e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI : https://dx.doi.org/10.30872/jim.v18i2.17707

Kriptografi Berbasis Jam dengan Metode Base32 untuk Memperkuat Keamanan Data di Era Industri 4.0

Mardi Hardjianto[1], Yogie Setiawan Nugraha[2], Savero Winudhapratama[3]
[1,2,3)] Fakultas Teknologi Informasi, Program Studi Ilmu Komputer, Universitas Budi Luhur, Jakarta, Indonesia
E-Mail : mardi.hardjianto@budiluhur.ac.id [1)]; 2211601659@student.budiluhur.ac.id [2)];
2211602210@student.budiluhur.ac.id [3)];

ABSTRAK

Keamanan informasi menjadi perhatian utama di era Industri 4.0 di Indonesia karena potensi kerugian akibat kebocoran informasi rahasia. Penelitian ini mengusulkan kriptografi berbasis jam sebagai solusi untuk memperkuat keamanan data dengan merancang model enkripsi menggunakan sudut jarum jam sebagai variabel kunci. Kriptografi jam diuji dengan beberapa parameter dan diterapkan metode Base32 dalam proses enkripsi dan dekripsi. Hasil penelitian menunjukkan bahwa kriptografi berbasis jam dengan konversi ke dalam Base32 mampu menghasilkan cipher text yang sulit dikenali dan memiliki format yang beragam. Sudut jarum jam dan menit dapat dijadikan kunci dalam kriptografi, menunjukkan potensi pengembangan lebih lanjut dari algoritma ini.

Kata Kunci – Keamanan, Kriptografi, Industri 4.0, Base32, Enkripsi, Dekripsi, Potensi.

1. PENDAHULUAN

Industri 4.0 menghadirkan tantangan baru dalam keamanan informasi di Indonesia, dengan meningkatnya penggunaan internet dan teknologi untuk pertukaran data yang cepat dan luas. Menurut survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pengguna internet di Indonesia meningkat secara signifikan pada tahun 2023, mencapai 215,63 juta orang, meningkat 2,67% dari periode sebelumnya (Finaka, Nurhanisah & Devina, 2023). Meskipun internet memberikan manfaat besar, namun risiko keamanan yang menyertainya tidak dapat diabaikan (Mido et al., 2022).

Perkembangan teknologi yang pesat juga mendorong penggunaan teknologi dalam pengelolaan data rahasia, seperti di PT. Gunung Geulis Elok Abadi yang mengelola data keuangan, bahan baku, dan informasi member secara elektronik (Suranta & Sakti, 2022). Perlindungan data rahasia ini sangat penting untuk mencegah akses yang tidak sah dan pencurian data (Azhari, Mulyana, Perwitosari & Ali, 2022).

Kriptografi muncul sebagai teknik penting dalam melindungi informasi dari ancaman siber (Ratna Sari & Pawelloi, 2022). Dalam penelitian ini, kami merancang model enkripsi menggunakan sudut antara jarum panjang dan pendek dari jam serta algoritma Base32. Setiap sudut yang dibentuk oleh jarum panjang dan pendek digunakan sebagai variabel untuk memodifikasi kunci dalam proses enkripsi, dengan harapan memperkuat kunci utama dan membuatnya sulit terbaca.

Penelitian ini juga menyoroti pentingnya keamanan data dalam sektor kesehatan, seperti pada sistem informasi pasien di Klinik Kecantikan Ratu Beauty Studio yang memerlukan perlindungan khusus (Listiani et al., 2022). Penelitian sebelumnya menunjukkan berbagai metode kriptografi, termasuk kombinasi RSA dan Steganografi LSB (Mido & Ujianto, 2022), kriptografi visual skema meaningful shares dan steganografi LSB (Darmawan, Kusyanti & Primananda, 2022), dan metode Merkle Hellman Knapsack berbasis Android (Sari & Pawelloi, 2022).

Pengembangan kriptografi berbasis jam dengan metode Base32 diharapkan dapat memberikan lapisan keamanan tambahan yang responsif terhadap tantangan keamanan data yang terus berkembang. Studi ini bertujuan untuk merinci dan menguji efektivitas kriptografi berbasis jam sebagai langkah maju dalam memperkuat keamanan data di berbagai sektor.

2. TINJAUAN PUSAKA

2.1 Konsep Dasar Kriptografi

Kriptografi merupakan ilmu dan seni untuk mengamankan informasi sehingga hanya pihak yang berwenang yang dapat mengakses dan memahami informasi tersebut. Dalam konteks keamanan informasi, kriptografi berperan penting dalam melindungi data dari akses yang tidak sah, pengubahan, dan penghapusan. Kriptografi telah menjadi teknik utama dalam mengatasi ancaman siber (Ratna Sari & Pawelloi, 2022).

2.2 Metode Base32

Base32 adalah skema pengkodean binary-to-text yang mewakili data biner dalam bentuk yang tidak sensitif dan dapat digunakan untuk mewakili urutan arbitrari dari octet. Setiap karakter dalam Base32 mewakili 5 bit dari data biner, sehingga menghasilkan karakter yang dapat dicetak dan tidak sensitif terhadap case. Base32 menggunakan 32 karakter yang terdiri dari huruf A-Z dan angka 2-7, dengan karakter '=' sebagai padding jika diperlukan (RFC 4648, 2006).

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI : https://dx.doi.org/10.30872/jim.v18i2.17707

3. METODE PENELITIAN

3.1 Tahapan Penelitian

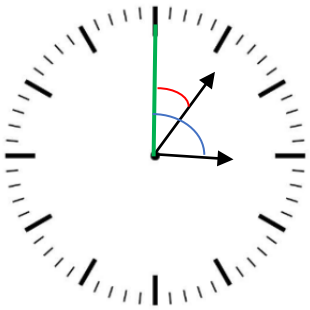
Untuk mencapai hasil yang baik dalam penelitian ini, maka perlunya dibuatkan tahapan-tahapan penelitian. Tahapan penelitian ini berguna sebagai dasar untuk mengerjakan penelitian menjadi terstruktur. Adapun tahapannya antara lain adalah:

1. **Mencari Sudut Antara Jarum Panjang dan Pendek**: Melakukan pencarian sudut antara jarum panjang dan pendek sebagai bagian dari metode penelitian.
2. **Merancang Model Enkripsi**: Merancang model enkripsi menggunakan kunci berupa sudut antara jarum panjang dan jarum pendek dari jam serta algoritma Base32.
3. **Penerapan Metode Kriptografi**: Penerapan metode kriptografi AES untuk sudut jarum jam dan model enkripsi.
4. **Uji Coba Kriptografi Jam**: Melakukan uji coba kriptografi jam dengan beberapa parameter yang menguji variasi *cipher text* dengan kemungkinan sudut jam yang dianggap sama atau kata sandi sama dengan *plain text* yang konstan.
5. **Aplikasi Simulasi Kriptografi Jam**: Membuat aplikasi simulasi kriptografi jam dengan halaman enkripsi dan dekripsi.
6. **Kesimpulan**: Menarik kesimpulan dari hasil penelitian yang dilakukan.
7. **Pengembangan Lebih Lanjut**: Menyatakan potensi pengembangan lebih lanjut dari penelitian ini, seperti pada pesan bersandi yang hanya bisa dibaca pada jam dan menit yang sudah ditentukan.

Dengan melakukan langkah-langkah tersebut, penelitian ini bertujuan untuk menguji efektivitas kriptografi berbasis jam sebagai langkah maju dalam memperkuat keamanan data di berbagai sektor.

3.2 Mencari Sudut Antara Jarum Panjang dan Pendek

Setiap jam dan menit akan membentuk suatu sudut. Sudut tersebut dapat dihitung menggunakan beberapa tahapan dan langkah. Sebelum melakukan tahapan dan langkah maka harus di definisikan dulu konsepnya. Pada Gambar 1. terlihat bahwa kita akan memperhitungkan selisi antar sudut menit dan sudut jam untuk menemukan selisih sudut antara menit dan jam.



Gambar 1. Sudut Jam dan Menit

Konsep Dasar

Perlu kita ketahui beberapa konsep dasar sebagai berikut:

a. Jarum Jam

$$12\ Jam\ (H) = 360° \quad (2.1)$$
$$1H = 30°$$

Keterangan: H = Jam

Untuk setiap menit yang bergerak kita perlu menghitung juga karena jarum jam akan bergerak ketika menit bergerak sehingga didapat persamaan 2.2:

$$1H = 60\ Menit\ (M) = 30° \quad (2.2)$$
$$1\ (M) = \frac{1}{2}°$$

Keterangan: H = Jam
M = Menit

Dari kedua persamaan tersebut maka kita dapatkan untuk setiap jam adalah persamaan 2.3:

$$30H + \frac{1}{2}M \quad (2.3)$$

Keterangan: H = Jam
M = Menit

Sebagai contoh pada jam 03:40 sudut yang terbentuk untuk jarum jam terhadap poros tengah (jam 12) adalah:

$$30H + \frac{1}{2}M = (30 * 3) + \left(\frac{1}{2} * 40\right)$$

$$90 + 20 = 110°$$

Keterangan: H = Jam
M = Menit

b. Jarum menit

DOI : https://dx.doi.org/10.30872/jim.v18i2.17707 e-ISSN 2597-4963 dan p-ISSN 1858-4853

$$60\,M = 360° \quad (2.4)$$
$$1\,M = 6°$$

Keterangan: M = Menit

Dari kedua persamaan tersebut dapat disimpulkan untuk mencari sudut dengan mengetahui jarum jam dan menit menjadi seperti persamaan 2.5:

$$= \left| (6M) - \left(30H + \frac{1}{2}M\right)\right| \quad (2.5)$$

$$= \left| 6M - 30H - \frac{1}{2M}\right|$$

$$= \left|\frac{12}{2}M - \frac{1}{2M} - 30H\right|$$

$$= \left|\frac{11}{2}M - 30H\right|$$

Keterangan: H = Jam
M = Menit

3.3 Metode Base32

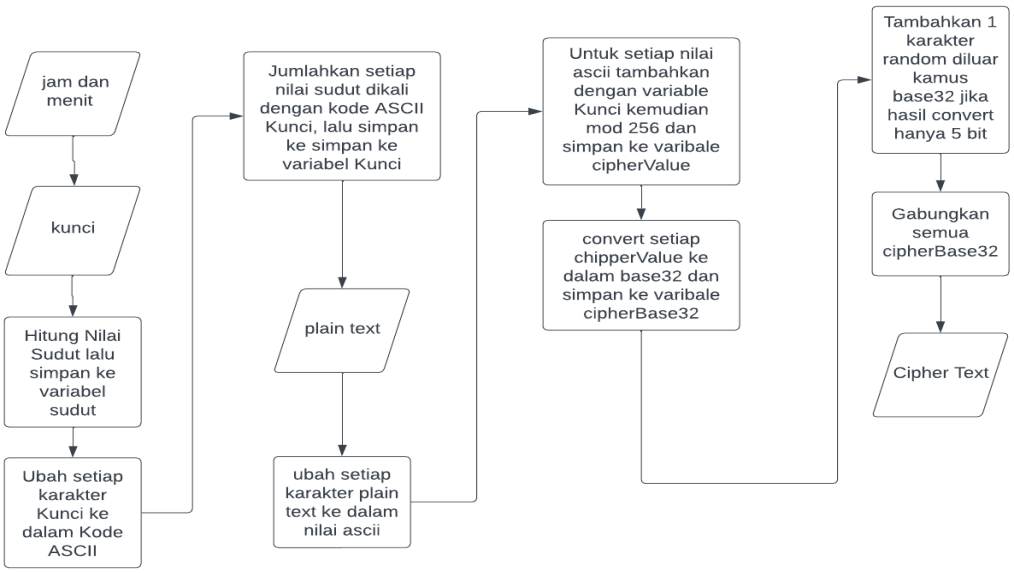
Base32 adalah skema pengkodean *binary-to-text* yang mewakili data biner dalam bentuk yang tidak sensitif dan dapat digunakan untuk mewakilkan urutan arbitrari dari *octet*. Ini menggunakan subset 33 karakter US-ASCII untuk mewakili 5 bit per karakter yang dapat dicetak, dengan karakter ke-33 "=", yang berarti fungsi pemrosesan khusus. Setiap karakter berurutan dalam nilai base-32 mewakili 5 bit berturut-turut dari urutan *octet* yang mendasari, dan setiap kelompok 8 karakter mewakilkan urutan 5 octet (40 bit). *Alphabet* dasar 32 terdiri dari 32 karakter yang dapat dicetak. Pengolahan khusus dilakukan jika kurang dari 40 bit tersedia pada akhir data yang dikodekan, dan *padding* di akhir data dilakukan dengan menggunakan karakter "=".

4. HASIL DAN PEMBAHASAN

Ide dasar dari kriptografi ini adalah menggunakan sudut jarum jam terhadap menit untuk mempengaruhi nilai kunci yang digunakan sebagai faktor penentu perubahan nilai suatu ASCII.
Dalam membentuk suatu *cipher text*, kita akan mendestruksi nilai ASCII yang selanjutnya diubah menjadi bentuk base32 sehingga berubah nilai dari bentuk aslinya. Saat ini perubahan itu akan dilakukan dengan menggunakan perhitungan kombinasi kunci dan nilai jam.

4.1 Rancang Model Enkripsi

Dalam rancangan model enkripsi ini dilakukan beberapa tahapan yang meliputi pembentukan kunci, mengambil nilai ASCII, melakukan enkripsi, mengubah nilai ASCII modifikasi ke bentuk base32, kemudian melakukan proses dekripsi. Adapun lebih detail terlihat pada Gambar 2:



Gambar 2. Flow Chart Enkripsi

Terlihat pada gambar 2 bahwa proses pembentukan kunci diperkaya dengan penggunaan nilai sudut jam sebagai *variable* yang melakukan penambahan nilai ASCII untuk selanjutnya dilakukan operasi modulus. Dalam implementasinya memang ada beberapa metode yang harus melalui tahapan modifikasi. Modifikasi itu antara lain:

a. Menentukan sudut antara jarum jam dan menit terdapat operasi bagi sehingga sangat memungkinkan adanya nilai desimal sedangkan dalam proses enkripsi ada proses modulus. Hal ini mungkin akan berpotensi menjadi masalah ketika akan melakukan konversi ke bentuk base32. Sehingga perbaikan persamaan 2.6 menentukan sudut menjadi seperti berikut:

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI : https://dx.doi.org/10.30872/jim.v18i2.17707

$$= CEIL \left| \frac{11}{2} M - 30H \right| \quad (2.6)$$

Keterangan: CEIL = Pembulatan ke atas
H = Jam
M = Menit

b. Konversi nilai ASCII yang telah diolah dalam rumus sebagai berikut:

Nilai ASCII final (NF) = (nilai ASCII tiap karakter (NA) + nilai kunci (K)) mod 256. Nilai ASCII final yang akan dikonversi ke dalam bentuk base32 akan menimbulkan masalah karena panjang karakter bervariasi. Hal ini bisa terlihat dari nilai NF terkecil adalah 0 dan nilai terbesar adalah 255 sehingga ketika dikonversi ke base32 menjadi A untuk nilai terkecil dan 7V untuk nilai terbesar. Panjang karakter yang berbeda ini akan menjadi masalah ketika ingin dilakukan dekripsi karena nilai 2 karakter *cipher text* mungkin saja berisi 1atau 2 karakter *plain text*. Untuk menghindari ambiguitas, maka dilakukan penambahan 1 karakter acak di luar ASCII base32 untuk setiap NF yang memiliki panjang 1 karakter.

Dari tahapan diatas maka kita akan lakukan uji coba kriptografi jam dengan beberapa parameter yang akan menguji variasi *cipher text* dengan kemungkinan sudut jam yang dianggap sama atau kata sandi sama dengan *plain text* yang konstan. Berikut hasil pengujiannya (tabel 1):

Tabel 1. Tabel Hasil Pengujian Mengubah *Plain Text* Menjadi *Cipher Text*

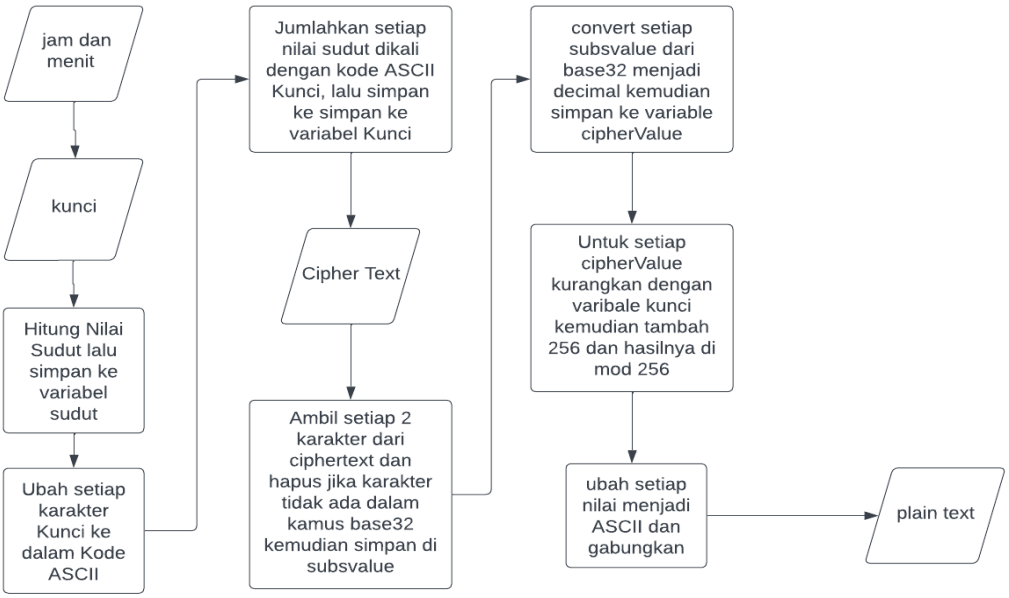
Kata Sandi	Jam dan Menit	*Plain Text*	*Cipher Text*
budiluhur	12:30	saya adalah mahasiswa jurusan magister ilmu komputer	7f6t7l6t4s6t 706t786t744s7 96t746t7f757f 7j6t4s767h7e7 h7f6t7a4s796t 73757f7g717e4 s7578797h4s77 7b797c7h7g717 e
budiluhur	3:45	saya adalah mahasiswa jurusan magister ilmu komputer	*312f372fLe2f 2i2f2q2f2mLe2 r2f2m2f312n31 352fIe2o33303 3312f2sOe2r2f 2l2n31322j30I e2n2q2r33Ie2p 2t2r2u33322j3 0*
budiluhur	6:00	saya adalah mahasiswa jurusan magister	*433h493h1g3h 3k3h3s3h3o1g3 t3h3o3h433p43 473h1g3q45424 5433h3u1g3t3h*
budiluhur	9:15	saya adalah mahasiswa jurusan magister ilmu komputer	*1p171v177617 1a171il71e76 1j171e171p1f 1p1t17761g1r 1o1r1p171k76 1j171d1f1p1q 1b1o761f1i1j 1r761h1l1j1m 1r1q1b1o*
berbudiluhur	2:25	saya adalah mahasiswa jurusan magister ilmu komputer	*736h796h4g6h 6k6h6s6h6o4g6 t6h6o6h736p73 776h4g6q75727 5736h6u4g6t6h 6n6p73746l724 g6p6s6t754g6r 6v6t707574617 2*
budi yang luhur	2:25	saya adalah mahasiswa jurusan magister ilmu komputer	*7s7aO27a597a 7d7a7l7a7h597 m7a7h7a7s7i7s I07a597j7u7r7 u7s7a7n597m7a 7g7i7s7t7e7r5 97i7l7m7u597k 7o7m7p7u7t7e7 r*
univ budi luhur	2:25	saya adalah mahasiswa jurusan magister ilmu komputer	*5s5a625a395a 5d5a5l5a5h395 m5a5h5a5s5i5s 605a395j5u5r5 u5s5a5n395m5a 5g5i5s5t5e5r3 95i5l5m5u395k 5o5m5p5u5t5e5 r*
tulus berbudi luhur	2:25	saya adalah mahasiswa jurusan magister ilmu komputer	*5q5860583758 5b585j585f37 5k585f585q5g 5q5u58375h5s 5p5s5q585l37 5k585e5g5q5r 5c5p375g5j5k 5s375i5m5k5n 5s5r5c5p*

Dari pengujian pembentukan *chipper text* terlihat bahwa meskipun dianggap memiliki sudut yang sama 90’ yaitu jam 12:30, 3:45, 6:00, dan 9:15 namun menghasilkan *cipher text* yang berbeda dan ini membuktikan bahwa perhitungan sudut jam dapat menghasilkan nilai yang spesifik.

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI : https://dx.doi.org/10.30872/jim.v18i2.17707

4.2 Rancang Model Dekripsi

Dalam rancang model dekripsi ini merupakan kebalikan langkah dari proses enkripsi. Tantangan dari proses dekripsi ini adalah memastikan bahwa *cipher text* akan menghasilkan *plain text* seperti pada awalnya. Berikut adalah *flow chart* dekripsi:



Gambar 3. Flow Chart Dekripsi

Dalam proses dekripsi ini *cipher text* yang merupakan nilai dari base32 akan dikembalikan menjadi *plain text*. Beberapa hal yang perlu diperhatikan antara lain sebagai berikut:

A. Pembentukan kunci tetap menggunakan seperti pada proses enkripsi. Hal ini karena kriptografi ini adalah kriptografi simetris sehingga kunci enkripsi dan dekripsi diperlakukan sama.

B. Untuk mendapatkan nilai ASCII kembali, dimulai dengan mengambil *cipher text* setiap 2 karakter kemudian melakukan identifikasi apakah itu 2 karakter murni atau 2 karakter yang telah disisipi. Seperti yang dijelaskan pada proses enkripsi dibutuhkan penyisipan karakter yang hanya memiliki panjang 1 karakter. Dengan melakukan proses filter ini kemudian akan didapatkan nilai base32 murni yang kemudian dilakukan dekripsi.

Dari tahapan diatas maka kita akan lakukan uji coba kriptografi jam dengan beberapa parameter yang akan menguji *cipher text* pada proses enkripsi untuk dikembalikan nilainya menjadi seperti semula. Berikut hasil pengujiannya (Tabel 2):

Tabel 2. Tabel Hasil Pengujian Mengubah Cipher Text Menjadi Plain Text

Kata Sandi	Jam dan Menit	*Cipher Text*	*Plain Text*
budiluhur	12:30	7f6t7l6t4s6t 706t786t744s7 96t746t7f757f 7j6t4s767h7e7 h7f6t7a4s796t 73757f7g717e4 s7578797h4s77 7b797c7h7g717 e	saya adalah mahasiswa jurusan magister ilmu komputer
budiluhur	3:45	*312f372fLe2f 2i2f2q2f2mLe2 r2f2m2f312n31 352fIe2o33303 3312f2sOe2r2f 2l2n31322j30I e2n2q2r33Ie2p 2t2r2u33322j3 0*	saya adalah mahasiswa jurusan magister ilmu komputer
budiluhur	6:00	*433h493h1g3h 3k3h3s3h3o1g3 t3h3o3h433p43 473h1g3q45424 5433h3u1g3t3h 3n3p43443l421 g3p3s3t451g3r 3v3t4045443l4 2*	saya adalah mahasiswa jurusan magister ilmu komputer

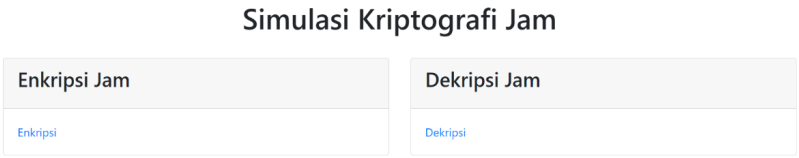
e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI : https://dx.doi.org/10.30872/jim.v18i2.17707

Kata Sandi	Jam dan Menit	*Cipher Text*	*Plain Text*
budiluhur	9:15	*1p171v177617 1a171i171e76 1j171e171p1f 1p1t17761g1r 1o1r1p171k76 1j171d1f1p1q 1b1o761f1i1j 1r761h1l1j1m 1r1q1b1o*	saya adalah mahasiswa jurusan magister ilmu komputer
berbudiluhur	2:25	*736h796h4g6h 6k6h6s6h6o4g6 t6h6o6h736p73 776h4g6q75727 5736h6u4g6t6h 6n6p73746l724 g6p6s6t754g6r 6v6t7075746l7 2*	saya adalah mahasiswa jurusan magister ilmu komputer
budi yang luhur	2:25	*7s7aO27a597a 7d7a7l7a7h597 m7a7h7a7s7i7s I07a597j7u7r7 u7s7a7n597m7a 7g7i7s7t7e7r5 97i7l7m7u597k 7o7m7p7u7t7e7 r*	saya adalah mahasiswa jurusan magister ilmu komputer
univ budi luhur	2:25	*5s5a625a395a 5d5a5l5a5h395 m5a5h5a5s5i5s 605a395j5u5r5 u5s5a5n395m5a 5g5i5s5t5e5r3 95i5l5m5u395k 5o5m5p5u5t5e5 r*	saya adalah mahasiswa jurusan magister ilmu komputer
tulus berbudi luhur	2:25	*5q5860583758 5b585j585f37 5k585f585q5g 5q5u58375h5s 5p5s5q585l37 5k585e5g5q5r 5c5p375g5j5k 5s375i5m5k5n 5s5r5c5p*	saya adalah mahasiswa jurusan magister ilmu komputer

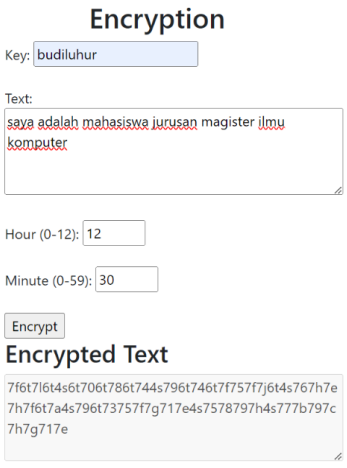
Data Dari pengujian pada tabel 2 membuktikan bahwa kriptografi ini berjalan sesuai yang diharapkan.

Berisi hasil implementasi aplikasi ataupun hasil program (yang penting saja), ataupun hasil dari pengujian metode.

4.3 Aplikasi Simulasi Kriptografi Jam

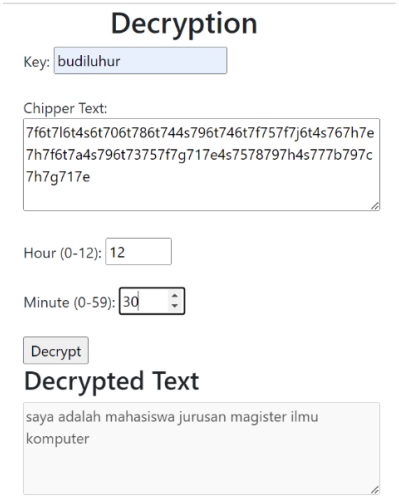


Gambar 4. Halaman Index Simulasi Kriptografi Jam



Gambar 5. Halaman Enkripsi Simulasi Kriptografi Jam

DOI : https://dx.doi.org/10.30872/jim.v18i2.17707 e-ISSN 2597-4963 dan p-ISSN 1858-4853



Gambar 6. Halaman Dekripsi Simulasi Kriptografi Jam

5. KESIMPULAN

Dari tahapan proses yang sudah dilakukan maka dapat dibuktikan bahwa sudut jarum jam dan menit dapat dijadikan salah satu kunci dalam kriptografi. Selain itu juga didapatkan kesimpulan bahwa proses *encoding* dan *decoding* base32 dapat diterapkan dalam pembentukan *cipher text* yang dikonversi dalam setiap karakter ASCII. Kombinasi antara kriptografi jam dan konversi ke dalam base32 membuat *cipher text* akan susah dikenali karena memiliki format yang beragam.

Penelitian ini sangat berpotensi untuk dikembangkan lebih lanjut seperti pada pesan bersandi yang hanya bisa dibaca pada jam dan menit yang sudah ditentukan ataupun pada kasus lain. Diharapkan algoritma kriptografi ini dapat memperkaya variasi pembentukan pesan bersandi kedepannya.

6. DAFTAR PUSTAKA

Anwar, Y. J., Habibi, R., & N., R. (2022). Penerapan Metode Kriptografi AES untuk Mengamankan File Dokumen. *Jurnal Tekno Insentif*, 1-13.

Ariska, W. (2022). Penerapan Kriptografi Menggunakan Algoritma Data Encryption Standard (DES). *Jurnal Sintaks Logika*, 1-11.

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains dan Komputer*, 163-171.

Darmawan, F. A., Kusyanti, A., & Primananda, R. (2022). Pengamanan Citra Berwarna Menggunakan Kriptografi Visual Skema Meaningful Shares dan Steganografi LSB. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, 1-8.

Finaka, A. W., Nurhanisah, Y., & Devina, C. (2023, May). *Indonesia baik.id*. Retrieved from Indonesia baik.id Web site: https://indonesiabaik.id/infografis/orang-indonesia-makin-melek-internet

Gunawan, I. (2023). Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES dari Serangan Brute Force. *Jurnal Media Informatika (JUMIN)*, 1-8.

Listiani, I., Nasution, M. S., Sari, W. I., & Nasution, A. B. (2022). Perancangan Keamanan Data Pasien di Klinik Kecantikan Ratu Beauty Studio Menggunakan Metode Kriptografi RSA. *Jurnal Informatika Teknologi dan Sains (JINTEKS)*, 1-7.

Mido, A. R., & Ujianto, E. I. (2022). Analisis Pengaruh Citra Terhadap Kombinasi Kriptografi RSA dan Steganografi LSB. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, 1-8.

Riadi, I., Fadlil, A., & Tsani, F. A. (2022). Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher. *Jurnal Informatika Sunan Kalijaga (JISKA)*, 1-13.

Sari, D. R., & Pawelloi, A. I. (2022). Penerapan Kriptografi Pada File Teks Dengan Menggunakan Merkle Hellman Knapsack Berbasis Android. *Jurnal Sintaks Logika*, 1-10.

Suranta, A. I., & Sakti, D. V. (2022). Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi. *SKANIKA: Sistem Komputer dan Teknik Informatika*, 1-10.

Thahara, A., & Siregar, I. T. (2021). Implementasi Kriptografi untuk Keamanan Data dan Jaringan Menggunakan Algoritma DES. *JURTI*, 1-8.

Sari, D. R., & Pawelloi, A. I. (2022). Penerapan Kriptografi Pada File Teks Dengan Menggunakan Merkle Hellman Knapsack Berbasis Android. Jurnal Sintaks Logika, Vol. 2 No. 3, September 2022. E-ISSN: 2775-412X.

Josefsson, S. (2006). The Base16, Base32, and Base64 Data Encodings. Network Working Group, Request for Comments: 4648, SJD. Obsoletes: 3548. Category: Standards Track.