PENERAPAN KRIPTOGRAFI CAESAR CHIPER DALAM PENGAMANAN DATA

by Maulid Hidayat

Submission date: 16-May-2023 12:43AM (UTC-0400)
Submission ID: 2094358990
File name: 7._Jurnal_JUKIM_Maulid_Hidayat.doc (867.5K)
Word count: 1836
Character count: 10854

JUKIM
ADMI Jurnal Ilmiah Multidisiplin
JURNAL JUKIM Vol 2 No. 2 Maret 2023 | P-ISSN: 2829-0488E-ISSN: 2829-0518, Halaman 12-

PENERAPAN KRIPTOGRAFI *CAESAR CHIPER* DALAM PENGAMANAN DATA

Maulid Hidayat[1], Muhlis Tahir[2], Achmad Sukriyadi [3], Amir Sulton [4], Cindi Ajeng S.A [5], Sofyan Abduh F [6]
[1, 2, 3, 4, 5, 6] Program Studi Pendidikan Informatika, Universitas Trunojoyo Madura

Article History
Received :
Revised :
Accepted :
Published :

Corresponding author*:
190631100100@student.trunojoyo.ac.id
No. Contact:

Cite This Article:

DOI:

Abstract: *Information is no longer stored if it is stolen and misused by unaffected groups. That's why we need information security that can protect data from unattached groups. The caesar cipher algorithm is a very simple and very popular encryption method. Where in it there is a code and this code consists of all the letters of the original text (plaintext), which are then replaced with other codes and then changed with other letters with certain positional differences in the alphabet. Caesar encryption can protect and recover data without changing its original form (plaintext).*
Keywords: *data theft, security, caesar encryption*

Abstrak: Informasi tidak lagi disimpan jika informasi tersebut dicuri dan disalahgunakan oleh kelompok yang tidak terpengaruh. Itu sebabnya kami membutuhkan keamanan informasi yang dapat melindungi data dari grup yang tidak terikat. Algoritma *caesar cipher* merupakan metode enkripsi yang sangat sederhana dan sangat populer. Dimana di dalamnya terdapat sebuah kode dan kode ini terdiri dari semua huruf dari teks asli (*plaintext*), yang kemudian diganti dengan kode lainnya dan kemudian diubah dengan huruf lain dengan perbedaan posisi tertentu dalam alfabet. *Enkripsi caesar* ini dapat melindungi dan memulihkan data tanpa mengubah bentuk aslinya (*plaintext*).
Kata Kunci: pencurian data, keamanan, *enkripsi caesar*.

PENDAHULUAN

Keamanan menjadi aspek yang sangat penting saat ini di mana pertukaran data dan informasi menjadi tuntutan baik pekerjaan dan lainnya. Berbagai cara dilakukan untuk mengamankan data atau informasi di antaranya menggunakan Kriptologi. Sebelum adanya komputer, pensil dan kertas merupakan media untuk menerapkan algoritma kriptografi. Algoritma kriptografi (*cipher*) yang digunakan dinamakan algoritma klasik. Algoritma klasik merupakan algoritma yang berbasis karakter. Dimana proses enkripsi dan dekripsi dilakukan pada setiap karakter pesan [10].

Kriptografi (*Cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia.Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi [1]. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Berbagai macam teknik digunakan untuk upaya mengamankan data atau informasi yang penting.

Pada pengamanan dalam kriptografi ini banyak metode atau algoritma yang dapat digunakan, seperti *Caesar*, Abjad Majemuk, DES, IDEA, RSA dan lain sebagainya. Ilmu kriptografi juga adalah suatu teknik untuk mengamankan data atau pesan, pengamanan data atau pesan dapat dilakukan dengan menggunakan berbagai algoritma, salah satunya dapat menggunakan sandi caesar. Oleh karena itu, dibutuhkan suatu keamanan yang membuat data aman dari kelompok yang tidak bersangkutan. Banyak cara dapat dilakukan untuk menyembunyikan data atau pesan yang akan dikirim. Salah satunya menggunakan kriptografi. Kriptografi berfungsi untuk menyamarkan pesan menjadi pesan yang tersandi. Adapun algoritma kriptografi yang bisa menyamarkan pesan adalah algoritma *Caesar Cipher*. Algoritma *Caesar Cipher* adalah metode enkripsi sangat sederhana dan sangat populer. Kode ini terdiri dari semua huruf pada teks asli (*plaintext*) disubstitusi dengan kode kemudian berubah menjadi huruf lain yang mempunyai selisih posisi tertentu dalam alfabet [2].

Dengan penggunaan algoritma *Caesar Cipher* pengguna dapat mengamankan isi data yang akan diberikan si penerima sehingga integritas data dapat terjaga kerahasiaannya.

METODE PENELITIAN

Kriptografi

Kata kriptografi terdiri dari dua bagian yang berasal dari bahasa yunani, yaitu kripto dan graphia dimana kripto dapat diartikan sebagai secret (rahasia) dan graphia sebagai writing (tulisan). Berdasarkan istilahnya kriptografi merupakan ilmu dan seni pengamanan pesan saat pesan dipindahkan pada suatu tempat ketempat lainnya [4]. Kriptografi adalah suatu ilmu menganalisis teknik matematika yang berkaitan dengan pengamanan informasi seperti penyembunyian data, kesahan data, integritas data, serta keaslian data [5]. Kriptografi yaitu ilmu pengetahuan dan seni melindungi pesan supaya terjaga (aman). Sasaran penggunaan kriptografi yaitu membentuk sesuatu yang samar, berupa pesan rahasia seperti teks, suara, gambar dan video [6]. Menurut Mollin, sistem kriptografi (*Cryptosystem*) adalah kumpulan dari fungsi enkripsi dan dekripsi yang berkoresponden terhadap kunci enkripsi dan dekripsi [12].

Kriptografi bertujuan untuk memberi layanan keamanan (juga dinamakan sebagai aspek-aspek keamanan). Untuk dapat menggunakan teknik kriptografi, dibutuhkan sebuah metode salah satunya adalah metode Caesar Cipher [11]. Caesar Cipher merupakan salah satu algoritma tertua, dan merupakan salah satu jenis cipher substitusi yang menyusun huruf dalam plaintext yang digeser dan diganti dengan huruf beberapa posisi tetap dibawah alfabet. Namun beberapa algoritma kriptografi klasik yang telah banyak diketahui secara luas memiliki kelemahan yang dapat diketahui dan dipecahkan oleh *cryptanalysis*. Kriptanalisis melakukan pengecekan serangan teks biasa dengan mempelajari pengaruh hasil putaran pasangan teks cipher iteratif.

Tujuan lainnya dari kriptografi adalah untuk memberikan layanan keamanan [9] yaitu:

a. Penyembunyian (*Confidentiality*) kerahasiaan informasi dilakukan dengan menyembunyikan informasi dari segala aspek yang tidak berhak.
b. Kelengkapan data (*Integrity*) adalah data tidak terganti sampai pada penerima saat proses pengiriman.
c. Keaslian (*Message Authentication*) kejelasan identitas semua entitas yang terkait dan autentikasi sumber data.
d. Tidak ada penolakan (*Non Repudiation*) setiap entitas saling berhubungan dan tidak dapat menolak atau membantah data yang dikirim atau diperoleh

Kriptografi memiliki beberapa hal yang harus diketahui antara lain [1]:

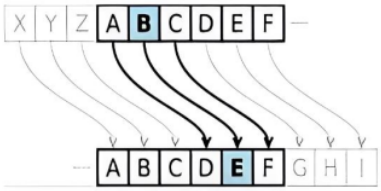
a. Pengirim dan Penerima Pengirim (*sender*) merupakan kesatuan yang mengirimkan message kepada penerima (receiver) dengan aman tanpa ada gangguan dari penyadap (*eavesdropper*). Penerima merupakan entitas yang memperoleh pesan oleh pengirim.
b. Plaintext dan Ciphertext Pesan murni pada kriptografi disebut dengan plaintext, sedangkan pesan murni yang telah disamarkan disebut ciphertext.
c. Enkripsi dan Dekripsi Pada prosedurnya, pergantian plaintext jadi ciphertext disebut enkripsi (*encryption*) dan pergantian ciphertext menjadi plaintext disebut dekripsi (*decryption*).
d. Kriptografer, Kriptanalis, dan Kriptologis Seseorang yang mempelajari dan menggunakan metode kriptografi untuk mengamankan pesan dinamakan kriptografer. Sebaliknya, metode yang menggunakan teknik komputasi matematika untuk menyerang metode kriptografi dinamakan kriptanalis, dan orang yang mempelajari kriptanalisis dinamakan kriptanalis. Kata kriptologi merupakan cabang ilmu yang mempelajari kriptografi sekaligus dengan kriptanalisis. Orang yang mempelajari kriptologi tersebut dinamakan kriptologis.
e. Cipher Algoritma kriptografi (*cipher*) merupakan fungsi matematika dalam penggunaan enkripsi dan dekripsi. Dalam menyelesaikan persoalaan cipher, dibutuhkan sebuah entitas yang disebut dengan kunci (dilambangkan K). Kunci mempunyai nilai bilangan yang sangat besar. Besar kecilnya nilai ini dinamakan keyspace. Beberapa algoritma kriptografi menggunakan cipher dengan beda kunci antara kunci bagi enkripsi dan dekripsi.
f. Penyadap (*Eavesdropper*) adalah orang yang ingin mendapatkan informasi sebanyak-banyaknya dari pesan yang telah dikirim dan memecahkan ciphertext dari sistem kriptografi. Penyadap mempunyai akses komunikasi antara pengirim dan penerima.

Algoritma *Caesar Cipher*

Pada kriptografi, sandi Caesar, atau sandi pindah, kode Caesar yaitu metode enkripsi sangat sederhana dan sangat populer. Kode ini terdiri dari semua huruf pada teks asli (*plaintext*) disubstitusi dengan kode kemudian berubah menjadi huruf lain yang mempunyai selisih posisi tertentu dalam alfabet. Dalam Caesar cipher, huruf-huruf diubah dengan huruf selanjutnya dari posisi alphabet yang sama [7].

Proses Caesar Cipher adalah [3]:

a. Tentukan berapa besar pemindahan karakter yang dipakai untuk membuat *cipherteks* ke *plainteks*.
b. Tukar posisi karakter *plainteks* menjadi *cipherteks* berdasarkan pemindahan yang telah ditentukan sebelumnya. Contoh, pemindahan = 3. Jadi huruf A digeser menjadi huruf D, huruf B menjadi huruf E, dan berikutnya



Gambar 1 Proses *Caesar Cipher*

Proses *enkripsi* menggunakan persamaan 1 di bawah ini:

$$Cp = (Pt + k) \text{ modulo } 26 \quad (1)$$

Dimana 26 adalah jumlah alphabet, persamaan 1 digunakan pada proses enkripsi.

Proses *dekripsi* menggunakan persamaan 2 di bawah ini :

$$Pt = (Cp-k) \text{ modulo } 26 \quad (2)$$

Berikut satuan dari abjad atau alphabet pada *Caesar Cipher* sebagai berikut [8]:

Tabel 1 Satuan Alphabet

Alphabet	Nilai Urut
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23

Y	24
Z	25

HASIL DAN PEMBAHASAN

Perhitungan *Caesar Cipher*

a. Tahap Enkripsi

Tahap yang mengubah cipher dari yang dapat dipahami (*plaintext*) menjadi ciphertext yang tidak dapat dipahami (*ciphertext*). Misalnya, plaintext yang diketahui adalah sebagai berikut:

Plaintext = DAYAT

Kunci = 10

Maka langkah yang harus dikerjakan yaitu:

1) Cek nilai alphabet dari huruf yang ada pada table 1, terlihat bahwa D=3, A=0, Y=24, A=0 dan T=19
2) Setelah itu lakukan perhitungan ciphertext Cp = (Pt +k) modulo 26 dan cek pada Tabel 1 alphabet dari nilai ciphertext yang dihasilkan

Cp_1 = Pt_1 + k modulo 26
= (3+10) modulo 26
= 13 modulo 26
= 13
= N

Cp_2 = Pt_2 + k modulo 26
= (0+10) modulo 26
= 10 modulo 26
= 10
= K

Cp_3 = Pt_3 + k modulo 26
= (24+10) modulo 26
= 34 modulo 26
= 34
= I

Cp_4 = Pt_4 + k modulo 26
= (0+10) modulo 26
= 10 modulo 26
= 10
= K

Cp_5 = Pt_5 + k modulo 26
= (19+10) modulo 26
= 29 modulo 26
= 29
= D

3) Hasil *enkripsi* adalah "NKIKD".
Maka didapatkan *ciphertext* dari *plaintext* "DAYAT" adalah **NKIKD**

b. Tahap Dekripsi

Berbeda dengan fase enkripsi, yaitu merubah password dari yang tidak dapat dipahami (*ciphertext*) menjadi password yang dapat dimengerti (*plaintext*). Contoh kasus. Jika ciphertext yang diberikan adalah sebagai berikut:

Plaintext = NKIKD

Kunci = 10

Maka langkah yang harus dikerjakan yaitu:

1) Cek nilai alphabet dari huruf dimana pada Tabel 1 terlihat bahwa N=13, K=10, I=8, K=10 dan D=3
2) Kemudian lakukan perhitungan plaintext dimana P= C - k mod 26. Jika hasilnya minus(-) maka akan terus ditambah 26 sampai hasilnya positif (+) kemudian dihitung modulonya dan cek pada Tabel 1 alphabet dari nilai *plaintext* yang dihasilkan.

Cp_1 = Pt_1 + k modulo 26
= (13-10) modulo 26
= 3 modulo 26

= 3
= D

Cp_2 = Pt_2 + k modulo 26
= (10-10) modulo 26
= 0 modulo 26
= 0
= A

Cp_3 = Pt_3 + k modulo 26
= (8-10) modulo 26
= -2 modulo 26
= -2
= Y

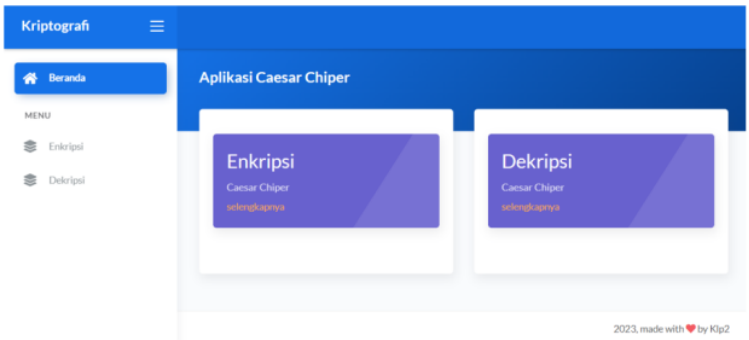
Cp_4 = Pt_4 + k modulo 26
= (10-10) modulo 26
= 0 modulo 26
= 0
= A

Cp_5 = Pt_5 + k modulo 26
= (3-10) modulo 26
= -7 modulo 26
= -7
= T

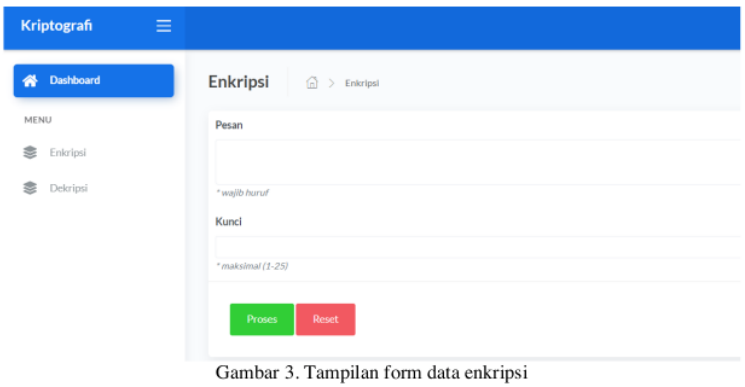
3) Hasil *dekripsi* adalah "DAYAT"
Maka didapatkan *plaintext* dari *ciphertext* "NKIKD" adalah **DAYAT**

Tampilan Program

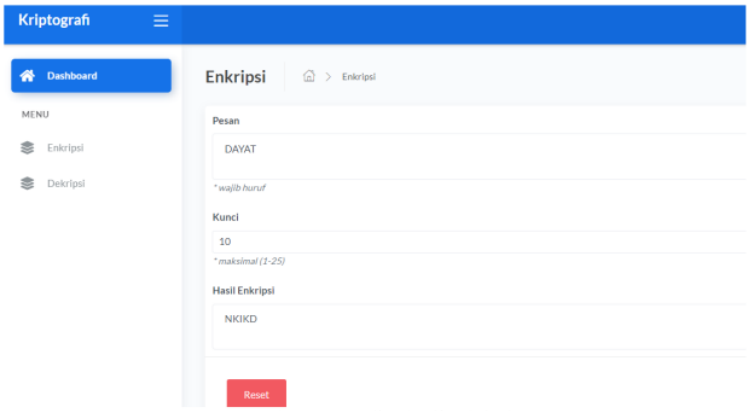
Pada aplikasi ini terdapat 5 tampilan. Berikut ini merupakan tampilan aplikasi caesar chiper (*enkripsi* dan *dekripsi*)



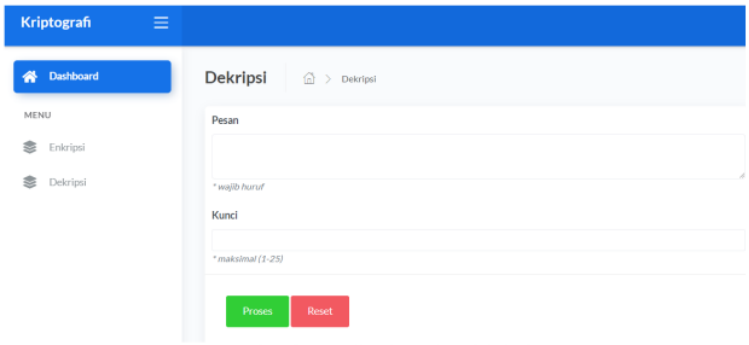
Gambar 2. Tampilan awal aplikasi caesar chiper



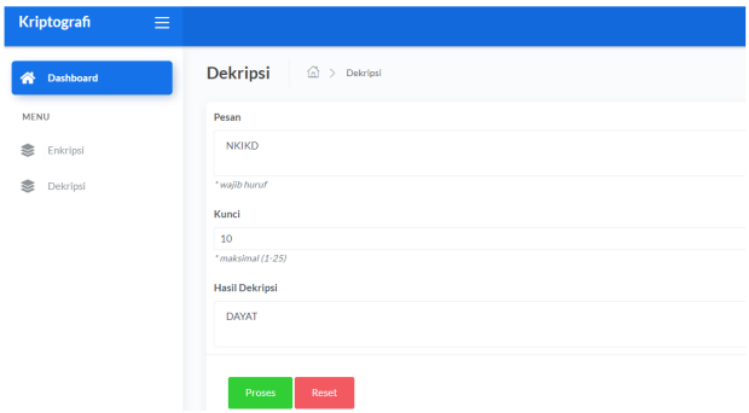
Gambar 3. Tampilan form data enkripsi



Gambar 4. Tampilan hasil enkripsi



Gambar 5. Tampilan form data dekripsi



Gambar 6. Tampilan hasil dekripsi

KESIMPULAN

Proses penyandian dengan algoritma Caesar Cipher berhasil digunakan untuk menyembunyikan pesan dan dapat mengembalikan pesan tersebut seperti semula. Program hanya dapat memproses karakter A hingga Z dikarenakan penggunaan angka 26. Karakter akan dihapus jika karakter bukan A hingga Z.

DAFTAR PUSTAKA

[1] M. M. Amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," Pseudocode, vol. 3, no. 2, pp. 129–136, 2017, doi: 10.33369/pseudocode.3.2.129-136.

[2] A. B. Nasution, "Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher Dan Transposisi Cipher," J. Teknol. Inf., vol. 3, no. 1, p. 1, 2019, doi: 10.36294/jurti.v3i1.680.

[3] Basuki, Armaja.2016. Aplikasi Kriptografi Berlapis Menggunakan Algoritma Tansposisi, Vigenere dan Blok Cipher Berbasis Mobile. Seminar Nasional Teknologi Informasi dan Multimedia 20116, Februari 2016 : 31-35.

[4] Gurning, R.R.A. 2014. Perancangan Aplikasi Pengamanan Pesan Dengan Algoritma Caesar Cipher. Pelita Informatika Budi Darma, Volume: VI, Nomor: 3, April 2014: 106-110.

[5] Zuli, F., Irawan, A. 2014. Penerapan Kombinasi Caesar dan Vigenere Untuk Pengamanan Data Pesan Pada Surat Elektronik. Studi Informatika: Jurnal Sistem Informasi. 7(2), 2014 : 1-11.

[6] Septiarini, A., Hamdani. 2011. Sistem Kriptografi Untuk Text Message Menggunakan Affine. Jurnal Informatika Mulawarman. Vol. 6, No.1, Februari 2011: 50-53.

[7] Seftyanto, Donny. 2012. Peran Algoritma Caesar Cipher Dalam Membangun Karakter Akan Kesadaran Keamanan Informasi. Seminar Nasional Matematikan dan Pendidikan Matematikan FMIPA UNY. November 2012 : MP 883-890

[8] Rahima. 2014. Implementasi Penyembunyian dan Penyandian Pesan Pada Citra Menggunakan Algoritma Affine Cipher dan Metode Least Significant Bit. Pelita Informatika Budi Darma, Volume: VI, Nomor: 1, Maret 2014: 144-148.

[9] Rachmawati, D., Candra, A. 2015. Implementasi Kombinasi Caesar dan Affine Cipher untuk Keamanan Data Teks. Jurnal Edukasi dan Penelitian Informatika (JEPIN). Volume 1, No. 2 : 60-63

[10] Pradipta, A. 2016. Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi. Indonesian Journal on Networking and Security, 5(3), 3–6.

[11] I. W. Utomo, R. Latifah, and D. Risanty, "APLIKASI KRIPTOGRAFI BERBASIS ANDROID MENGGUNAKAN ALGORITMA CAESAR CIPHER DAN VIGENERE CIPHER."

[12] Mollin, R. A. 2007. An Introduction to Cryptography. 2nd Edition. Chapman & Hall/CRC : Boca Raton, Florida.

PENERAPAN KRIPTOGRAFI CAESAR CHIPER DALAM PENGAMANAN DATA

ORIGINALITY REPORT

35%	35%	24%	16%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Clarkston Community Schools Student Paper	5%
2	journal.uvers2.ac.id Internet Source	5%
3	www.coursehero.com Internet Source	4%
4	ejournal.unib.ac.id Internet Source	3%
5	afifahnurlita.blogspot.com Internet Source	3%
6	www.jurnal.akba.ac.id Internet Source	2%
7	www.researchgate.net Internet Source	2%
8	text-id.123dok.com Internet Source	2%
9	Ahmad Tantoni, Mohammad Taufan Asri Zaen. "IMPLEMENTASI DOUBLE CAESAR	1%

CIPHER MENGGUNAKAN ASCII", Jurnal Informatika dan Rekayasa Elektronik, 2018
Publication

10	download.garuda.kemdikbud.go.id Internet Source	1 %
11	e-journal.potensi-utama.ac.id Internet Source	1 %
12	Saefudin ., Syamsudin .. "Aplikasi Enkripsi Pesan Teks Dengan Metode Advanced Encryption Standard Pada Ponsel Berbasis Android", JSiI (Jurnal Sistem Informasi), 2017 Publication	1 %
13	journal.fkpt.org Internet Source	1 %
14	jurnal.pancabudi.ac.id Internet Source	1 %
15	journal.admi.or.id Internet Source	1 %
16	si.fst.uinjkt.ac.id Internet Source	1 %
17	www.scilit.net Internet Source	1 %
18	Adnan Buyung Nasution. "Modifikasi Algoritma Affine Cipher untuk Mengamankan Data", Jurnal Teknologi Informasi, 2020 Publication	1 %

19	www.jptam.org Internet Source	1 %

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		