SAES2

Tugas 2 IF4020 Kriptografi

Marcellus Michael Herman Kahari- 13520057
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13520057@std.stei.itb.ac.id

Malik Akbar Hashemi Rafsanjani - 13520105
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13520105@std.stei.itb.ac.id

Hafidz Nur Rahman Ghozali - 13520117
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13520117@std.stei.itb.ac.id

***Abstract*—Sektor keamanan informasi menjadi sektor yang penting untuk perkembangan dunia saat ini. Oleh karena itu, penulis menciptakan SAES2, sebuah block cipher baru dengan menggunakan penggabungan antara AES, playfair cipher, dan mode operasi cipher blok CBC. Metode umum pada SAES2 terdiri dari proses Playfair Cipher akan dijalankan tepat setelah proses AddRoundKey pada AES. Selain itu, digabungkan pula metode CBC dengan melakukan mode operasi xor setelah proses AES dijalankan. Xor pertama akan dilakukan dengan kunci master key. Untuk n berikutnya akan dijalankan dengan xor hasil enkrip c_{n-1}.**

Keywords—AES, Playfair Cipher, CBC

I. Pendahuluan

Sektor keamanan informasi adalah sektor yang penting untuk dunia zaman ini. Semakin banyak informasi penting yang tersebar di dunia maya, semakin penting pula penjaminan keamanan informasi tersebut. Oleh karena itu, kriptografi menjadi ilmu yang penting untuk dipelajari.

Kriptografi adalah ilmu yang mempelajari tentang keamanan suatu informasi menggunakan metode operasi matematika. Pada makalah ini, penulis menciptakan sebuah blok cipher baru yang terinspirasi dari AES, kriptografi klasik Playfair Cipher, dan mode operasi *cipher* blok CBC.

II. Dasar Teori

A. AES

Algoritma AES yang digunakan pada makalah ini adalah algoritma AES-128. Algoritma ini memiliki panjang kunci 128 bit sehingga memiliki jumlah kemungkinan kunci adalah 2^{128} atau setara dengan $3,4 * 10^{38}$ kemungkinan kunci. AES diharapkan dapat menghindari serangan terhadap *exhaustive key search attack* dan menutup celah kekurangan dari algoritma DES.

Garis besar Algoritma Rijndael yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut (di luar proses pembangkitan round key):

1. AddRoundKey: tahap ini disebut pula sebagai *initial round*. Pada tahap ini, dilakukan operasi xor antara *plain teks* dengan *cipher key*.
2. Dilakukan putaran sebanyak n - 1 dengan proses tiap-tiap putaran adalah:
   a. SubBytes: substitusi byte dengan menggunakan tabel substitusi (S-box).
   b. ShiftRows: pergeseran baris-baris array state secara wrapping.
   c. MixColumns: mengacak data di masing-masing kolom array state.
   d. AddRoundKey: melakukan XOR antara state sekarang round key.
3. Pada tahap akhir, dilakukan *final round* dengan proses sebagai berikut:
   a. SubBytes
   b. ShiftRows
   c. AddRoundKey

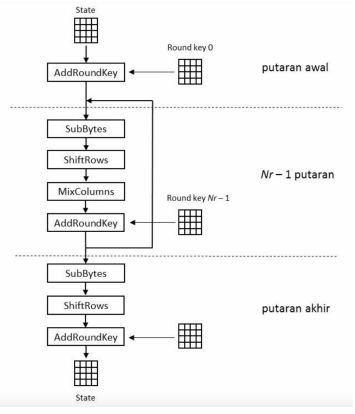

Fig. 1. Contoh langkah enkripsi AES

B. Playfair Cipher

Cipher ini akan melakukan enkripsi pasangan huruf (*bigram*), bukan huruf tunggal seperti pada algoritma *cipher* klasik lainnya. Pada umumnya, kunci kriptografi yang digunakan terdiri dari 25 buah huruf yang disusun dalam sebuah matriks bujursangkar dengan ukuran 5 x 5. Sebelum dilakukan enkripsi, pesan akan diatur sebagai berikut.

1. Ganti huruf j (bila ada) dengan i

2. Tulis pesan dalam pasangan huruf (bigram).

3. Jangan sampai ada pasangan huruf yang sama. Jika ada, sisipkan x di tengahnya

4. Jika jumlah huruf ganjil, tambahkan huruf x di akhir

Untuk melakukan enkripsi, pesan yang sudah diatur dapat dinekripsikan menggunakan matriks bujursangkar yang sudah diatur dengan langkah-langkah sebagai berikut.

1. Jika terdapat huruf-huruf pada bigram yang terletak pada baris yang sama, dilakukan pergeseran ke sebelah kanan dan bersifat siklik.

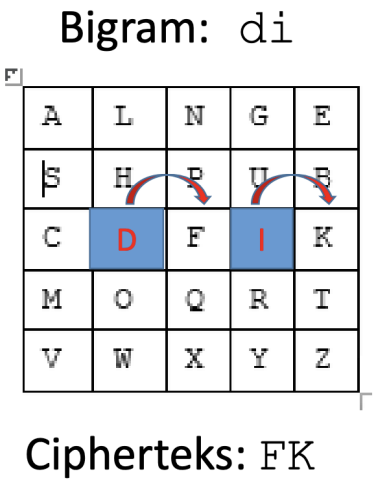

Fig. 2. Contoh proses langkah ke-1

2. Jika terdapat huruf-huruf pada bigram yang terletak pada kolom yang sama, dilakukan pergeseran huruf ke bawah secara siklik.

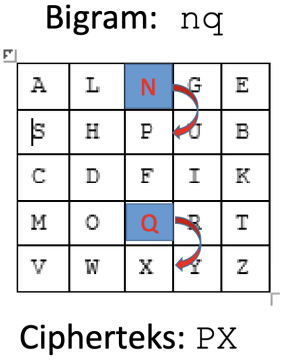

Fig. 3. Contoh proses langkah ke-2

3. Jika huruf-huruf pada bigram tidak terletak baris yang sama atau kolom yang sama:

- huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua.
- huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari tiga huruf yang digunakan sampai sejauh ini.

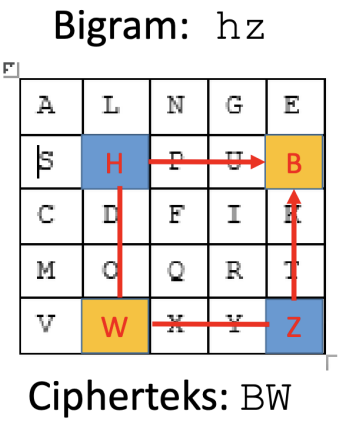

Fig. 4. Contoh proses langkah ke-3

C. CBC

CBC (*Cipher Block Chaining*) adalah salah satu mode operasi *cipher* blok yang digunakan untuk membuat ketergantungan antar blok. Mode operasi ini diciptakan untuk mengatasi kelemahan pada mode operasi ECB. Enkripsi blok pertama memerlukan sebuah blok semu yang dapat disebut sebagai IV atau *initialization vector*. IV dapat diberikan langsung oleh pengguna atau dibangkitkan dengan menggunakan sebuah blok acak. Hasil enkripsi dari blok ini akan diberikan ke blok-blok berikutnya dan pada blok berikutnya, dilakukan enkripsi berdasarkan hasil enkripsi blok sebelumnya.

Blok-blok *plainteks* yang sama menjamin akan dihasilkan sebuah blok *cipher* yang sama. Hal ini akan menyulitkan proses kriptanalisis sehingga akan sulit untuk dilakukan dekrip tanpa mengetahui kuncinya. Hal inilah yang menjadi alasan utama digunakannya CBC sebagai salah satu mode operasi blok *cipher*.

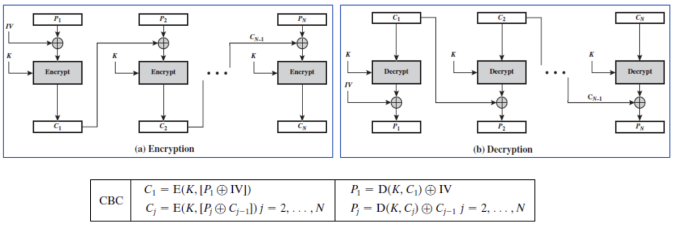

Fig. 5. Gambaran umum mode operasi CBC

III. RANCANGAN BLOK CIPHER

A. *Gambaran Umum Blok Cipher*

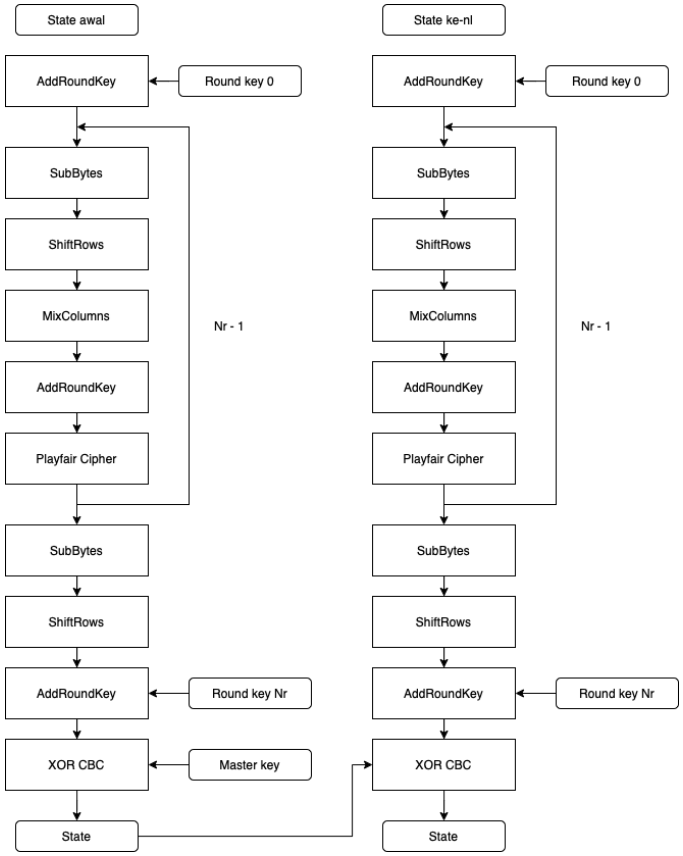

Fig. 6. Gambaran umum enkripsi rancangan blok cipher yang diusulkan

Proses enkripsi berjalan sebagai berikut. Untuk state awal, mula-mula akan dilakukan proses AddRoundKey dengan round key 0. Setelah itu, akan dilakukan proses iterasi sebanyak $n_r - 1$. Di dalam setiap iterasi, dilakukan proses SubBytes, ShiftRows, MixColumns, AddRoundKey, dan Playfair Cipher. Setelah proses iterasi selesai, dilakukan dilakukan kembali proses SubBytes, ShiftRows, AddRoundKey, dan XOR CBC. Proses XOR CBC yang pertama dilakukan dengan master key yang diberikan oleh pengguna.

Untuk proses enkripsi berikutnya, keseluruhan proses sama seperti proses enkripsi pertama kali. Akan tetapi, perbedaannya adalah pada XOR CBC, key yang digunakan adalah hasil enkripsi pada proses berikutnya sehingga akan menimbulkan sebuah *chaining* atau bisa disebut sebagai sebuah ketergantungan dengan proses sebelumnya.

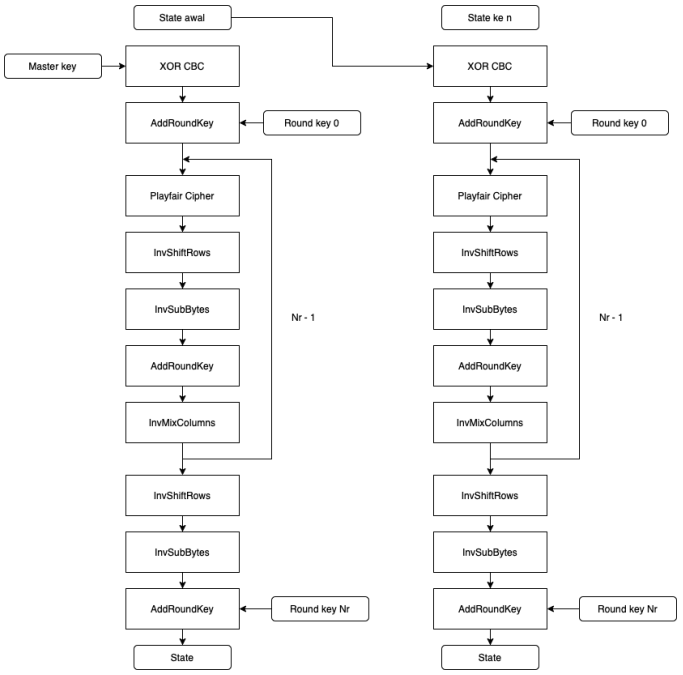

Fig. 7. Gambaran umum dekrip rancangan blok cipher yang diusulkan

Proses dekripsi berjalan sebagai berikut. Untuk state awal, mula-mula akan dilakukan proses XOR CBC dengan master key yang sudah didefinisikan. Setelah itu, dilakukan AddRoundKey dengan round key 0. Berikutnya, akan dilakukan proses iterasi sebanyak $n_r - 1$. Di dalam setiap iterasi, dilakukan proses Playfair Cipher, InvShiftRows, InvSubBytes, AddRoundKey, dan InvMixColumns.. Setelah proses iterasi selesai, dilakukan dilakukan kembali proses. InvShiftRows, InvSubBytes, dan AddRoundKey.

Untuk proses dekrip berikutnya, keseluruhan proses sama seperti proses dekrip pertama kali. Akan tetapi, perbedaannya adalah pada XOR CBC, key yang digunakan adalah hasil enkripsi pada proses sebelumnya.

B. *Playfair Cipher*

Proses playfair cipher dimulai dengan membangkitkan tabel kunci playfair. Kunci dalam setiap *round* diambil dari baris-baris *master key* yang bersesuaian. Setiap huruf akan ditranslasi ke dalam *hexadecimal* dan kedua byte representasi akan digunakan untuk mengisi tabel playfair.

Misalkan terdapat *master key* sebagai berikut

0xBB	0X64	0X54	0XE8
0XDE	0X02	0x33	0x80
0xB7	0X68	0X02	0XB2
0X47	0X47	0XA7	0X00

Fig. 8. Contoh *master key*

Pada round ini, baris 2 akan digunakan untuk membangkitkan tabel playfair sehingga berbentuk sebagai berikut

D	E	0	2
3	8	1	4
5	6	7	9
A	B	C	F

Fig. 9. Tabel playfair yang dibangkitkan berdasarkan *master key*

Setelah tabel tersebut dibangkitkan, proses enkripsi akan mengikuti kaidah-kaidah yang ada di dalam playfair cipher, yaitu:

1. Jika dua byte terdapat pada baris yang sama, maka setiap huruf disubstitusi byte di sebelah kanannya dan bersifat siklik.
2. Jika dua byte terdapat pada kolom yang sama, maka setiap byte disubstitusi dengan byte di bawahnya dan bersifat siklik.
3. Jika kedua byte tidak berada pada kolom atau baris yang sama, maka byte pertama disubstitusi dengan byte pada perpotongan baris byte pertama dan byte kedua. Byte kedua disubstitusi dengan byte pada titik sudut keempat yang membentuk segiempat dengan ketiga posisi byte yang lain.

Setiap tabel yang dibangkitkan pada setiap round akan berbeda. Penerapan playfair cipher ini akan membuat analisis frekuensi setiap huruf akan semakin berimbang. Pada proses dekripsinya akan mengikuti kaidah-kaidah sebagai berikut:

1. Jika dua byte terdapat pada baris yang sama, maka tiap byte disubstitusi dengan huruf sebelah kirinya dan bersifat siklik.
2. Jika dua byte terdapat pada kolom yang sama, maka tiap byte disubstitusi dengan byte di atasnya dan bersifat siklik.
3. Jika kedua byte tidak berada pada kolom atau baris yang sama, maka byte pertama disubstitusi dengan byte pada perpotongan baris byte pertama dan byte kedua. Byte kedua disubstitusi dengan titik sudut keempat yang membentuk segiempat dengan ketiga byte yang lain.

IV. Eksperimen dan Hasil Eksperimen

Berikut merupakan hasil eksperimen pada data teks berukuran kecil, sedang, dan besar.

1. Data teks berukuran kecil

```
Merancang dan Mengimplementasikan
Cipher Blok Baru
```

Plainteks tersebut dienkripsi dengan kunci "passwordif4020__" menghasilkan pesan sebagai berikut

```
EzTk0kOh2914a9WUnEBMSHaACSVtprTPbHh
WvuRVyFjLQUBqLIXkI/BXu/oHQ9o0Id7o+S
7hYK1XXdXGCGK2vA==
```

Proses enkripsi pada plainteks tersebut hanya berlangsung dalam waktu 0.004 detik. Apabila satu huruf plainteks diubah, misalkan huruf pertama diubah menjadi huruf "T", maka hasil enkripsi akan menjadi seperti berikut

```
EhdOobg7+U3csRHNOvjsv3ejo1aWPJZfyKK
S50LtaK/KYuoZ1x/Gs1SNf6Oh+3rDIP1Cit
V7Qj3zhxGfrtoWSw==
```

2. Data teks berukuran sedang

```
Himpunan Mahasiswa Informatika
(HMIF) ITB melangsungkan Home
Tournament 2023 yang diadakan pada
28 - 29 Januari dan terdiri dari
beberapa cabang olahraga
diantaranya basket, futsal, voli
dan badminton. Kegiatan ini
merupakan salah satu program kerja
dari divisi ClubHouse HMIF untuk
kembali mempererat kedekatan dan
kekeluargaan massa HMIF yang
setelah sekian lama hanya dapat
berinteraksi secara daring.
ClubHouse sendiri merupakan salah
satu divisi dari HMIF yang mewadahi
hobi para anggotanya, khususnya
dalam bidang olahraga. Divisi ini
juga bertanggung jawab untuk
mengakomodasi dan memfasilitasi
kebutuhan anggota melalui
sekretariat HMIF. Setiap minggunya,
biasanya divisi ini mengadakan
kegiatan olahraga kebersamaan
dengan sesama massa HMIF ataupun
pertandingan persahabatan dengan
himpunan lain.
```

Plainteks tersebut dienkripsi menggunakan kunci "informatikaifitb" menghasilkan pesan sebagai berikut

```
go6Ua3trsHgn/42q2B7Le4ciRCN6RQdxDCo
oGV6yk1SKEESVavYF+N169HIMnCTe/9iMWs
vpKxdyZtQycUESUUdBXDMalaXad3rzYuTIk
EIV4nosxD4QqCCCviMoQqF1OU2OtcwiDU41
hunkpyO+gQZhIOP/AjRyjyGjLVw6F3BroQW
8MBi8LOJAW8i66mQtKCI2SuhBGFWgNCe6F6
L4oBeuDrB85w0JiB6zd4n2kP08k8Rsk0Mhw
DNR0wk7x364RAq+RZcgp0H6AlNlZBvIqV42
r863emin4hBVhiNy1fMitvzUkNkXEZMiWft
Np01/X9C3n1YIPQtwlgp8FpFW0Gefe9rfdK
ZjHlFCjksI4IsUTg0KC+lxPiy1SoC4R5Q7/
5YS3w3czF//aVZ/6xX1r9Va2FKZFo+dpkrf
ZSGY+S3CmmAnveRqixCbM1sdbSvWUmE8fJz
7j6KxnbBJAVXUWawXHo5NDUW3OCVkVgw4ry
dZM7Cv6nx0w5g0bkNE27izoB/Ed8xwsKYf0
F7CiTgAmm8cAaKKyhe2Lx837m8OmIqORG+q
Ld53tg2wa2hsMU7K4v8Fthy8qQC1IyhyfZU
SpI/EY+lFo2TKW/wd8NxHpUzTgYPDIzaWYG
A3jraAiI5IdkVlobn+f87gP2oSO5FNsgP05
6Pit3zEAKRXO/cwrJ68EHcJzK8jzaScTtQO
Zg1sT0AcFhj7QXLBkQZDo2UaEwMHy5BW9Nw
/slENplvS089ON3mASl+5SL4kzIzP48gAEF
JPSqQoEZ905iJaapCRPjUpim5ZWdsHp2UCM
YeBBR7VRCFIFa+rI7NXewUcQazXaWqAXxQd
/oAnN9hTTlykMu6Ltrd94FBRwJ1mwhrPXBF
hQ/kYfI06fdMp3nEEeVatlGgsEYatPmqtDh
Tv7Ki4QV3TU5rYdw5AxCgfQNxY8DejbNFAB
Qhi+3AxehaXx4W06v/xeLFEyfWE4V4Aa93e
Lw5lNEL2wAzFRRHRWlF/34t5U3yK5t4NE5Z
1fkkLBOFv2YsQDU4pYZp7T9E63HilwbTiJH
yNFTYZTTtGqzy4Zb23aYvKLUs263BuMCKRB
57Z
```

Proses enkripsi plainteks tersebut membutuhkan waktu sebesar 0.04199 detik. Apabila satu huruf plainteks diubah, misalkan huruf pertama diubah menjadi huruf “S”, maka hasil enkripsi akan menjadi seperti berikut

```
kOVr2jTbtvuVQ5IoXGW9tZVJu5I19QHyvpY
3m9rJ5ZqYe7skJUYDe2/G6/CI51IQ7bNz64
RZLZTA2suw9Tpkn1Uqo4JVJaNZxcbs4GCz5
owHiYWdi44WK5I+oaGsOde7KyZxBIOSC82H
OvZmI1jITxQK31KwsjLxPZ28r9hBYb55yvo
Nf6i6r1D8REo+kRLjOknJ+6fxHtYSiDg4k9
mObgXF8QEzVwuKOqKs9Q2N5jMu+Dvd3PMnQ
4HtzIu/vAh2VmFB9NiQocJIvkzn4GC+Z0xd
UH/4ym4kUKxKBKcJoz0w3QNl32kRkiGeRnn
J3DuxTbtILhm4O4jCKhX+kuogHnX0hGuQxK
DgrO1dDM9zlkUGJfK7RFl3vZ4JVQI8POL17
f3tbkJsytxN1Un9b26DYccxJ+PWpokeFPbA
56Xjj+PQ8Z+W8lRsCKInLNmZFl0YQArDzdN
LiSEDIa/LhS6il7584T8CvUM0ipl71IhD2e
lLWE8epcxyQCqIccHAoM59snQ7xoPAtiWtb
EFADUN2VH13/hPFehE1naMobOt17kScL5Ab
Ym5xNb8MdOroSjgE8JT6B1MMr4MHnzfw+e5
kap2vnFgKE2JJ6UACclg804LB6nxybIaQ49
KLkTQE8/iGZC6aEPZOeU1Sg3WQv+o7fBGfG
BKtB3pHshhIuXNL2lCue4i4gx8lThYgUVaK
HXuiXSvjp1dLR/FzLRnBJx5s3RFsNCEZRNq
8AO0SJN+ppQFcXIYxBe+/ywyY0w5LmL7OAj
mw++uYFxzGWj3Y7uvn8CdCdd8W6d2EFdkds
wP6c9DHL975Wh+toAHrZIeYOtoZewF/7lut
+AOVi8fRyifS/PzgSQYyUFbSciF5QJ60Kt9
zKAapMz08/mGVwfOAAiBjhgPToMkdOOkfsg
ttaNPOj0+4rCuXxwjDdpQAwlgjhvmxBy7xS
rhkeMKNZZQTvPN6+JQOyf70z3Y2XUGC76ao
4RwOy/O5cApG963O2NUEqUVrOIM7qW4LkCT
JYcuPf5ehy+DvvAGZZxnJ8864WAPTD6aJ28
3CpTCa/4dZKbjDE3OlAnR7YvswaMLSL6AVf
OgX
```

3. Data teks berukuran besar

```
Integrated Petroleum Festival
(IPFEST) 2023 kembali hadir sebagai
event rutin tahunan berbasis
kompetisi perminyakan internasional
yang diadakan oleh 3 organisasi
yang ada di Teknik Perminyakan ITB,
organisasi tersebut antara lain
Himpunan Mahasiswa Teknik
Perminyakan PATRA (HMTM) ITB,
Ikatan Ahli Teknik Perminyakan
Indonesia Seksi Mahasiswa (IATMI
SM) ITB, dan Society of Petroleum
Engineer ITB Student Chapter (SPE
ITB SC). Untuk pertama kalinya
sejak tahun 2020, IPFEST
diselenggarakan kembali secara
luring. IPFEST 2023 mengusung tema
“Integrating the Prominent Role of
Oil and Gas in The Energy
Transition”, melalui tema tersebut,
acara ini diharapkan dapat menjadi
platform untuk mengakomodasi
pengembangan keterampilan teknis
dan non-teknis di bidang teknik
perminyakan dan menginisiasi
inovasi dalam industri perminyakan
melalui kompetisinya untuk menjaga
keberlanjutan industri perminyakan
dalam menghadapi masalah energi di
masa depan. Selain itu, IPFEST 2023
juga diharapkan dapat menjadi
platform kolaborasi melalui event
dan kompetisi. "Tahun ini kami
memiliki delegates international
dari Filipina dan Algeria. Untuk
main eventnya sendiri
diselenggarakan pada tanggal 24
Februari 2023 berupa competition
```

day. Pada tanggal 25 Februari akan diselenggarakan IPCONVEX yaitu grand seminar dengan pembicara dari pimpinan lembaga migas di Indonesia, acara ini terbuka untuk umum yaa. Di hari yang sama, akan diselenggarakan Tour de Bandung juga ke Orchid Forest, namun acara ini hanya terbatas untuk delegates kami. Malamnya akan dilakukan awarding night pada acara Gala Dinner. Istilahnya acara ini merupakan acara perpisahan dan malam apresiasi untuk delegates IPFEST 2023." Jelas Devanto Wicaksono Soekardi, selaku Executive Director IPFEST 2023. Kompetisinya terbagi dalam 8 lomba yaitu Business Case Competition, Geothermal Development Plan Competition, Plan Of Development, Smart Competition, Mud Innovation, Paper and Poster Competition, dan Oil Rig Design Competition, dengan lomba terbaru yaitu Well Design Competition. Tetapi dalam pelaksanaannya terdapat serangkaian pre-event yang sudah dimulai sejak Oktober 2022, terbaru terdapat Company Expo dan kegiatan sosial kemasyarakatan berupa Blood Donation yang telah dilaksanakan di Multipurpose Hall Gedung CRCS ITB, Kamis (9/3/2023). Company Expo merupakan pameran terkait perusahaan-perusahaan di sekitar industri Migas dimana perusahaan-perusahaan tersebut akan hadir untuk memberikan informasi menarik dan mempromosikan inovasi perusahaannya disertai dengan pembahasan mengenai proses rekrutmen perusahaan tersebut. Untuk Blood Donation bekerjasama dengan Community Outreach SPE ITB SC dan PMI ITB terkait pelaksanaan teknis dan pendistribusiannya. Target pendonornya yaitu masyarakat umum, tetapi sebagian besar yang berkontribusi merupakan mahasiswa ITB beserta dosen dan staf pendidik. Nantinya, setelah pelaksanaan kompetisi, masih terdapat serangkaian acara post-event sebagai penutup dari acara ini. Dengan nilai-nilai semangat, progresif, sinergi, adaptif, dan berdampak, IPFEST 2023 sebagai platform kolaborasi diharapkan dapat mengakomodasi keinginan masyarakat untuk belajar dan berkembang sebagai seorang profesional.

Plainteks tersebut dienkripsi menggunakan kunci "kriptografiasikk" menghasilkan pesan sebagai berikut

```
l110ILSG8wfZOgS/DoqSOqyFKota912zGt4
xGPtG7OHwap+pKhEOTp1aLxc8Zswvr4k8sQ
GXM+E4ic+TCRHa3VMr5/qOQfontGqamgxKw
sAmq9vbyiF/362gYbd1fu1O2zAWCbOSo77t
hw/YEvGjgkLS8Kq2VPDQM12IB/sscIcE+KX
NIuhigMCqflDQeyblxGfrIeWKH4l5oXt/j1
kZPRIC4737v/F34IoGvw0msyHHJ/oQrduB7
dkpr78EgQYLYZp2s85+OptRw60gDXPq48/G
GyYO+WfUPmyfB6icgUQ/SLJMRpbD/dwOV07
yGUT+28EbeU0f9Jhu4VLVpF2/6f8HZLe2ir
v5g7xULXniLM7/R44CKVXDem9JVzbPGtSBq
tlBwimi4yaxKjd+pfuzBXdrZjlCUZBn1wfP
FndzsLtRrGJ7bZ91LOFGjI0omMUfWCKvH6i
hERG+h2nMhS+9RwRtHKG0CGYnuf302GotbF
UYmPtYA1lKYuk/0JdeZIjMeHdRMus2i8VNM
7pWN0AOm66x04g2l2XN3da82uYQGtgBXQG/
oIPScnMJvlkSnAa3SYimfJ4OTdJebFbasz4
DFrH16kOt8w0ipWHw3e52BJ+3SpWkPZOXYa
MN6tF6gpiNyYnlpxjB/et1q6G+nhJa2e9y7
SHVVxCIv1ErELkaxkCx0UBlj3P8MabjtX4x
NvKH5MwxhOzBQ02A4+8+IJ6vbHQj7ojzEHm
/B/00OzKqNBc+Je4d371YOrcY6eSFwQS6Uu
/SRVBSDm/OX/MiPoTuSb+RRwi1Bl042JwWe
aOTrDHUPd46NtD/v1yS0CoQQHcLvz1AZ3zh
3FJO4SwuqFaFXQ3cpCDaaTb8oRp1X+4DbXA
0roGcC6igJiCU3dd52DF3H7gIht+kh1dnSj
vbHL41QoxsQKcQEmsxIVwy8ZpWwbeA7hxJH
L3WUchxw6XBph26PFHqJtY3vaUCUOA4HoS3
kVZHTgh8STSu06o0BttZm9O2FxyfMttpvf0
XatbuYtx2TXKeAxhOmSNIt4jFMSjZpk/X+D
+MaOzMdS+IRzu3il2HAv8wWB7xZZSWY7G1p
Ith+d/oFr9jI3hqwZcyg14x4FCVmgRo8366
YKEoL0aC2rKcY0wm8gOUUZFSEO31NBrozdz
NqkE8TnZHOpnN3gkz7O3pRADZsinaIVvjRX
SXiH+mCKbzHnyjIUuXIEimTvyitBNMccphC
YQk+Xj9NLCDAnKiUtDrjiUb0rxoJw6MxVl2
+4I9s6mrEtpAocOyVizlRJIbi8ORBmFh/Wt
uNyBxKB12/dQxljUNzwy0OH+ANOjhGUmp7h
zjgC5wYj/buZcPuGoC6Tm5Lqwb6dDBl1JkB
9FbtNLakQMBnwTwaCnvp9hxeM5CoZeMABUP
ejbcDiV4Qpa6QwbLL5zjW2nnBX31PD5pnuH
p8ze5Cx1B+tGrYZb6DhIYmgAMtf0R1XcR3r
proGLZbddhuihQLvfU6U68SoZdUXZxNyHE7
viLKrlGr6FlKdvzJEERywM1WmRZ7G55NiIU
0zjyt+HoSZczLESQq+F0IQPIUhp2GibgLTG
```

```
HBLNVjUahbB51zIcG53bz4hQf5LiD/CAHe4
po+J679niGGkCQYKB6W2H+Uw6P3dz+xGkmq
pdsUd/oH7WoAJe75qMYQb65MGZxY4LOTTk8
uaXN3X2Oq2UBINGSJaxgo3mtRKK6F+T2ZZf
IQLafwdcTy7ZmWzrkCZ/c9m6Mpf8R+hMvNK
IFx0Gc4qbnld7ShqYlSuxb9v/mm20i7fG//
4zu32WMdICu73DPEWjoGE2au/i7kz6xRzjb
0smA5xwN4cqck0+SWoPqdCW3f3i+4hAkX/x
QgZmT4qmQpKv1SCx56d9Zdag6O4uMVVSla+
CmfdiOeh8gQsFp3ZXeHKhDcsfFl0Vx9uCnz
KyZZZXDYP1rXgBNkRn2ubmxGOYJq3mCThtU
GS3P1aqLtfs4LLkvM215CdXkyyDxh2pUBmt
ohd4YqIe9vq8d6t8Gy0F3L1zQMrNrOYsdOO
ZHbyVJadM4x/QqyKGeEAivjeUsNDdOIAuhL
L+nFE5yNooa5BKyCzyMhiLChwgj9Z6L1PwM
sdkhOBErMDYEeShsRAazQoUNibBvwkeN0H3
Mxv1D34AsfZYao9qRAZ79xIdZcKrk76wnO3
NfXXfSbMXVmLJDr167vPR06Kv4XE7aNtJ7h
DDXKtOC234L4bm7vsAydmG0QAkql7eeOXRE
6y7gGyZ+k2OtWlvepLcQNwLbN7BbHamhkH5
wHl0z+36V/dzTm8Jo/Kdcs8omuivuPT/zHA
k5iXnXz5y0BeV9udz+yDlXQRP/7dJyxJQ1B
6nEF54Rmb9k9Vx2raZYzMo6Ye926lnu5bXx
zXHYKl7wJHDAMog0EqJpE1xCGcaS18fiitD
N1nqbLo+POaG0Scae3ES489LsYRtr22vtwv
3AAzXY0eG2YW/BxLs2YD2+9Cpi9lqsGEY5A
NHPBOi7N4UBVpFi1qRhQssmBL9tB01cH9/n
82d5WuzR8tAT51j6en1fRmwVngTR9zQWURj
pCLZJxhS0xMK7UTqkAj7wAT0OkLGDgyjwQb
QQvLqUI3m2MiQKcapr2yNlQtGsit0GaLJLx
gS9B5uVBjSDsyQnbGH3S5iZ1cHBNPzUOX0A
pjl/YY1dznoEXCNkXcJVuC8eSRaZrvCu56A
04G4l7JTvg3lqPoWsQxeOfFuuBDjtkqD3jv
ope5rr+/Q8w36EsRQLUm5c8qLyAZkox+cZ0
oumj2O+ntlS6TOiqCPIb+s3TsIlGr5wFATB
OH+TmhqI8FfuJTnxUE0z9wMyEWGNJBByVjT
x5N5WYo2e192wRPXKG3mDBUOT30BpEthWkA
ImuZg+KVWjUdu7OCCFqXUGxKDEJDrcS7IAi
dhENaK4LsHSFIfZDeDTrQN9bHbQ+Szw486Q
BZT0uBpsyZ1nTtvn8bBe8xHaSm+eqXWBj8t
nXmavDmFv9zXxhKN1ZlOvHMduKP9U/F+w7N
EeoSHH/MUqL/sscKkF69qnX4cOoauRzdfqY
gc4/ww1JyfD6a104GQwVGMOeaeKO/7jKOCc
0dCbZvZD9qdSFLlt4grvsZJwnVCto66rKj3
+7f13mZWdkntOF38B88CO1hJ8GawTw/bYL2
Uhe98EAICsyGyUiv/GB8K3QDkMQxzJfTFoa
FHnan8OV4fg1z3gDdK9O0fV+dePj4527HIx
IZ7P2cNrM2EVieLWGhVkAchCzIFAruHN9Ef
w4igAfJqtcvmi7ABtoVMrFPDLNdsxsUjTMD
rEVc6AtBLXbVPfGOKuRN3Ybpz3PpWnT/Y6M
2JTP2mY+h6kV6PeD2SXDn5X/+4ZTava+wu+
JF2dDSRO5iew8f2D17HiCiINtNrFytnzqsc
DboKdIRISqKSbtSO66S9yYZLaG7oqErP4y7
sXDsxNjlvXlmeibp80AIlpB2eKn/0gvO7Kd
VQ5O0z6Y4D0ghJKAu9P3OnVGr0lf9Oor4bA
vEnNVkcWoApfbCSuzihvTgs3wllEpFEsrnU
tLQHop1LKn5028Iu526HAzcYf/BasUd/KPP
```

```
38iBsK6iZps+/4HzWcyuT8m14g/i2XYVwy6
FFShxMXvx2M8r7Q2irP7ey4Uz5wuatOjQkO
MXK67YxwMVJ7ktvITdfJ2nlx3lT6X1LmMs2
ZvAFhE5wYfJOz6K+0mqvV9WwECtREWzcOit
/eqd23yV4QPSloL0IURnhKxTyR95XJS4JQX
sMyXphqxXBNHSwOkzy2iT3jIMxJ62Fjm+Cs
LLulu3lhP8hdv5yH+Qa2Iu0DE0DL2Oyj7jz
JjwFYWZQWU2V9SqxQJupFm61/edeSqs0jQl
3lMzb3MqMGj0rl55/S8WNUv6UOSo2kZeBqM
RO8lIeAD26hqXpUwtTEIpQa6h8uFRuOfSK4
RhDkqDsCXiqzXSOJIu0vg9JQlAuNp6G4aS+
KQZO9P2JePwV4bPctchY/rLNsNPTzv73ezx
FczWbI3NjEhiXPASYzioR6fxqoBujDxWcgD
Fs4z99jDl7wMbBN/t53l0QYDNByX/7yU5BX
q/fBG1SpOirzeZnNbrPTAC+RrlcrwTrwya9
cU2TwVwVQhVhI+9YM9kmtU5wlPs/YZ+bjQP
obw7iJ23scCO3Vd9gEV/0H8XFllb8Z1DGD1
MdYUpSJ5s8NGqjsjZaR7xWm9ZsC6XTuE/Af
DAHAWGO+bL/P/n9u7Y5dIPUqUKy0RsWDEfK
uikXVX+sWQJKQqZNr5FxXyE0bR7dokQbi+D
v9H7lj78VsN6MM0lub
```

Proses enkripsi plainteks tersebut membutuhkan waktu sebesar 0.153 detik. Apabila satu huruf plainteks diubah, misalkan huruf pertama diubah menjadi huruf “E”, maka hasil enkripsi akan menjadi seperti berikut

```
PRc0HiZ+TIX1g+w6Kq4S6wbParXID+IxNmf
Znd9ibDBaIN+XuOmxzLHjx5IYQkz+BcN8j5
NvjGMUMCcWLTVaDPlhp8QcuUWlmNNyHyhuQ
hGM4ZvlWNnAXYEZiTJRWm2fcXpWNyFqHDzB
PuddNtUjU+iYsJQkrE9SH+Rggt8I8FausuX
zsBDdAuwTltX0X6Y0bi2rH3dyoAtVGJP6q3
2Z7LhIo4NpR071zDPuOikCM/BtbbouPyM+b
/WQRzogpYbay9A2jVyGhRl9ekWlKVdqMmWM
WxicAdhWEtV3goy4AZWVAvJy1G58f/C3v8v
WPcQvcYtbR9/nSxpCWLpQgHk/OFVNJIkkcg
R7rwW8qF3GrB9VDc48u618+EPwv7PrPlRQA
JMB/LtaXKSdk9/7gd8z1N0hJgfQqS/l+74n
k1NXMGr75iJF/2fKrs3/ZAgMvEXO8mjvITp
ZrpOSPoFJoQs9lq4nXJ8m8NmllUQcXU4J7I
Sy0rtmkaH14MWGOBJ6QAgd0j0RDHnONEdhi
lLTE2SOSgT7k7akb9pP8W9UX8I0mgmrF0GB
Mntt8F+wVtw2uIZm48LmQgz28lBy1b5flxq
Dxxu/qn0/C7KgidgYWMpShE4dANWar2so44
+0AlRephhcY8OlmYo5QmlZEkk7ujbaCEU4r
R9Hr68Kk+jDlZ0+RpEbmwBbHYtDs4paXfsV
EnJWToZxun45/M+sWge7BLovvd5prrZh6MY
9K0TcvhaOtMaUb64jTUXnuJuhAWGh5YRr+K
WSe8Kqse3i5hunGqBumBXbBzYn/uK69CX+/
Ie3LOB+d54EpChAPXArOK80ZPfaFXcAWe4Z
Y9BiWMSrjHIFjKeW5B5IkYl+jaOd2son7aG
e5MGimVAfpAwtNVJd/LGmtfJIuE1cONVL89
NeOJq1kyYmAJmC6tSzDeXadL5yQWYqpFx3j
kVp0+TIKyDlgp1rlhuqGETPAicu6Qi9OqA3
```

```
QPwNDjbusYss/xPcg/99GwIcXVyhoCPWP9G
uglPKRlyn5zjePYq2JqFkDmBAFQxZd+WduA
EekFNOWZZgwh+TCowtSL8OyuZO57gvizSRg
AuwU5WoKC2bnPpGeH+3p3qxMfrf2jr6C8E4
TBjAqmKmWmM2KQwYYPsr073r+GjREJo5Z5a
NlNPE8fRrg3FI+i2zPUejBD5LSpZYDeILwF
CzCK4MQubNjIQco2cuyM2CanxzHlkMT1iZt
gYIQJB4EJQD09joEu55dpqZ/gWAoiqoRYjc
scIDIVEUkPb5SUaWcqw07thbtVFpueNNRIP
rEwTx+bc8veqjboqP47VcvVuktDlLUwmXfO
RcAgLJirr/nRfeEiBC16tBkS43UDhEs3bk1
nsR9OxIabyDs70Y7Q3LJwnbMo58M28zgjm2
krP4KqWp6Nz6fZQzkB7P4oFiIVl17ZQj3t9
7C4g7J6Spf/WP4UdQRFImCPizN9GoPfI1+j
q6CiiZU0WZBap8lx9RzWo8mywXEUjjz55Gw
kFjr51iL3DPY5vNtrmuSS+MsuF9yO6onGhU
7aoKCGPE8H+2CGAQeks+YT1aqqX0Np8IqBW
jhGL/xwaf/ubKTqu/D/PXxpTOTvLDwrL/xA
hEQXY+0lwGy+raIJ7oo958f7dnWPjaRLiM4
NdSwydXnZkR6BKfwiPJ6/T5DvSJ3ADi9NG5
nYFNDNfE61uT2G4QCRWIJl2JxHMQXaTI929
3wpomKVI37za38XCkNw0kSeygHBeU3jev5Q
hPh38OGhlluWc6A4IByj3xvL/YCZWdb90GF
wnK++Vd3sru0eI3rurEoaUfn9w7QpT7BwZJ
KnYCy6XlZO64E544EMPU5t0I/VQHCpUAe3y
BK9PT3DtoGynZ8cT8zfvZpAJwe7UeresnR1
lO+Pyq+s6KCIFXT21hnoT6mkLhs8WgXKrn8
j5h2hfv2RXueiTNQLO8+Ycj4FmLh8Bqyz9w
mfxln+q1JwOHrpWW2+hdLVU1YWqxufisuel
EPDadjKM9bwVXquGUM/71A+U4t5dPuVq3cq
Z5/d326/+BL3EO7CFPukLvs3fUi7VimeMkC
JsnxeQ4drSIHK0wJ4VkAwbmB9mJv961RgSz
M/WY0JQPFLbV02IsepRL/QchMFjq5mMNAde
GhsPRJz+uUS/yJv61gU9Xjsdn4lJbbYCe0/
Z7efcDxo+VpiC7ENyXBRzxzI94jeSQduzpf
I9VBmpqXlovYWgR9IAM5JkLwiWTfzK6HfSV
QWSgJbSGLOGB47NbgJOQ5qiRd47J5RYjvMe
Ym3kXe68/t5ztCTrXfovlW08Cnqs/l3WzIp
vBNvv7dnQxIcH9aHa0iAfFuax9wWuaQbARh
3huXd4vC0fbd3DPRSN86Erry6U21MsWWjfd
dJldDnpw9dqKcram6h3rP+WqnOK2VxZIwJD
zRIIkrKM20SSQbUZPdg74zUAU3plHYoNo5t
lA0p+Skd8kmdBD6ALe5RmadPvIvBqSir6Gg
v127G2fEwXQ/Nsi6DaZ/UkKvVfoI2ncznWt
s1nrolNT3mn7Ynze+qz1DCwrDPxudRivuZ3
NLDaYbF70+lBD7riIu9Z1JRmOQRvJwxZiuQ
uSkAN8pl2SsvWgO+pVSdvawP0VYlgiTDKab
E79OQltubavCsyiSEV3mjLTlf9TzENWFcTo
Ix1b4Vz3hDo6ztvb3+7sUKo6bZZIBLru2TL
MX+wJVXxqp13q7y/mAykchOQsKIEFF4TTDi
uDMdrVaQyDQVI9WZEvdu6NWOiyPwvQeGU1a
2Mjq0c+T3MYqQ0wUJxKQ1Lfy+YBmm/aXkT/
qocsGDYxGNLKAbkg+gdzyZHKruOhnfj3chB
xNXQcIrMML2IyaEwinl2nhZI5lQBXgCDpEi
6fUR0aDdVy+5H7BrJ9FvcqfUhBAB5cmhhKy
ebWzR06Ang6kaP9jTF550ND/o5vewBJC0u0
IRQlElAs9w+f8VnLSFjb1zVam8XU6UsTd3T
```

```
lct9Hi0VLd+RbzuNL9KsQnuvXwHpw2N9hRp
ten7M/Q0cGlhOpVI2FOnDtH7mcWRQT4W4C5
yMcf92fbWf9e1XLYkiJvOYqXSdbkbSjFnJk
blK33x7G0oPSxRMnojR9SS3yselFJoqPqux
Up71JC20iEFf3//ol10BffFg8Jz7rfHT0lo
2kX/uE0SrmiFIGckBEK3tfxR0ow81jN3FW+
qlY6FO3vwLE870xp5j9BdUtRlWjNmbzyFax
8DSFmf35y96XpVs+nzFAgRnohsF+PBlydmt
JCq0kWBp82LPi0pKVHtEHrRhOEf+xYOKZcA
RWrXECmKs/6Hf7mDMEDp3m/GRIvLkep3MeF
+KClSPYxIxc6CHytowSKlrXLkRTDZVIA7Q8
COR1iABqZvYau729RUldiA60XF/h7lkiAI1
DUBBlnpA+EUwekQc6OIU4IaxI4wWoPgoQTp
8zjh3nxBvpBJ8d7LON6AxNI+dbNbdggnwyy
tYVgqR/R6R0U7gAQtHdJFZXNgTN+veML1dq
9gnzxL+pIibmhKGK6qi+5EF3/Mu8G9MAF52
oCSVodviA36OkCDQ79xgoSOI7fMcGG5/0rg
VDCjezAqNNl28ptX/c9HYEJNwMR8USRXiyO
fsYxy2FR6IO3gc4Xw7rbT0SGX5OK1PxDyW3
2feeyQyhmxg7rEkw8lXlY5H0+nB6jviscvM
LRL7jPyXw+beXaH4e0OvrZ5S7iPj9s7Iqrl
8PA5f398zogqtElqqRYlzKFJbbt6tbsz3Sc
nra27xORaHnV2wwAcQJCxFayEltz+GyMars
EildBPtNhiDYm7gHKKz8YtOR6/9J9FVLaxj
tD9DyE9QowZ3CyIDpzm9hvy2u053SlF/b/d
/Jit5yFoeGXuCvp6FACdzWkxzmz6mA5THAe
1OCBn8/jUIYQf9w5lQViN5a1I3WqpmixMo9
YjRkeZFIHhQhpZwLDlTHBvZ0FNon7eGG+9c
1w78E1+d6G4Wpxr1tTITHEzFAjRx2m5leHr
sWjVhaJGdGqpwnhAIXClXQNVqWlBB8R0uZ5
N4c61+ypBSwDyK1QVxbLqydKPTyjlS4E67F
U0hDN+1Bvw7X+UhnJPPtktcuLHuSKb/U7S+
N+S6waZeoOtpkQj6J0m0tgjZvfvFKn1lhbE
PzRpytW6q2Qq3r5SC71dG+GfRBsT/IfnvD6
lWg7RalXyeIPoxsXDzbrys0DSSAxc0GltQ7
jNBqEiOA/kdwfFPXBQt5BHX7+ub0eFd7rnC
CM61Qe8+WkTja6a35HOPV5PTzwpNMEddIsn
vDjUHcbenV3yYo9ttK
```

Secara umum, proses enkripsi menggunakan algoritma ini cukup cepat. Algoritma ini mampu menyelesaikan enkripsi teks berukuran kecil hanya dalam waktu 0,004 detik. Data berukuran sedang hanya membutuhkan waktu sekitar 0,042 detik dan data berukuran besar hanya membutuhkan waktu sebesar 0.153 detik.

Efek longsoran *(avalanche effect)* yang diakibatkan algoritma ini sangat besar. Hal ini diakibatkan oleh adanya operasi *subBytes, shift row, xor,* dan enkripsi playfair. Hal ini juga telah dibuktikan oleh eksperimen-eksperimen di atas. Pada eksperimen pertama, efek longsoran yang disebabkan oleh berubahnya huruf pertama adalah sebesar 95,45%. Jika menggunakan algoritma AES, eksperimen pertama hanya akan menghasilkan perbedaan sebesar 94,318%. Pada eksperimen kedua, efek longsoran yang terjadi adalah sebesar 96, 875%. Jika eksperimen tersebut dijalankan menggunakan algoritma AES, maka akan menghasilkan perbedaan sebesar 97,97%. Pada eksperimen dengan data berukuran besar, algoritma ini

menghasilkan efek longsoran sebesar 95,3125%, sedangkan dengan algoritma AES menghasilkan efek longsoran sebesar 98%. Perbedaan ini dapat dihiraukan karena cukup kecil dan banyak dipengaruhi oleh pemilihan teks.

Algoritma ini melakukan enkripsi dengan membagi plainteks menjadi blok blok berukuran 128 bit. Algoritma ini hanya menerima kunci dengan panjang 128 bit. Ruang kunci yang dapat dihasilkan adalah sebesar 2^{128} atau setara dengan $3,4 * 10^{38}$ kemungkinan kunci. Oleh karena itu, algoritma ini sangat susah dipecahkan dengan menggunakan *exhaustive key search attack*. Jika sebuah komputer dapat melakukan percobaan sebanyak 1 juta kunci per milidetik, maka dibutuhkan waktu sekitar $5,4 * 10^{18}$ tahun untuk mencoba seluruh kunci.

Algoritma ini juga memiliki keunggulan berupa frekuensi kemunculan setiap karakter akan terdistribusi secara uniform. Hal ini disebabkan oleh penggunaan algoritma playfair pada setiap *round*. Hal ini dapat dilihat pada hasil eksperimen ketiga pada data berukuran besar.

Algoritma ini memiliki kelebihan lain yaitu mencegah blok plainteks menghasilkan cipherteks yang sama. Hal ini sesuai dengan karakteristik mode CBC. Hal ini tercapai dengan membuat ketergantungan antar blok. Misalkan terdapat plainteks "MalikAkbarRafsanTidakKenalDenganMalikAkbarRafsanGan" dengan kunci "abcdefghij123456". Dalam pesan ini, blok pertama pesan yaitu "MalikAkbarRafsan" sama dengan blok ketiga pesan yaitu "MalikAkbarRafsan" juga. Mode CBC akan mencegah blok plainteks yang sama menghasilkan blok cipherteks yang sama pula.

Jika digunakan enkripsi menggunakan AES, akan dihasilkan cipherteks sebagai berikut.

```
UCSjg+n0hf6uxuPPHA3ejbii5pwT5u6PUREsWF+/R
91QJKOD6fSF/q7G488cDd6NV5tLp6z/3PydSh5Z4C
qE0Q==
```

Jika terdapat *intruder* yang melihat pesan ini, ia dapat melakukan *decoding* base64, dan didapatkan byte cipher blok sebagai berikut.

```
[b'P$\xa3\x83\xe9\xf4\x85\xfe\xae\xc6\xe3
\xcf\x1c\r\xde\x8d',
b'\xb8\xa2\xe6\x9c\x13\xe6\xee\x8fQ\x11,X
_\xbfG\xdd',
b'P$\xa3\x83\xe9\xf4\x85\xfe\xae\xc6\xe3\
xcf\x1c\r\xde\x8d',
b'W\x9bK\xa7\xac\xff\xdc\xfc\x9dJ\x1eY\xe
0*\x84\xd1']
```

Dari byte cipher blok tersebut, *intruder* tersebut akan mengetahui bahwa blok pesan pertama sama dengan blok pesan ketiga. Hal ini dapat menambah pengetahuan dari *intruder* tersebut dalam upaya memecahkan enkripsi pesan dengan AES ini.

Sementara itu, jika digunakan algoritma SAES2, cipherteks yang dihasilkan adalah sebagai berikut.

```
ITUMok/iUldO0zyLh+PunukJchL1POmAsgfCgVcGE
RKpXh3U37jcv5W+zzjj0cq6s/35IjSF9W0cc3+3i0
WU6g==
```

Jika cipherteks tersebut di-*decode* dengan base64, akan didapatkan byte cipher blok sebagai berikut.

```
[b'!5\x0c\xa2O\xe2RWN\xd3<\x8b\x87\xe3\xe
e\x9e',
b'\xe9\tr\x12\xf5<\xe9\x80\xb2\x07\xc2\x8
1W\x06\x11\x12',
b'\xa9^\x1d\xd4\xdf\xb8\xdc\xbf\x95\xbe\x
cf8\xe3\xd1\xca\xba',
b'\xb3\xfd\xf9"4\x85\xf5m\x1cs\x7f\xb7\x8
bE\x94\xea']
```

Dari byte cipher blok tersebut, *intruder* tersebut tidak akan mengetahui bahwa blok pesan pertama sama dengan blok pesan ketiga. Dapat dilihat bahwa byte blok pertama sangat berbeda dengan byte blok ketiga padahal memiliki blok pesan yang sama. Hal ini dapat mencegah bertambahnya pengetahuan dari *intruder* tersebut dalam upaya memecahkan enkripsi pesan dengan algoritma ini.

V. KESIMPULAN

Dari pembuatan *block cipher* baru yang telah penulis buat, penulis menyimpulkan bahwa sebuah blok *cipher* baru dapat dibuat dengan menggabungkan blok *cipher* yang pernah diciptakan dan mode operasi blok *cipher* yang sudah ada. Kekuatan blok *cipher* yang penulis buat lebih baik dibandingkan dengan blok *cipher* AES ataupun Playfair Cipher, khususnya jika keamanan jika terdapat *intruder* pada proses enkripsi dekripsi.

VI. SARAN

Penulis menyarankan untuk mengembangkan lebih lanjut algoritma ini, seperti melakukan optimasi sehingga proses enkripsi dan dekripsi dapat berjalan dengan lebih cepat.

DAFTAR PUSTAKA.

[1] Munir, Rinaldi. (2020). Kriptografi Klasik (Bagian 2) [Presentasi PowerPoint]. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Klasik-Bagian2.pdf

[2] Munir, Rinaldi. (2023). Review Beberapa Block Cipher (Bagian 3: Advanced Encryption Standrad (AES) [Presentasi PowerPoint]. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/17-Beberapa-block-cipher-bagian3-2023.pdf

[3] Munir, Rinaldi. (2023). Block Cipher (Bagian 1) [Presentasi PowerPoint]. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/13-Block-Cipher-Bagian1-2023.pdf