Analisis Kombinasi Algoritma *One Time Pad* Dan *Vigenere Cipher* Untuk Keamanan Data Teks

Andi Hanifah Putri Rani[1], Nurdin[2], Rudy Donny Liklilwatil[3].
[1]Jurusan Teknik Informatika Universitas Dipa Makassar
Jln. Perintis Kemerdekaan KM. 9 Makassar
e-mail: [1]haniran011@gmai.com, [2]nurdin@dipanegara.ac.id
[3]rudydonnyliklilwatil@dipanegara.ac.id

Abstrak

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Enkripsi adalah transformasi data kedalam bentuk yang tidak dapat terbaca tanpa sebuah kunci tertentu. Dekripsi merupakan kebalikan dan enkripsi, yaitu transformasi data terenkripsi kembali ke bentuknya semula. Cryptanalysis adalah ilmu untuk mengubah kembali suatu ciphertext menjadi plaintext tanpa mengetahui key-nya. Cryptanalysis dikatakan sukses jika dapat mengembalikan plaintext atau menemukan key-nya. One Time Pad adalah salah satu contoh metode kriptografi dengan algoritma jenis simetri. Sedangkan Vigenere Cipher adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Dimana pada penelitian ini hasil perbandingan dari Algoritma tersebut diketahui bahwa Kombinasi Algoritma One Time Pad dan Vigenere Cipher merupakan Algoritma yang membutuhkan waktu terlama dalam proses enkripsi-dekripsi. Hasil dari proses pemecahan kunci Kombinasi Algoritma One Time Pad dan Vigenere Cipher memiliki jumlah pemecahan kunci dimana kunci yang tidak ditemukan lebih banyak dibanding Algoritma lainnya.

Kata Kunci : *Kriptografi, Data Text, One Time Pad, Vigenere Cipher*

.

Abstract

Cryptography is the science and art of maintaining the secrecy of messages by encoding them in a form that the meaning can no longer be understood. Encryption is the transformation of data into an unreadable form without a certain key. Decryption is the opposite of encryption, namely the transformation of encrypted data back into its original form. Cryptanalysis is the science of converting a ciphertext back into plaintext without knowing the key. Cryptanalysis is said to be successful if it can return the plaintext or find the key. One Time Pad is an example of a cryptographic method with a symmetric type algorithm. Meanwhile, the Vigenere Cipher is a method of encoding alphabetic text using a series of Caesar ciphers based on the letters of the keyword. Where in this study the results of the comparison of the algorithms are known that the combination of the One Time Pad Algorithm and the Vigenere Cipher is the algorithm that takes the longest time in the encryption-decryption process. The results of the key solving process of the combination of the One Time Pad Algorithm and the Vigenere Cipher have a number of key solutions where the key that is not found is more than the other algorithms.

Key Word **:** *Cryptography, Text data, One Time Pad, Vigenere Cipher.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi sangat cepat dan pesat, hal ini yang menyebabkan munculnya kemajuan teknologi informasi. Secara langsung atau tidak, teknologi informasi telah menjadi bagian penting dari berbagai bidang kehidupan. Semakin pesatnya kemajuan teknologi memberikan berbagai kemudahan bagi setiap pihak dalam melakukan pertukaran informasi. Namun, kemudahan ini juga membawa ancaman karena banyak pihak yang tidak berwenang yang berusaha untuk mengambil informasi tersebut untuk kepentingan pribadi atau organisasi.

Masalah keamanan data ini, menjadi isu yang berkembang pada era teknologi informasi. Banyak kejahatan-kejahatan *cyber* yang sering kita dengar salah satunya seperti kasus *hacker byorka* yang mana menjadi topik hangat saat itu. Pelaku kejahatan memanfaatkan celah keamanan yang ada untuk dimasuki dan melakukan manipulasi. Yang mana jika hal tersebut sampai terjadi, kemungkinan besar akan merugikan bahkan membahayakan orang yang akan mengirim pesan, maupun organisasinya. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan. Selain itu data yang di bajak tersebut kemungkinan rusak atau hilang yang menimbulkan kerugian material yang besar.

Dengan kasus-kasus kejahatan *cyber* tersebut perlu dilakukan peningkatan keamanan dalam pertukaran informasi. Untuk itu diperlukan sistem komputer yang memiliki keamanan yang dapat terjamin, seperti penyandian data. Dalam kasus ini kriptografi memiliki peran dalam membantu meningkatkan keamanan data. Dengan adanya sebuah kriptografi yang meliputi proses enkripsi dan dekripsi maka pesan, data, maupun informasi dapat dikodekan sehingga dapat meningkatkan keamanan data. Algoritma kriptografi yang dianggap mampu untuk mengamankan data teks seperti Algoritma *One Time Pad* dan *Vigenere Cipher*. *One Time Pad* adalah salah satu contoh metode kriptografi dengan algoritma jenis simetri[1]. Sedangkan *Vigenere Cipher* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci[2].

Maka, dari permasalahan tersebut dilakukanlah penggabungan Algoritma *One Time Pad* dengan *Vigenere Cipher*. Dengan kombinasi kedua algoritma tersebut diharapkan dapat meningkatkan keamanan dalam penyandian data teks sehingga informasi yang dikirimkan dan diterima pun bisa terjamin kerahasiaan dan keamanannya.

2. METODE PENELITIAN

2.1 Jenis Penelitian

Jenis penelitian yang dilaksanakan oleh penulis dalam penelitian ini, ialah *Library research*, ialah penelitian yang dilaksanakan dengan Teknik membaca buku dan referensi-referensi lainnya untuk mendapatkan ilmu pengetahuan dan landasan teori yang berkaitan dengan *problem* yang dijelaskan oleh penulis[3]**.**

2. 2 Pengumpulan Data

Pengumpulan data dilaksanakan dengan mempelajari buku dan jurnal yang membantu pada penelitian ini, tercantum di dalamnya kepustakaan tentang penulisan dan berhubungan dengan hal-hal yang membantu implementasi temu kembali pada analisis[4].

2.3 Criptography

Kriptografi (*cryptography*) berasal dari bahasa yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia)[5].

2.4 Cryptanalysis

Cryptanalysis adalah ilmu untuk mengubah kembali suatu *ciphertext* menjadi *plaintext* tanpa mengetahui *key*-nya. *Cryptanalysis* dikatakan sukses jika dapat mengembalikan plaintext atau menemukan *key*-nya. Usaha untuk melakukan *cryptanalysis* disebut *attack*. *Cryptanalyst* adalah orang yang melakukan c*ryptanalysis*. Menurut Dutchman A. Kerckhoffs, kerahasiaan

sebuah c*iphertext* semuanya terletak pada *key* dengan asumsi bahwa seorang *cryptanalyst* memiliki detail lengkap algoritma *cryptography* dan implementasinya[6].

2.5 One Time Pad

Algoritma *One Time Pad* (OTP) adalah *stream cipher* yang melakukan enkripsi dan dekripsi satu karakter setiap kali. Algoritma ini merupakan perbaikan dari *Vernam cipher* untuk menghasilkan keamanan yang sempurna. *Cipher* ini termasuk ke dalam kelompok algoritma kriptografi simetri. *One Time Pad* (*pad* = kertas bloknot) berisi barisan karakter-karakter kunci yang dibangkitkan secara acak. Aslinya, satu buah *One Time Pad* adalah sebuah pita (*tape*) yang berisi barisan karakter-karakter kunci. Satu *pad* hanya digunakan sekali (*one time*) saja untuk mengenkripsi pesan, setelah itu *pad* yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain[7].

Rumus dari enkripsi *One Time Pad* yaitu :

$$Ci = (Pi + Ki - 2 \times 64) \bmod 26 + 64$$[7]

dan rumus dekripsi dari *One Time Pad* yaitu :

$$Pi = (Ci - Ki + 26) \bmod 26 + 64$$[7]

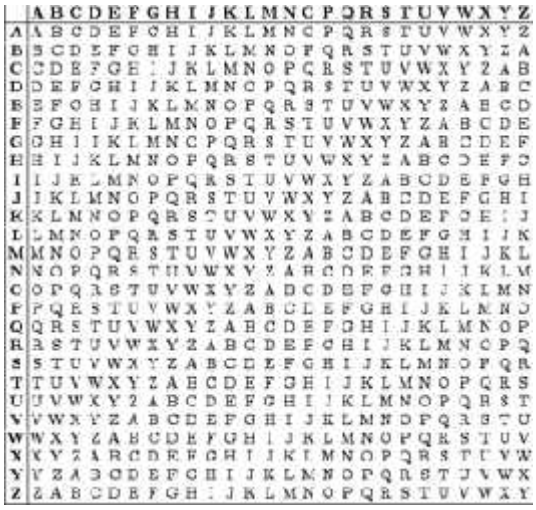
Keterangan rumus :

Ci = Cipherteks(*Ciphertext*)
Pi = Plainteks (*Plaintext*)
Ki = kunci (*Key*)

2.6 Vigenere Cipher

Vigenere Cipher merupakan suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso yang berbasis karakter, maka kunci yang digunakan biasanya berupa kata atau kalimat[8].

Melakukan enkripsi dengan *Vigenere Cipher*, lakukan pada bujur sangkar *Vigenere* sebagai berikut tarik garis vertikal dari huruf *plaintext* ke bawah, lalu tarik garis mendatar dari huruf kunci ke kanan. Perpotongan kedua garis tersebut menyatakan huruf *chipertext*-nya. Pada *Vigenere Cipher*, jika panjang kunci lebih pendek daripada panjang *plaintext*, maka kunci tersebut akan diulang penggunaannya[8].



Gambar 1 Tabula *Recta Vigenere Cipher*

Semisal huruf A pada *plaintext* disubstitusi dengan huruf yang berbeda-beda pada *ciphertext*, yakni U, I, S. Hal inilah yang menyebabkan *Vigenere Cipher* termasuk chiper abjad-majemuk.

Aturan enkripsi pada *Vigenere Cipher* bisa dinyatakan juga sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci, seperti rumus berikut:

$$Ci = (Pi + Ki) \bmod 26[8]$$

Dekripsi pada vigenere chiper dilakukan dengan cara yang berkebalikan, yaitu dengan cara menarik garis horizontal dari huruf kunci sampai ke huruf chiperteks yang dituju, lalu dari huruf cipherteks tarik garis vertikal ke atas sampai ke huruf plainteks atau bisa juga dinyatakan dalam persamaan berikut:

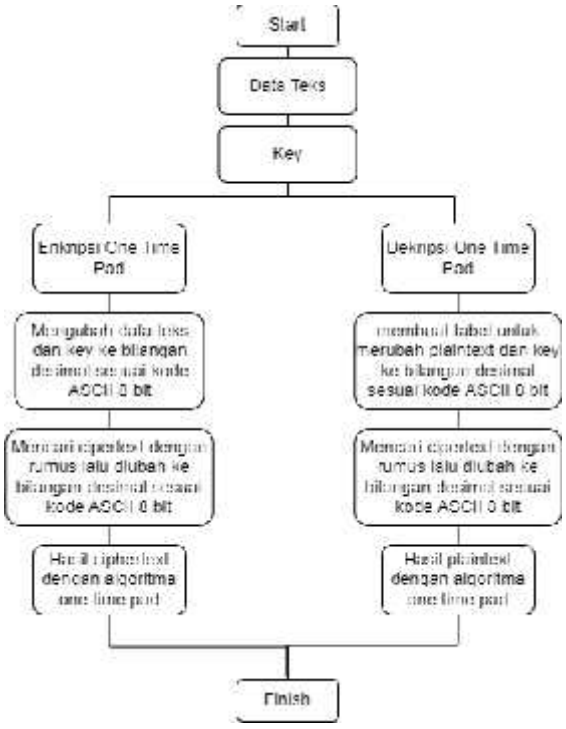
$$Pi = (Ci- Ki) \bmod 26[8]$$

dimana
Pi : karakter plainteks
Ki : karakter kunci
Ci : karakter ciperteks

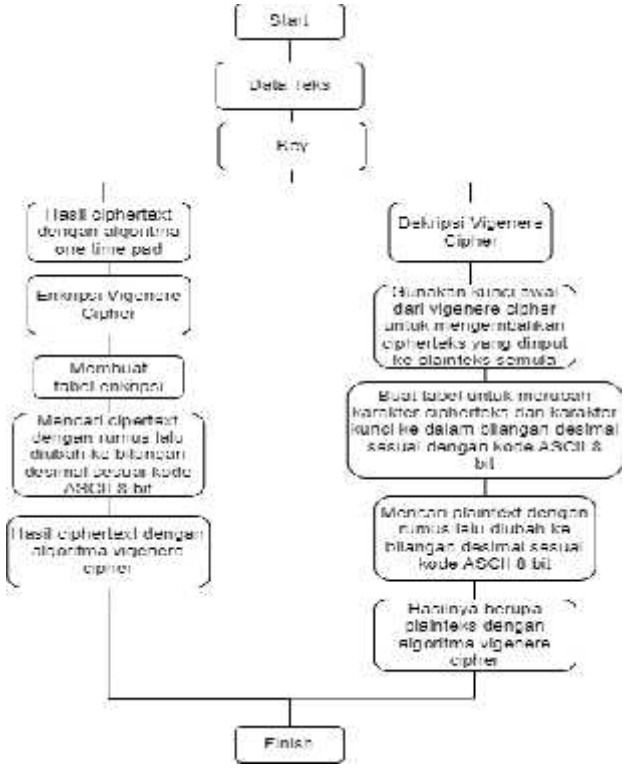
2.7 Pembagian Proses Analisis Data

Pada tahapan ini dimana analisis terbagi menjadi 3 bagian yaitu Analisis Algoritma *One Time Pad*, Analisis Algoritma *Vigenere Cipher*, dan Analisis Kombinasi Algoritma *One Time Pad* dan *Vigenere Cipher*.

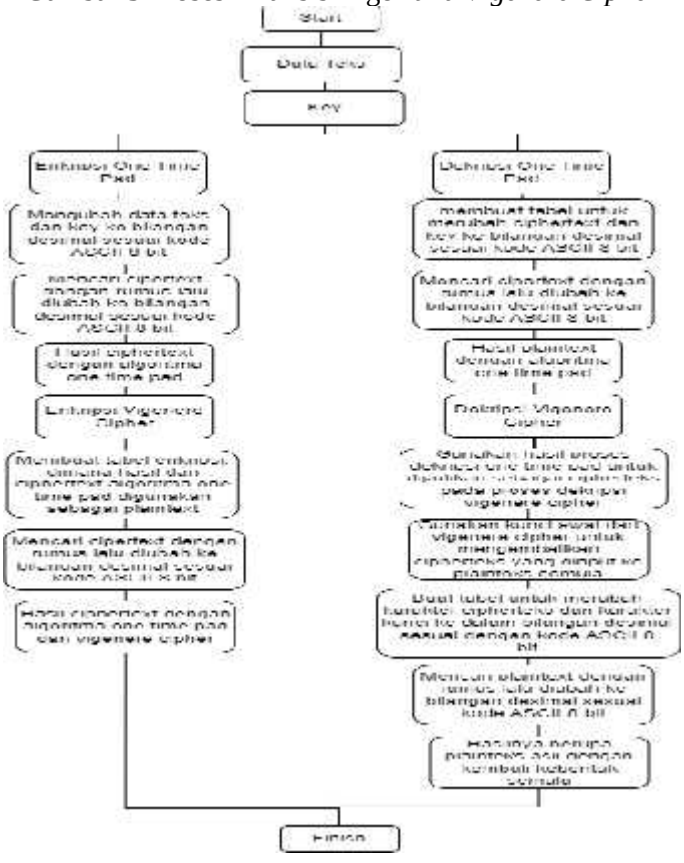
Dimana akan dilakukan perbandingan dari hasil masing-masing Algoritma yang telah dianalisis. Berikut ini proses dari masing-masing Algoritma yang akan dianalisis.



Gambar 2. Proses Analisis Algoritma *One Time Pad*



Gambar 3 Proses Analisis Algoritma *Vigenere Cipher*



Gambar 4 Proses Analisis Algoritma *One Time Pad* dan *Vigenere Cipher*

3. HASIL DAN PEMBAHASAN

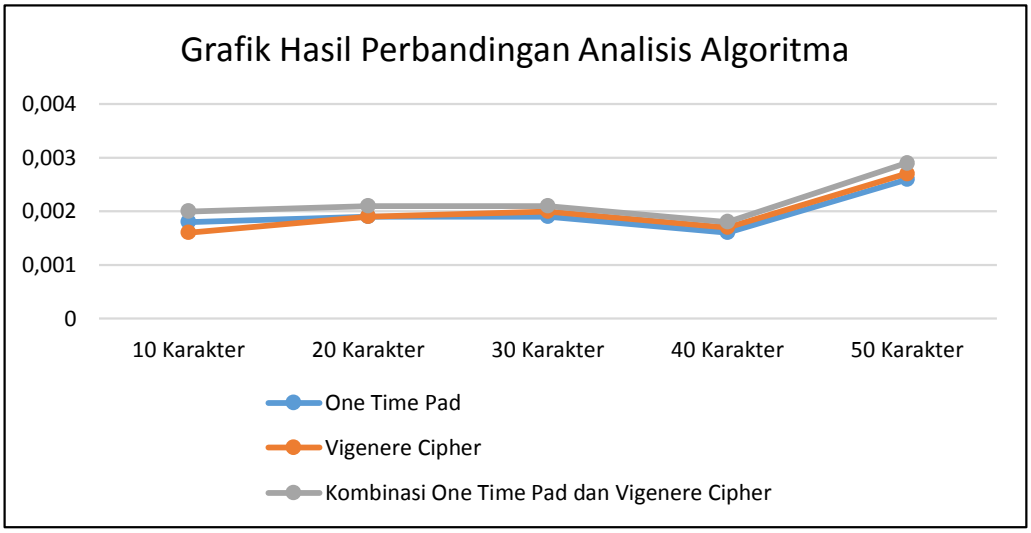
3.1 Hasil Analisis dari Masing-Masing Algoritma

Berikut adalah data hasil perbandingan total waktu proses berdasarkan hasil analisis masing-masing algoritma sebelumnya.

Tabel 1 Hasil perbandingan total waktu proses dari Analisis Algoritma

Variasi Data	Total Waktu Proses (detik)		
	One Time Pad	*Vigenere Cipher*	Kombinasi *One Time Pad* dan *Vigenere Cipher*
10 Karakter	0,0018	0,0016	0,0020
20 Karakter	0,0019	0,0019	0,0021
30 Karakter	0,0019	0,0020	0,0021
40 Karakter	0,0016	0,0017	0,0018
50 Karakter	0,0026	0,0027	0,0029

Penyajian Tabel 1 dalam bentuk grafik untuk masing-masing variasi data adalah sebagai berikut.



Gambar 5 Garfik Hasil Perbandingan Waktu Proses masing-masing Algoritma

Gambar 5 menunjukkan bahwa total waktu yang dibutuhkan untuk melakukan proses enkripsi-dekripsi pada masing-masing Algoritma tidak jauh berbeda. Pada Algoritma O*ne Time Pad* membutuhkan lebih sedikit waktu untuk melakukan proses enkripsi-dekripsi yaitu 0,0020 detik. Pada Algoritma *Vigenere Cipher* waktu yang dibutuhkan berada pada pertengahan tetapi tidak jauh berbeda dengan Algoritma *One Time Pad* yaitu 0,0020 detik. Sedangkan Kombinasi Algoritma *One Time Pad* dan *Vigenere Cipher* membutuhkan lebih banyak waktu dalam proses enkripsi-dekripsinya yaitu 0,0022 detik. Maka kesimpulan dari hasil perbandingan Algoritma tersebut diketahui bahwa Kombinasi Algoritma *One Time Pad* dan *Vigenere Cipher* merupakan Algoritma yang membutuhkan waktu terlama dalam proses enkripsi-dekripsi.

3.2 Hasil Pemecahan Kunci

Kemudian dilakukan proses pemecahan kunci dengan cipherteks dari data hasil enkripsi plainteks yang telah dipecah menjadi 10 sampai 50 karakter. Berikut hasil dari proses tersebut.

Tabel 2 Hasil Proses Pemecahan Kunci

Algoritma	Jumlah Kunci dan Teks	
	Ditemukan	Tidak Ditemukan
One Time Pad	96	54
Vigenere Cipher	107	43
Kombinasi *One Time Pad* dan *Vigenere Cipher*	79	71

Dari tabel diatas dapat dilihat bahwa Kombinasi Algoritma *One Time Pad* dan *Vigenere Cipher* memiliki jumlah pemecahan kunci dimana kunci yang tidak ditemukan lebih banyak dibanding Algoritma *One Time Pad* dan Algoritma *Vigenere Cipher*. Hal tersebut sebab dalam proses enkripsi jika digunakan plainteks dan kunci yang sama panjangnya maka cipherteks dari proses tersebut akan sangat sulit untuk dipecahkan juga apa bila kunci yang digunakan acak dan hanya sekali pakai.

4. KESIMPULAN

Setelah penulis melakukan penelitian analisis Algoritma *One Time Pad, Vigenere Cipher* dan Kombinasi Algoritma *One Time Pad* dan *Vigenere Cipher* dalam upaya peningkatan keamanan data teks maka dapat dihaslikan kesimpulan sebagai berikut:

1. Hasil analisis Algoritma *One Time Pad, Vigenere Cipher* dan Kombinasi Algoritma *One Time Pad* dan *Vigenere Cipher* dimana menunjukkan bahwa total waktu yang dibutuhkan untuk melakukan proses enkripsi-dekripsi pada masing-masing Algoritma tidak jauh berbeda.
2. Hasil perbandingan dari Algoritma tersebut diketahui bahwa Kombinasi Algoritma *One Time Pad* dan *Vigenere Cipher* merupakan Algoritma yang membutuhkan waktu terlama dalam proses enkripsi-dekripsi.
3. Hasil dari proses pemecahan kunci Kombinasi Algoritma *One Time Pad* dan *Vigenere Cipher* memiliki jumlah pemecahan kunci dimana kunci yang tidak ditemukan lebih banyak dibanding Algoritma *One Time Pad* dan Algoritma *Vigenere Cipher*

5. SARAN

Adapun saran yang ingin disampaikan penulis yaitu penelitian ini masih jauh dari kata sempurna oleh karena itu penulis menyarankan agar penelitian selanjutnya dapat menggunakan algoritma-algoritma yang lainnya agar proses penyandian juga dapat lebih baik dan akurat, juga dapat dilakukan analisa dengan menggunakan dua kunci, juga pada analisis frekuensi dapat dilakukan percobaan dengan Bahasa Indonesia, dan juga dimana pada penelitian ini masih menggunakan inputan teks manual maka dapat menambahkan fitur input data dari file.

UCAPAN TERIMA KASIH

Pada kesempatan ini penulis hendak mengucapkan terimakasih kepada keluarga, teman – teman, dan dosen pembimbing yang sudah mendukung, membantu dan memberi banyak masukan selama proses penyusunan skripsi ini berlangsung khususnya kepada:

1. Dr. Y. Jhony Wijaya. Soetikno, SE, MM. selaku Ketua Universitas Dipa Makassar.
2. Ir. H. Irsal, MT. selaku Ketua Jurusan Teknik Informatika program studi strata satu (S1) Universitas Dipa Makassar.
3. Nurdin S.Kom,. M.T. selaku Pembimbing I, yang telah membimbing penulis dalam penyelesaian skripsi ini.
4. Rudy Donny Liklilwatil S.E,. M.Kom. selaku Pembimbing II, yang telah banyak memberikan bimbingan dan arahan penulis dalam menyelesaikan skirpsi ini.
5. Dosen Universitas Dipa Makassar yang telah mendidik dan mengajarkan berbagai disiplin ilmu kepada penulis.

DAFTAR PUSTAKA

[1] Dakhi, O., Masril, M., Novalinda, R., Jufrinaldi, J., & Ambiyar, A. (2020). Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher. INVOTEK: Jurnal Inovasi Vokasional Dan Teknologi, 20(1), 27–36. https://doi.org/10.24036/invotek.v20i1.647

[2] ARNO PANDI. (2021). Implementasi Algoritma Kriptografi Vigenere Cipher Dalam Mengamankan Pengiriman Data Teks. Skripsi, Program Studi Sistem Komputer Universitas Pembangunan Panca Budi.

[3] R. F. Pringgar and B. Sujatmiko, "PENELITIAN KEPUSTAKAAN (LIBRARY RESEARCH) MODUL PEMBELAJARAN BERBASIS AUGMENTED REALITY PADA PEMBELAJARAN SISWA," *IT-Edu J. Inf. Technol. Educ.*, vol. 5, no. 01, pp. 317–329, 2020.

[4] I. Fahrezi, M. Taufiq, Akhwani, and Nafiah, "Meta-analisis Pengaruh Model Pembelajaran Project Based Learning Terhadap Hasil Belajar Siswa Pada Mata Pelajaran IPA Sekolah Dasar," *J. Ilm. Pendidik. Profesi Guru*, vol. 3, no. 3, Art. no. 3, 2020.

[5] Qamal, Mukti, *"Kriptografi File Citra Menggunakan Algoritma Tea (Tiny Encryption Algorithm)" JISKA J. Inform. Sunan Kalijaga, vol. 1, no. 1, Art. no. 1, October 2014, doi:* 10.29103/TECHSI.V6I2.174

[6] A. hidayat, A. Sholahuddin, and R. Rosadi, "Cryptanalysis Menggunakan Methode Vigenere Cipher", *SENTER*, pp. 314–317, Jan. 2018.

[7] Harahap, M. K., & Khairina, N. (2018). Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks. Jurnal & Penelitian Teknik Informatika, 1(April 2017), 58–62.

[8] Hulu, V., & Nadeak, B. (2020). Kombinasi Algoritma Vigenere Cipher dan One Time Pad untuk Mengamankan Data Teks. 02(01), 49–57.

[9] Hasmin, E., & Aisa, S. (2019). Penerapan Algoritma C4. 5 Untuk Penentuan Penerima Beasiswa Mahasiswa. *CogITo Smart Journal*, *5*(2), 308-320.