Jurnal Pelita Informatika, Volume 6, Nomor 4, April 2018
ISSN 2301-9425 (Media Cetak)
Hal: 473-478

PENERAPAN ALGORITMA GOLDBACH CODES PADA KOMPRESI FILE TEKS TERENKRIPSI HILL CIHPER

Ismail Almurtada, Muhammad Syahrizal

Teknik Informatika STMIK Budi Darma, Medan, Indonesia
Jalan Sisingamangaraja No. 338 Simpang Limun, Medan, Indonesia

ABSTRAK

Hill Cipher merupakan salah satu cara untuk menyandikan file, diera yang serba berteknologi canggih ini sangat penting akan adanya keamanan file, hill cipher salah satu algortima kriptografi yang dapat digunakan untuk keamanan tersebut Karena algoritma tersebut dapat mengenkripsikan file tersebut sehingga file tersebut tidak mudah dibukaoleh orang yang tidak berkepentingan. Selain keamanan, hal yang perludi perhatikan juga adalah tentang memori penyimpanan, dengan menggunakan algoritma goldbach codes kita dapat memaksimalkan memori penyimpanan, Karena dapa tmengurangi ukuran file tersebut, selain itu juga dapat lebih meningkatkan keamanan file tersebut.Maka dengan hal ini penulis membuat sebuah aplikasi yang dapa tmembantu dalam pengamanan sebuah file dan dapat memaksimalkan memori penyimpanan Karena file yang sudah dienkripsi akan dikompresi lagi agar dapat memperkuat keamanan dan memperkeci lukuran file tersebut.

KataKunci : Kompresi, FileTeks, AlgoritmaHill Cipher.

I. PENDAHULUAN

Teknologi yang terus berkembang dengan pesat menawarkan kemudahan dalam bertukar informasi secara *global*,hal ini merupakan sebuah keuntungan besar karena selain dapat menghemat waktu dan biaya juga dianggap sangat efisien untuk memenuhi kebutuhan pertukaran data secara *online*, serta terbuka jaringan yang menghubungkan satu komputer dengan komputer lain memungkinkan pertukaran data file teksmaupun data yang lainnya tidak mengenal waktu dan tempatlagi.

Sisi buruk dari ini adalah data yang penting dapat dengan mudah jatuh ketangan orang yang tidak bertanggung jawab disebabkan begitu pentingnya pertukaran informasi di era yang serba maju ini tentunya harus dibarengi dengan keamanan informasi.

Salah saru cara yang untuk mengatasi permasalahan di atas adalah dengan cara menyandikan meyandikan dan mengkompresi file teks tersebut sehingga isi dari file teks tersebut menjadi berubah dan teracak, Kompresi bertujuan untuk mengubah isi dan ekstensi dari file teks tersebut sehingga dapat mengurangi jumlah data yang digunakan untuk mewakili isi file teks, tanpa mengurangi kualitas data aslinya.

Pada penelitian sebelumnya, yang dilakukan oleh Surya Darma Nasution [1] menyimpulkan bahwa hasil file teks sebelum dan sesudah dikompresi setelah dibandingkan telah mencapai 50% rasio perbandingannya. Secara umum data dibedakan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Biasanya data yang biasa tidak terlalu di perhatikan atau tidak dilindungi, sedangkan yang bersifat rahasia, berisi tentang apa saja yang bukan konsumsi publik akan di simpan dan di amankan agar tidak dapat diketahui oleh orang yang tidak berhak oleh Karena itu data tersebut harus di amankan dengan menerapkan algoritma kriptografi.

Dalam penelitian sebelumnya, yang dilakukan oleh Akik Hidayat [2] menyimpulkan bahwa Teori *pseudo invers*, dapat dimanfaatkan pada algoritma Hill Cipher. Hal ini memungkinkan penggunaan matriks persegi panjang m x n ($m \geq n$ dan $n > 1$) pada algoritma Hill Cipher. Dalam penerapannya hill cipher menggunakan Teknik perkalian matrik dan Teknik invers terhadap matriks, kunci yang di gunakan oleh hill cipher adalah perkalian matrik n x n dimana n adalah ukuran blok.

II. TEORITIS

A. Algoritma Hill Cipher

HillCipher adalah salah satu algoritma kriptografi klasik, Algoritma *HillCipher* menggunakan matriks berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi [1]. Dasar teori matriks yang digunakan dalam *Hill Cipher* antara lain adalah perkalian antar matriks dan melakukan invers pada matriks. Dasar dari Dasar dari teknik *Hill Cipher* adalah aritmatika modulo terhadap matriks, *Hill Cipher* menggunakan perkalian matrik n x n, dengan n merupakan ukuran blok. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki inverse K^{-1} sehingga kunci harus memiliki invers, karena matriks K^{-1} tersebut adalah kunci yang digunakan untuk melakukan dekripsi.

Proses enkripsi pada algoritma Hill Cipher dimulai dengan menggonversikan plaintext kedalam angka sesuai dengan table ASCII. Selanjutnya angka–angkatersebut dikelompokkan menjadi beberapa blok, dimana masing-masing blokterdiri dari m anggota sesuai dengan ordo matriks kunci K(mxm). Selanjutnyadicari ciphertext dengan C= K * P.

Proses Dekripsi diawali dengan mengkonversikan ciphertext kedalam angka sesuai dengan table ASCII.Seperti halnya pada proses enkripsi, angka-angka tersebut dikelompokkanmenjadi beberapa blok dengan anggota masing-masing blok sebanyak m, laludicari plaintextnya dengan $P = K^{-1}. C$.

Matriks yang digunakan pada Hill Cipher adalahmatriks yang invertible. Matriks invertible

adalah matriksberukuran n x n dan memiliki determinan ≠ 0 sehinggamemiliki invers. Jika matriks kunci memiliki determinan= 256, maka matriks dapat digunakan dalam prosesenkripsi, namun akaan gagal ketika proses dekripsi.Sehingga penting untuk diperhatikan dalam memilihmatriks kunci yang sesuai.

B. Algoritma Goldbach Codes

Algoritma *Goldbach Codes* adalah algoritma yang di asumsikan menggunakan teori*Goldbach conjecture* yaitu "semua bilangan genap positif yang lebih besar dari 2 merupakan penjumlahan dari dua bilangan prima" [2][4][8].

Goldbach Codes memiliki tiga kode, *Goldbach Codes* yang pertama dinamakan "G0". G0 mengkodekan bilangan bulat positif *n* dengan mengubahnya menjadi bilangan bulat positif genap dengan 2(*n* + 3) dan kemudian menuliskan pasangan penjumlahan bilangan prima dalam keadaan terbalik [2][4][8]. *GoldbachCodes* kedua dinamakan "G1". Prinsip G1 adalah menentukan dua bilangan prima P*i* danP*j* (dimana $i \leq j$) yang jumlahnya menghasilkan bilangan bulat *n*, dan mengkodekan pasangan (*i.j-i*+1) dengan *gamma codes.Goldbach Codes* yang ketiga dinamakan "G2" adalah perluasan dari *G1codes* dengan kasus seperti berikut:

1. Bilangan bulat 1 dan 2 dikodekan menjadi 110 dan 111 (selainbilanganbulat 1 dan 2 tidak adalagi yang pekodeannya dimulai dengan 11…).
2. Bilangan bulat genap dikodekan seperti pada *G1 code*, namun dengan sedikit perbedaan. Jika ditentukan *n* = P*i* dan P*j*, maka akan dikodekan pasangannya (*i*+1, *j* – *i* + 1) menggantikan (*i.j-i*+1). Sehingga, jika*i*= 1, maka akan dikodekan menjadi 010, *gamma code*dari 2. Ini menjadikan bahwa bilangan bulat genap dari G2 *Code* tidak akan dimulai dari 1 dan akan selalu memiliki bentuk 0…:0…
3. Jika *n* adalah bilangan prima P*i*, maka akan dikodekan sebagai *gamma code* dari (*i* + 1) di ikuti oleh 1 tunggal untuk menghasilkan 0…:1.
4. Jika *n* adalah bilangan ganjil tapi bukan bilangan prima, maka G2 *Code* dimulaidari 1 di ikutidengan G2 *code* dari anggka genap*n-1*. Menghasilkan *gamma code* memiliki bentuk 1:0…:0….

Panjang kode G2 lebih sulit diperkirakan, tetapi pada eksperimen yang sederhana yang menghitung kode-kode ini untuk nilain *n* nilai dari 2 sampai 512 menunjukan bahwa panjangnya (yang mana seringkali bervariasi 2-3 bit dari kode ke kode) dapat didekati dengan kelancaran fungsi.

III. ANALISA DAN PEMBAHASAN

Dalam penerapannya, terlebih dahulu dilakukan pembacaan dari isi file teks, format file tesk yang digunakan disini memiliki ekstensi ".txt" dan isi dari file tersebut yang akan natinya di enkripsikan dan hasil dari enkripsinya akan dikompresi kembali.

Misalnya isi dari file teks tersebut adalah "ISMAIL ALMURTHADA" maka proses enkripsinya sebagai berikut:

1. Proses Enkripsi

Secara matematis proses enkripsi pada *Hil lCipher* adalah sebagai berikut:

C = K.P.....(3.1)

dimana:

C=*Ciphertext*

K= Kunci

P=*Plaintex*

plaintext P = ISMAIL ALMURTHADA

Dan kunci K = $\begin{bmatrix}2 & 8 & 1\\8 & 2 & 8\\4 & 5 & 9\end{bmatrix}$, Maka:

a. Koversikan *plaintext* P menjadi angka sesuai tabel ASCII dan bagi digitnya terdiri dari 3 kelompok

P = I S M A I L A L M U R T H A D A

P = 73 83 77 65 73 76 32 65 76 77 85 82 84 72 65 68 65

Kelompok yang di dapat:
(73 83 77), (65 73 76), (32 65 76), (77 85 82), (84 72 65), (68 65 32).

b. Kalikan setiap angka P dengan matriks kunci

K = $\begin{bmatrix}2 & 8 & 1\\8 & 2 & 8\\4 & 5 & 9\end{bmatrix}$

$$\begin{bmatrix}2 & 8 & 1\\8 & 2 & 8\\4 & 5 & 9\end{bmatrix}.\begin{bmatrix}73\\83\\77\end{bmatrix}=\begin{bmatrix}146+ & 664+ & 77\\584+ & 166+ & 616\\292+ & 415+ & 693\end{bmatrix}=\begin{bmatrix}887\\1366\\1400\end{bmatrix}$$

$$\begin{bmatrix}2 & 8 & 1\\8 & 2 & 8\\4 & 5 & 9\end{bmatrix}.\begin{bmatrix}65\\73\\76\end{bmatrix}=\begin{bmatrix}130+ & 584+ & 76\\520+ & 146+ & 608\\260+ & 365+ & 684\end{bmatrix}=\begin{bmatrix}790\\1274\\1309\end{bmatrix}$$

$$\begin{bmatrix}2 & 8 & 1\\8 & 2 & 8\\4 & 5 & 9\end{bmatrix}.\begin{bmatrix}32\\65\\76\end{bmatrix}=\begin{bmatrix}64+ & 520+ & 76\\256+ & 130+ & 608\\128+ & 325+ & 684\end{bmatrix}=\begin{bmatrix}660\\994\\1137\end{bmatrix}$$

$$\begin{bmatrix}2 & 8 & 1\\8 & 2 & 8\\4 & 5 & 9\end{bmatrix}.\begin{bmatrix}77\\85\\82\end{bmatrix}=\begin{bmatrix}154+ & 680+ & 82\\616+ & 170+ & 656\\308+ & 425+ & 738\end{bmatrix}=\begin{bmatrix}916\\1442\\1471\end{bmatrix}$$

$$\begin{bmatrix}2 & 8 & 1\\8 & 2 & 8\\4 & 5 & 9\end{bmatrix}.\begin{bmatrix}84\\72\\65\end{bmatrix}=\begin{bmatrix}168+ & 576+ & 65\\672+ & 144+ & 520\\336+ & 360+ & 585\end{bmatrix}$$
$$=\begin{bmatrix}809\\1336\\1281\end{bmatrix}$$

$$\begin{bmatrix}2 & 8 & 1\\8 & 2 & 8\\4 & 5 & 9\end{bmatrix}.\begin{bmatrix}68\\65\\32\end{bmatrix}=\begin{bmatrix}136+ & 520+ & 32\\544+ & 130+ & 256\\272+ & 325+ & 288\end{bmatrix}$$
$$=\begin{bmatrix}688\\930\\885\end{bmatrix}$$

2. Lakukan operasi mod 256 kepada setiap hasil matriks angka tersebut

$$\begin{bmatrix}887\\1366\\1400\end{bmatrix} Mod\ 256=\begin{bmatrix}119\\86\\120\end{bmatrix}$$

$$\begin{bmatrix}790\\1274\\1309\end{bmatrix} Mod\ 256=\begin{bmatrix}22\\250\\29\end{bmatrix}$$

$$\begin{bmatrix}660\\994\\1137\end{bmatrix} Mod\ 256=\begin{bmatrix}148\\226\\113\end{bmatrix}$$

$$\begin{bmatrix}916\\1442\\1471\end{bmatrix} Mod\ 256=\begin{bmatrix}148\\162\\191\end{bmatrix}$$

$$\begin{bmatrix}809\\1336\\1281\end{bmatrix} Mod\ 256=\begin{bmatrix}41\\56\\1\end{bmatrix}$$

$$\begin{bmatrix}688\\930\\885\end{bmatrix} Mod\ 256=\begin{bmatrix}176\\162\\117\end{bmatrix}$$

3. Ubahsetiapmatriksangkamenjadihurufdenganaturankonversisesuaitabel ASCII

$$\begin{bmatrix}119\\86\\120\end{bmatrix}=\begin{bmatrix}w\\v\\x\end{bmatrix}$$

$$\begin{bmatrix}22\\250\\29\end{bmatrix}=\begin{bmatrix}¶\\ú\\\end{bmatrix}$$

$$\begin{bmatrix}148\\226\\113\end{bmatrix}=\begin{bmatrix}"\\â\\q\end{bmatrix}$$

$$\begin{bmatrix}148\\162\\191\end{bmatrix}=\begin{bmatrix}"\\¢\\¿\end{bmatrix}$$

$$\begin{bmatrix}41\\56\\1\end{bmatrix}=\begin{bmatrix})\\8\\¶\end{bmatrix}$$

$$\begin{bmatrix}176\\162\\117\end{bmatrix}=\begin{bmatrix}°\\¢\\u\end{bmatrix}$$

4. Di dapatkan teks ISMAIL ALMURTHADA yang telah terenkripsi menjadi “wvx¶ú "âq"¢¿)8¶°¢u”

2. Proses Kompresi

Tabel 1. Data SebelumDikompresi

Char	Freq	ASCII Decimal	ASCII Binary	Bit	Bit x Freq
w	1	119	01110111	8	8
y	1	118	01110110	8	8
x	1	120	01111000	8	8
¶	2	22	00010110	8	16
ú	1	250	11111010	8	8
	1	32	00100000	8	8
"	2	34	00100010	8	16
â	1	226	11100010	8	8
q	1	113	01110001	8	8
¢	2	162	10100010	8	16
¿	1	191	10111111	8	8
)	1	41	00101001	8	8
8	1	56	00111000	8	8
°	1	176	10110000	8	8
u	1	117	01110101	8	8
Jumlah Bit x *Frequency*					112

Hasil kompresi menggunakan algoritma Goldbach Codes dapat dilihat pada table 2 berikut ini:

Tabel 2. Data SetelahDikompresi

Char	Freq	n	2(n+3)	Bilangan Prima	*Codeword*	Bit	Bit x Freq
¶	2	1	8	3 + 5	11	2	4
"	2	2	10	3 + 7	101	3	6
¢	2	3	12	5 + 7	011	3	6
q	1	4	14	3 + 11	1001	4	4
u	1	5	16	5 + 11	0101	4	4
v	1	6	18	7 + 11	0011	4	4
w	1	7	20	7 + 13	00101	5	5
x	1	8	22	5 + 17	010001	6	6
	1	9	24	11 + 13	00011	5	5
ú	1	10	26	7 + 19	0010001	7	7
â	1	11	28	11 + 17	000101	6	6
¿	1	12	30	13 + 17	000011	6	6
)	1	13	32	13 + 19	0000101	7	7
8	1	14	34	11 + 23	00010001	8	8
°	1	15	36	17 + 19	0000011	7	7
Jumlah Bit x *Frequency*							85

Pada tabel 2. menunjukan bahwa teks tersebut memiliki jumlah kapasitas berkurang menjadi 85 bit, maka rasio kompresi:

$$\text{Rasio}=\frac{\text{Ukuran File Terkompresi}}{\text{Ukuran File Asli}}\text{x 100 \%}$$

$$\text{Rasio}=\frac{85}{112}\text{x 100 \% = 75\%}$$

Hasil dari rasio kompresinya adalah 75% itu artinya 75% dari kapasitas file teks telah dimanpatkan atau di kompres.

Langkah selanjutnya adalah menyusun kembali kode-kode yang telah dibuat pada tabel sesuai dengan posisi karakter pada string. String yang telah dibaca dari file teks adalah “wvx¶ú "âq"¢¿)8¶°¢u”, Sehingga diperoleh string bit sebagai berikut :
00101001101000111001000100011101000010110011
01011000011000010100010001110000011010101

Pada proses dekompresi atau pengembalian ke data awal dapat dilakukan dengan cara pembacaan pada string bit yang diperoleh pada proses kompresi terhadap table 2. Pembacaan string bit dilakukan dari indeks terkecil sampai indeks terakhir dengan terus menambahkan nilai pada indeks sebelumnya yang tidak mewakili karakter pada tabel 2.

Proses dekripsi pada *hil lcipher* pada dasarnya saman dengan proses enkripsinya. Namun matriks kunci harus dibalik (*invers*) terlebih dahulu, secara matematis proses dekripsi pada *hil lciphe r*dapat di turunkan dari persamaan berikut

$C = K \cdot P$

$K^{-1}. C = K^{-1}. K . P$

$K^{-1}. C = I . P$

$P = K^{-1} . C$

Sehingga proses dekripsi dapat di tulis dengan persamaan:

$P = K^{-1} . C$

Dimana:

P = *Plaintext*

K^{-1} = *invers*matrikskunci

C = *Ciphertext*

Dengan menggunakan kunci$K = \begin{bmatrix} 2 & 8 & 1 \\ 8 & 2 & 8 \\ 4 & 5 & 9 \end{bmatrix}$, maka

proses dekripsi diawali dengan mencari *invers* K.

Determinan K $\begin{bmatrix} 2 & 8 & 1 \\ 8 & 2 & 8 \\ 4 & 5 & 9 \end{bmatrix} \begin{bmatrix} 2 & 8 \\ 8 & 2 \\ 4 & 5 \end{bmatrix}$

detK=(2x2x9+8x8x4+1x8x5)-(4x2x1+5x8x2+9x8x8) = -332

Minor:

$\lvert M_{11}\rvert = \begin{bmatrix} 2 & 5 \\ 9 & 8 \end{bmatrix}$ $\lvert M_{11}\rvert = 2x9 - 5x8 = -22$	$\lvert M_{12}\rvert = \begin{bmatrix} 8 & 5 \\ 1 & 9 \end{bmatrix}$ $\lvert M_{12}\rvert = 8x9 - 1x5 = 67$	$\lvert M_{13}\rvert = \begin{bmatrix} 8 & 2 \\ 1 & 8 \end{bmatrix}$ $\lvert M_{13}\rvert = 8x8 - 1x2 = 62$
$\lvert M_{21}\rvert = \begin{bmatrix} 8 & 4 \\ 8 & 9 \end{bmatrix}$ $\lvert M_{21}\rvert = 8x9 - 4x8 = 40$	$\lvert M_{22}\rvert = \begin{bmatrix} 2 & 4 \\ 1 & 9 \end{bmatrix}$ $\lvert M_{22}\rvert = 2x9 - 1x4 = 14$	$\lvert M_{23}\rvert = \begin{bmatrix} 2 & 8 \\ 1 & 8 \end{bmatrix}$ $\lvert M_{23}\rvert = 2x8 - 1x8 = 8$
$\lvert M_{31}\rvert = \begin{bmatrix} 8 & 4 \\ 2 & 5 \end{bmatrix}$ $\lvert M_{31}\rvert = 8x5 - 2x4 = 32$	$\lvert M_{32}\rvert = \begin{bmatrix} 2 & 4 \\ 8 & 5 \end{bmatrix}$ $\lvert M_{32}\rvert = 2x5 - 8x4 = -22$	$\lvert M_{33}\rvert = \begin{bmatrix} 2 & 8 \\ 8 & 2 \end{bmatrix}$ $\lvert M_{33}\rvert = 2x2 - 8x8 = -60$

$Adj\text{K} = \begin{bmatrix} -22 & 67 & 62 \\ 40 & 14 & 8 \\ 32 & -22 & 60 \end{bmatrix} x \begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$

$Adj\text{K} = \begin{bmatrix} -22 & -67 & 62 \\ -40 & 14 & -8 \\ 32 & 22 & 60 \end{bmatrix}$

Invers matrik:

$K^{-1} = \frac{1}{-332} \begin{bmatrix} 2 & -8 & 1 \\ -8 & 2 & -8 \\ 4 & -5 & 9 \end{bmatrix}$

$K^{-1} = \begin{bmatrix} -664 & -2656 & -332 \\ -2656 & -664 & -2656 \\ -1328 & -1660 & -2988 \end{bmatrix} Mod\ 256$

$K^{-1} = \begin{bmatrix} -152 & -96 & -76 \\ -96 & -152 & -96 \\ -48 & -124 & -172 \end{bmatrix}$

Matrik K^{-1} akan menjadi matriks kunci pada proses dekripsi, maka:

a. Bagi *plaintext* P menjadi matriks 3x1 dan konversikan keangka sesuai dengan tabel ASCII

$\begin{bmatrix} w \\ v \\ x \end{bmatrix} = \begin{bmatrix} 119 \\ 86 \\ 120 \end{bmatrix}$

$\begin{bmatrix} ¶ \\ ú \\ \end{bmatrix} = \begin{bmatrix} 22 \\ 250 \\ 29 \end{bmatrix}$

$\begin{bmatrix} " \\ â \\ q \end{bmatrix} = \begin{bmatrix} 148 \\ 226 \\ 113 \end{bmatrix}$

$\begin{bmatrix} " \\ ¢ \\ ¿ \end{bmatrix} = \begin{bmatrix} 148 \\ 162 \\ 191 \end{bmatrix}$

$\begin{bmatrix}) \\ 8 \\ ¶ \end{bmatrix} = \begin{bmatrix} 41 \\ 56 \\ 1 \end{bmatrix}$

$\begin{bmatrix} ° \\ ¢ \\ u \end{bmatrix} = \begin{bmatrix} 176 \\ 162 \\ 117 \end{bmatrix}$

b. Kalikan setiap angka dengan matriks kunci

$K^{-1} = \begin{bmatrix} -152 & -96 & -76 \\ -96 & -152 & -96 \\ -48 & -124 & -172 \end{bmatrix} . \begin{bmatrix} -152 & -96 & -76 \\ -96 & -152 & -96 \\ -48 & -124 & -172 \end{bmatrix} . \begin{bmatrix} 119 \\ 86 \\ 120 \end{bmatrix}$

$= \begin{bmatrix} -18088 - 8256 - 9120 \\ -11424 - 13072 - 11520 \\ -5712 - 10664 - 20640 \end{bmatrix} = \begin{bmatrix} -35464 \\ -36016 \\ -37016 \end{bmatrix}$

$K^{-1} = \begin{bmatrix} -152 & -96 & -76 \\ -96 & -152 & -96 \\ -48 & -124 & -172 \end{bmatrix} . \begin{bmatrix} 22 \\ 250 \\ 29 \end{bmatrix}$

$$= \begin{bmatrix} -3344 - 24000 - 2204 \\ -2112 - 38000 - 2784 \\ -1056 - 31000 - 4988 \end{bmatrix} = \begin{bmatrix} -29548 \\ -42896 \\ -37044 \end{bmatrix}$$

c. Lakukan operasi mod 256 kepada setiap matriks angka tersebut agar dapat di konversi menggunakan tabel ASCII

$$\begin{bmatrix} -35464 \\ -36016 \\ -37016 \end{bmatrix} Mod\ 256 = \begin{bmatrix} 73 \\ 83 \\ 77 \end{bmatrix}$$

$$\begin{bmatrix} -29548 \\ -42896 \\ -37044 \end{bmatrix} Mod\ 256 = \begin{bmatrix} 65 \\ 73 \\ 76 \end{bmatrix}$$

$$\begin{bmatrix} -52780 \\ -59408 \\ -54564 \end{bmatrix} Mod\ 256 = \begin{bmatrix} 32 \\ 65 \\ 76 \end{bmatrix}$$

$$\begin{bmatrix} -52564 \\ -57168 \\ -60044 \end{bmatrix} Mod\ 256 = \begin{bmatrix} 77 \\ 85 \\ 82 \end{bmatrix}$$

$$\begin{bmatrix} -11684 \\ -12544 \\ -9084 \end{bmatrix} Mod\ 256 = \begin{bmatrix} 84 \\ 72 \\ 65 \end{bmatrix}$$

$$\begin{bmatrix} -51196 \\ -52752 \\ -48660 \end{bmatrix} Mod\ 256 = \begin{bmatrix} 68 \\ 65 \\ 32 \end{bmatrix}$$

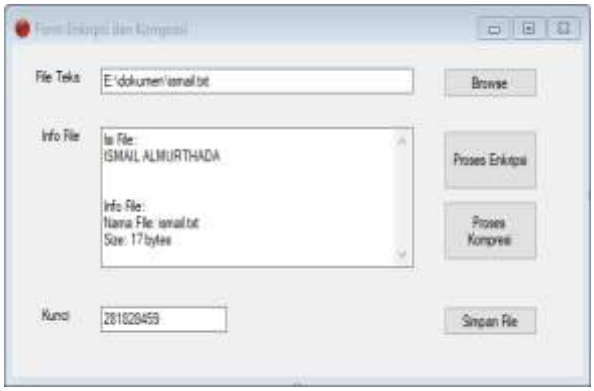
d. Didapatkan teks “wvx¶ú"âq"¢¿)8¶°¢u” yang telah didekripsi menjadi “ISMAIL ALMURTHADA”.

IV. IMPLEMENTASI

Implementasi sistem program ini mencakup spesifikasi kebutuhan perangkat keras (*hardware*) dan spesifikasi perangkat lunak (*software*). Tampilan program terdiri dari *print screen* dari tampilan *input, output*, dan proses yang dirancangan. Adapun tampilan program yang dirancang adalah sebagai berikut:

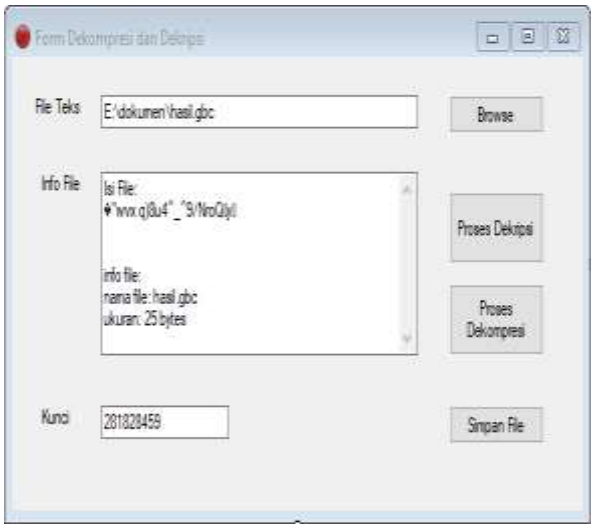
Gambar 1. *Form* Menu Utama

Gambar 1 *Form* menu utama merupakan tampilan yang pertama kali muncul ketika menjalan program. Pada tahap ini akan muncul beberapa pilihan menu yang berfungsi untuk mengakses *form-form* yang terdapat di dalam sistem tersebut.



Gambar 2 *Form* Enkripsi dan Kompresi

Pada gambar 2 merupakan *form* ini akan ditampilkan proses enkripsi *file* teks berektensi.txt dengan menggunakan algoritma *Hill Cipher*. Dimana dalam prosesnya terlebih dahulu *user* menginputkan *file* yang akan dikompresi dalam bentuk file teks dan diikuti dengan melakukan proses enkripsi terlebih dahulu terhadap *file* tersebut. Selanjutnya *user* melakukan proses kompresi lalu menyimpan file tersebut dengan ekstensi.*gbc*. Ada pun gambar proses tersebut dapat dilihat pada gambar dibawah ini :



Gambar 3 *Form* Dekompresi dan Dekripsi

Pada gambar 3 adalah proses dekompresi *file* teks berektensi *.gbc (Goldbach Compression)* dengan menggunakan algoritma *Goldbach Codes*. Dimana dalam prosesnya terlebih dahulu *user* menginputkan *file* yang akan di dekompresi kedalam bentuk file teks dan selanjutnya *user* melakukan proses dekripsi untuk mengembalikan teks kebentuk awal dan kemudian memilih lokasi penyimpanan yang di dekripsi dengan ekstensi *.txt*.

V. KESIMPULAN

Dari hasil penelitian dan pembahsan pada bab-bab sebelumnya, maka penulis dapat mengambil suatu kesimpulan sebagai berikut:

1. Algoritma *Goldbach Codes* merupakan algoritma pengkompresian file yang cukup handal dalam proses pengkompresian file.
2. Dengan adanya aplikasi pengkompresian data teks menggunakan metode *Goldbach Codes* dapat memberikan kemudahan bagi pengguna untuk lebih mengamankan data dan menghemat memori yang dimilikinya.
3. Dalam perancangan aplikasi ini menggunakan bahasa pemrograman *Visual Basic 2008* file teks dari hasil enkripsi *Hill Cipher* kemudian dikompresi Karena hasil dan isi enkripsi berubah kebentuk dan karakter lain, sehingga membuat data lebih aman.

REFERENCES

[1] A. Hidayat and T. Alawiyah, "Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang," Matematika Integratif, vol. 9, no. 1412-6184, pp. 39 - 51, 2013.

[2] S.D. Nasution, PERANCANGAN APLIKASI KOMPRESI FILE TEKS DENGAN MENERAPKAN ALGORITMA GOLDBACH CODES, J. Ilm. INFOTEK. 1 (2013) 104–109.

[3] W. Komputer, Pemrograman Visual Basic 2008, Salemba Infotek, 2009.

[4] S.D. Nasution, G.L. Ginting, M. Syahrizal, R. Rahim, Data Security Using Vigenere Cipher and Goldbach Codes Algorithm, Int. J. Eng. Res. Technol. 6 (2017) 360–363.

[5] R. Rahim, Mesran, M. Syahrizal, and A. P. U. Siahaan, "Data Security with International Data Encryption Algorithm," J. Online Jar. COT POLIPD, vol. 8, no. 1, pp. 63–68, 2017.

[6] M. Syahrizal, Murdani, S. D. Nasution, Mesran, R. Rahim, and A. P. U. Siahaan, "Modified Playfair Cipher Using Random Key Linear Congruent Method," J. Online Jar. COT POLIPD, vol. 8, no. 1, pp. 45–49, 2017.

[7] S.Perkasa, M. Syahrizal, and P. B. N. Simangunsong, "IMPLEMENTASI KEAMANAN DATA TEKS DENGAN ALGORITMA MODIFIKASI CAESAR CHIPER DAN MENGKOMPRESI FILE MENGGUNAKAN ALGORITMA SHANNON FANO," Infotek, vol. 2, no. 1, pp. 69–73, 2017.

[8] S.D. Nasution, Mesran, Goldbach Codes Algorithm for Text Compression, IJournals Int. J. Softw. Hardw. Res. Eng. 4 (2016) 43–46.