) \ mod \ 26 = 22$$

4) Huruf ke-22 dalam alfabet adalah W.
   T (posisi 19) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci = (19 + 2) \ mod \ 26 = 21$$

5) Huruf ke-21 dalam alfabet adalah V.
   A (posisi 0) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci = (0 + 2) \ mod \ 26 = 2$$

6) Huruf ke-2 dalam alfabet adalah C.
   M (posisi 12) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci = (12 + 2) \ mod \ 26 = 14$$

7) Huruf ke-14 dalam alfabet adalah O.
A (posisi 2) dan Kunci (2) dihitung menggunakan rumus:
$Ci = (0 + 2) \ mod \ 26 = 2$

8) Huruf ke-2 dalam alfabet adalah C.

Hasil Ciphertext dari Vigenère Cipher :
$\boldsymbol{MCRWVCOC}$

3.4 Enkripsi Menggunakan Beaufort Cipher

Setelah menghasilkan ciphertext dari Vigenère Cipher, kita melanjutkan proses enkripsi menggunakan Beaufort Cipher.
Plaintext: $MCRWVCOC$
Kunci: 2
Beaufort Cipher menggunakan rumus berikut untuk mengenkripsi huruf

$$E = C = (K - P) \ mod \ 26$$

Di mana :
a. E = Enkripsi
b. P = Plainteks (huruf asli)
c. K = Kunci
d. C = Cipherteks

Langkah-langkah enkripsinya adalah sebagai berikut:
1) Huruf M (posisi 12) dihitung dengan rumus $(2 - 12) \ mod \ 26 = (-10)$
$(-10) \ mod \ 26 = 16$. Huruf ke-16 dalam alfabet adalah Q.
2) Huruf C (posisi 2) dihitung dengan rumus $(2 - 2) \ mod \ 26 = 0$
$0 \ mod \ 26 = 0$. Huruf ke-0 dalam alfabet adalah A.
3) Huruf R (posisi 17) dihitung dengan rumus $(2 - 17) \ mod \ 26 = (-15)$
$(-15) \ mod \ 26 = 11$. Huruf ke-11 dalam alfabet adalah L.
4) Huruf W (posisi 22) dihitung dengan rumus $(2 - 22) \ mod \ 26 = (-20)$
$(-20) \ mod \ 26 = 6$. Huruf ke-6 dalam alfabet adalah G.
5) Huruf V (posisi 21) dihitung dengan rumus $(2 - 21) \ mod \ 26 = (-19)$
$(-19) \ mod \ 26 = 7$. Huruf ke-7 dalam alfabet adalah H.
6) Huruf C (posisi 2) dihitung dengan rumus $(2 - 2) \ mod \ 26 = 0$
$0 \ mod \ 26 = 0$. Huruf ke-0 dalam alfabet adalah A.
7) Huruf O (posisi 14) dihitung dengan rumus $(2 - 14) \ mod \ 26 = (-12)$
$(-12) \ mod \ 26 = 14$. Huruf ke-14 dalam alfabet adalah O.
8) Huruf C (posisi 2) dihitung dengan rumus $(2 - 2) \ mod \ 26 = 0$
9) $0 \ mod \ 26 = 0$. Huruf ke-0 dalam alfabet adalah A.

Hasil Ciphertext dari Beaufort Cipher :
$\boldsymbol{QALGHAOA}$

3.5 Dekripsi Menggunakan Beaufort Cipher

Setelah proses enkripsi selesai, kita akan mengembalikan ciphertext dari Beaufort Cipher menjadi ciphertext hasil dari Vigenère Cipher. Karena Beaufort Cipher bersifat self-inverse, proses dekripsi dilakukan dengan metode yang sama seperti proses enkripsi.
Plaintext: $QALGHAOA$
Kunci: 2
Beaufort Cipher menggunakan rumus berikut untuk mengdeskripsi huruf

$$D = P = (K - C) \ mod \ 26$$

Di mana :
a. D = Deskripsi
b. P = Plainteks (huruf asli)
c. K = Kunci
d. C = Cipherteks

Langkah-langkah dekripsinya adalah sebagai berikut:
1) Huruf Q (posisi 16) dihitung dengan $rumus$ $(2 - 16) \ mod \ 26 = (-14)$

$(-14)\ mod\ 26\ =\ 12$. Huruf ke-12 dalam alfabet adalah M.

2) Huruf A (posisi 0) dihitung dengan rumus $(2\ -\ 0)\ mod\ 26\ =\ 2$ $2\ mod\ 26\ =\ 2$. Huruf ke-2 dalam alfabet adalah C.
3) Huruf L (posisi 11) dihitung dengan rumus $(2\ -\ 11)\ mod\ 26\ =\ (-9)$ $(-9)\ mod\ 26\ =\ 17$. Huruf ke-17 dalam alfabet adalah R.
4) Huruf G (posisi 6) dihitung dengan rumus $(2\ -\ 6)\ mod\ 26\ =\ (-4)$ $(-4)\ mod\ 26\ =\ 22$. Huruf ke-22 dalam alfabet adalah W.
5) Huruf H (posisi 7) dihitung dengan rumus $(2\ -\ 7)\ mod\ 26\ =\ (-5)$ $(-5)\ mod\ 26\ =\ 21$. Huruf ke-21 dalam alfabet adalah V.
6) Huruf A (posisi 0) dihitung dengan rumus $(2\ -\ 0)\ mod\ 26\ =\ 2$ $2\ mod\ 26\ =\ 2$. Huruf ke-2 dalam alfabet adalah C.
7) Huruf O (posisi 14) dihitung dengan rumus $(2\ -\ 14)\ mod\ 26\ =(-12)$ $(-12)\ mod\ 26\ =\ 14$. Huruf ke-2 dalam alfabet adalah O.
8) Huruf A (posisi 0) dihitung dengan rumus $(2\ -\ 0)\ mod\ 26\ =\ 2$ $2\ mod\ 26\ =\ 2$. Huruf ke-2 dalam alfabet adalah C.

Hasil Dekripsi dari Beaufort Cipher:

$$\boldsymbol{MCRWVCOC}$$

3.6 Dekripsi Menggunakan Vigenère Cipher

Terakhir Dekripsi pada Vigenère Cipher dilakukan dengan membalik proses enkripsi, yaitu dengan menggeser huruf ciphertext ke belakang sejauh nilai kunci yang diberikan.

Plaintext: $MCRWVCOC$

Kunci: 2

Vigenère Cipher menggunakan rumus berikut untuk mengdeskripsi huruf

$D\ =\ Pi\ =\ (Ci\ -\ Ki\ )\ mod\ 26$ atau

$Pi\ =\ (\ Ci\ -\ Ki\ )\ +\ 26$

Di mana :

a. D = Deskripsi
b. Ci = Cipherteks
c. Pi = Plainteks
d. Ki = Kunci

Langkah-langkah dekripsinya adalah sebagai berikut:

M (posisi 12) dan Kunci (2) dihitung menggunakan rumus:

$$Ci\ =\ (12\ -\ 2)\ mod\ 26\ =\ 10$$

1) Huruf ke-9 dalam alfabet adalah K.
   C (posisi 2) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci\ =\ (2\ -\ 2) mod\ 26\ =\ 0$$
   Huruf ke-0 dalam alfabet adalah A.
   R (posisi 17) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci\ =\ (17\ -\ 2)\ mod\ 26 = 15$$
2) Huruf ke-15 dalam alfabet adalah P.
   W (posisi 22) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci\ =\ (22\ -\ 2)\ mod\ 26\ =\ 20$$
3) Huruf ke-20 dalam alfabet adalah U.
   V (posisi 21) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci\ =\ (21\ -\ 2)\ mod\ 26\ =\ 19$$
4) Huruf ke-19 dalam alfabet adalah T.
   C (posisi 2) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci\ =\ (2\ -\ 2) mod\ 26\ =\ 0$$
   Huruf ke-0 dalam alfabet adalah A.
   O (posisi 14) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci\ =\ (14\ -\ 2) mod\ 26\ =\ 12$$
   Huruf ke-12 dalam alfabet adalah M.
   C (posisi 2) dan Kunci (2) dihitung menggunakan rumus:
   $$Ci\ =\ (2\ -\ 2) mod\ 26\ =\ 0$$

Huruf ke-0 dalam alfabet adalah A.

Hasil Ciphertext dari Vigenère Cipher :

KAPUTAMA

4. KESIMPULAN

Penelitian ini mempunyai kesimpulan penggunaan metode super enkripsi yang mengombinasikan algoritma Vigenère Cipher, Beaufort Cipher, dan generator kunci Blum Blum Shub (BBS) untuk menciptakan sistem pengamanan data yang lebih kuat dan sulit ditembus.

Penggunaan Blum Blum Shub (BBS) sebagai generator kunci acak bertujuan untuk memastikan keamanan kunci. Dengan kunci yang lebih acak, tingkat keamanan data meningkat karena kunci menjadi lebih sulit ditebak oleh pihak yang tidak berwenang. Kombinasi dari ketiga metode tersebut meningkatkan ketahanan sistem terhadap serangan kriptanalisis, seperti serangan brute force dan analisis pola. Karena Beaufort Cipher dan Vigenère Cipher memiliki pola operasi yang berbeda, proses enkripsi ganda ini membuat pola pada ciphertext menjadi sulit dikenali.

Penggunaan BBS sebagai generator kunci juga memberikan tingkat keacakan kunci yang tinggi, sehingga risiko serangan berbasis kunci berulang dapat diminimalkan. Secara keseluruhan.

5. SARAN

Berdasarkan penelitian yang telah dilakukan mengenai super enkripsi menggunakan kombinasi algoritma Vigenère Cipher, Beaufort Cipher, dan Blum Blum Shub (BBS), terdapat beberapa saran untuk pengembangan lebih lanjut:

1. Penelitian selanjutnya disarankan untuk menguji ketahanan metode super enkripsi ini terhadap berbagai serangan kriptografi, seperti brute force dan analisis pola, untuk mengevaluasi tingkat keamanan secara lebih mendalam.
2. Disarankan untuk menerapkan metode ini pada data teks dalam skenario nyata, seperti pengamanan pesan teks dalam aplikasi komunikasi atau data sensitif dalam instansi pemerintah, untuk membuktikan efektivitas dan kepraktisannya.

DAFTAR PUSTAKA

[1] K. Wibowo, U. Hidayat, and V. Yasin, “Kajian Cyber Security Dalam Rangka Koperasi Menghadapi Revolusi Industri 4.0,” *JISAMAR (Journal Inf. Syst. Applied, Manag. Account. Res.*, vol. 7, no. 3, pp. 634–645, 2023.

[2] L. B. Handoko and C. Umam, “KOMBINASI AUTOKEY CIPHER DAN TRANSPOSISI KOLOM DALAM MODEL SUPER ENKRIPSI,” in *Semnas Ristek (Seminar Nasional Riset dan Inovasi Teknologi)*, 2024.

[3] A. Tampubolon, “Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks,” *J. SAINTIKOM (Jurnal Sains Manaj. Inform. Dan Komputer)*, vol. 20, no. 1, pp. 38–43, 2021.

[4] D. Ariyus, *Pengantar ilmu kriptografi: teori analisis & implementasi*. Penerbit Andi, 2008.

[5] J. T. Santoso, “BUKU MONOGRAF Meningkatkan Keamanan Data Pada Attendance System Berbasis Face Recognition: Integrasi Machine Learning, Deep Learning Dan Ensemble Ai Pada Manajemen Proyek Teknologi Informasi,” *Penerbit Yayasan Prima Agus Tek.*, pp. 1–218, 2024.

[6] B. M. Rambe, E. B. Nababan, and M. K. M. Nasution, “Performance Analysis Of The Combination Of Blum Blum Shub And Rc5

Algorithm In Message Security," *J. INFORMATICS Telecommun. Eng.*, vol. 7, no. 2, pp. 409–423, 2024.

[7] G. P. H. Panjaitan, "Sistem Kriptografi Kuantum".

[8] S. D. Santoso, "Implementasi penyandian super enkripsi Vigenere Cipher dan Railfence Cipher menggunakan Python," 2019, *Universitas Islam Negeri Maulana Malik Ibrahim*.

[9] D. A. Putra, "TA: Implementasi Sistem Autentifikasi Terintegrasi pada Domain Controller dan Application Server Labkom Stikom Surabaya," 2011, *Stikom Surabaya*.

[10] Y. P. Ruhiat, "Membangun Sistem Keamanan Siber Di Ibu Kota Nusantara (IKN) Dalam Rangka Menunjang Pembangunan Nasional Yang Berkelanjutan Oleh: Brigadir Jenderal Polisi Kertas Karya Ilmiah Perorangan (Taskap) Program Pendidikan Singkat Angkatan (Ppsa) Xxiv Lemhan," 2023.

[11] A. Fauzi, "Analisa Kombinasi Pesan Teks Ke Dalam File Audio Memanfaatkan Algoritma Data Encryption Standard Dan Metode End of File," *JTIK (Jurnal Tek. Inform. Kaputama)*, vol. 3, no. 1, pp. 1–8, 2019.

[12] L. P. Devi, "Implementasi Algoritma Algoritma Vigenere Chiper Dan Advanced Encryption Standart (Aes) Untuk Keamanan Data Teks," *Bull. Inf. Syst.*, vol. 1, no. 1, pp. 25–29, 2023.

[13] S. A. Zebua, "Modifikasi Algoritma Vigenere Cipher dengan Pembangkit Kunci Random Number Generator Dalam Pengamanan Citra Digital," *J. Comput. Informatics Res.*, vol. 1, no. 3, pp. 71–81, 2022.

[14] L. Agustina, "Membangun super enkripsi dengan Vigenere Cipher dan Bifid Cipher menggunakan pemrograman python untuk mengamankan pesan," 2021, *Universitas Islam Negeri Maulana Malik Ibrahim*.

[15] M. Boru, A. A. Sultani, A. Y. Mauko, S. A. S. Mola, K. Letelay, and D. M. Sihotang, "Kombinasi Cipher Subtitusi (Beaufort Dan Vigenere) Menggunakan Pembangkit Kunci RC4 Pada Kriptogtrafi Video Audio Video Interlaced (AVI)," *Telekontran J. Ilm. Telekomun. Kendali dan Elektron. Terap.*, vol. 12, no. 2, pp. 187–195, 2024.

[16] S. H. Waruwu, "Analisis dan Implementasi Modifikasi Algoritma Kriptografi GOST Menggunakan Blum Blum Shub Generator Pada Sistem Pengamanan Login Pada Website," *KETIK J. Inform.*, vol. 1, no. 03, pp. 30–46, 2024.

[20] 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.

[17] T. B. Surbakti, A. Fauzi, and H. Khair, "Hybrid Sistem Algoritma Rivest Shamir Adleman (RSA) dan Algoritma Blum Blum Shub (BBS) dalam Mengamankan File Database E-Absensi," *Indones. J. Educ. Comput. Sci.*, vol. 1, no. 3, pp. 89–97, 2023.