DAWASCrypt

Wisnu Aditya Samiadji - 13519093
David Owen Adiwiguna - 13519169

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13519093@std.stei.itb.ac.id, 13519169@std.stei.itb.ac.id

***Abstract*—Pada makalah ini penulis akan membuat sebuah algoritma *block cipher* baru dengan memanfaatkan berbagai prinsip serta teknik dari *block cipher* seperti *Diffusion* dan *Confusion*, Substitusi dan Transposisi, Cipher berulang, Jaringan Feistel. Hal lain yang digunakan untuk memperkuat algoritma ini adalah dengan membangkitkan sbox berdasarkan kunci eksternal yang dimasukkan pengguna dan juga penggunaan jaringan Feistel di dalam jaringan Feistel .**

Kata Kunci—Kriptografi; Block Cipher; Feistel; Diffusion dan Confusion; cbc; ecb

I. Pendahuluan

Pada masa ini, teknologi sudah banyak sekali berkembang, berbagai informasi tersedia di dalam internet, banyaknya data yang dikirim dan diterima dari satu tempat ke tempat lain, hal ini tentu saja memerlukan keamanan yang sepadan, agar informasi yang dikirim dari sebuah pihak ke pihak lain tidak dapat dibaca atau diakses oleh pihak ketiga untuk tindak kriminal atau kejahatan. Terlebih lagi, belakangan ini ada sangat banyak kebocoran data di Indonesia, hal ini dapat ditanggulangi dan dicegah salah satunya dengan menggunakan algoritma kriptografi yang baik dan sulit untuk dipecahkan.

Kriptografi sudah ada sejak zaman Yunani Kuno untuk menjaga keamanan dari pesan yang dikirim antara dua belah pihak. Kriptografi yang digunakan dulunya masih kuno dan sangat mudah dipecahkan jika dibandingkan dengan kriptografi yang sudah ada sekarang. Hal itu dikarenakan kriptografi dulu masih menggunakan teknik-teknik yang mudah dan simpel, sehingga akan sangat mudah dipecahkan secara *brute force* sekalipun dengan tenaga komputasi yang ada sekarang.

Kriptografi modern saat ini kebanyakan sudah menggunakan operasi bit, dan bukan dalam alfabet lagi ataupun ASCII seperti Kriptografi dulu. Karena semua operasi dilakukan dalam bit, maka Plainteks, Kunci dan Cipherteks juga dalam bentuk bit. Operasi yang paling sering digunakan di dalam kriptografi modern adalah XOR atau *shift register*.

Pada kesempatan ini, penulis akan membuat sebuah algoritma *block cipher* yang diharapkan akan lebih sukar dipecahkan dibandingkan block cipher biasa dengan memanfaatkan berbagai teknik enkripsi *block cipher*.

II. Dasar Teori

A. Block Cipher

Pada *Block Cipher*, bit-bit plainteks akan dibagi-bagi menjadi beberapa blok yang ukurannya sama panjang dan telah ditetapkan. Blok-blok pesan ini kemudian akan dienkripsi dengan kunci yang sama panjang sehingga akan menghasilkan cipherteks yang sama panjang pula.

B. Diffusion dan Confusion

Prinsip *diffusion* dan *confusion* adalah sebuah prinsip yang diperkenalkan oleh Shannon yang bertujuan untuk membuat serangan berbasis statistik lebih sulit untuk dilakukan. *Confusion* bertujuan untuk menyembunyikan hubungan statistik antara cipherteks, plainteks dan kunci. Sementara *diffusion* bertujuan agar satu perubahan kecil pada plainteks , cipherteks atau kunci menghasilkan perubahan yang besar terhadap hasil enkripsi atau dekripsi.

C. Substitusi dan Transposisi

Substitusi adalah sebuah teknik yang mengubah bit dalam sebuah blok tanpa mengubah urutannya. Sementara transposisi adalah teknik untuk memindahkan bit dalam sebuah blok dengan aturan tertentu yang sudah ditetapkan sebelumnya.

D. Cipher Berulang

Cipher berulang dilakukan untuk membuat cipher menjadi lebih kuat, hal ini dicapai dengan melakukan fungsi transformasi yang mengubah sebuah plainteks menjadi cipherteks berulang kali, dimana untuk setiap putaran digunakan kunci putaran yang berbeda.

E. Jaringan Feistel

Feistel Network adalah sebuah teknik kriptografi yang dinamai atas kriptografer dari Jerman bernama Horst Feistel . Feistel Network menerapkan Feistel Cipher berulang kali pada data yang dituju. Feistel Cipher itu sendiri adalah sebuah struktur kriptografi yang melakukan substitusi dan permutasi terhadap data dengan membagi dua data, lalu menerapkan fungsi yang ditetapkan pengguna (Fungsi Feistel) dari satu bagian ke bagian lain lalu menukarnya. Feistel Network mempermudah proses enkripsi dan dekripsi dengan menyederhanakan struktur Feistel Cipher dan menyerahkan obfuscation kepada Feistel Function dan jumlah Cipher di Feistel Network , hal ini menyebabkan tidak diperlukannya

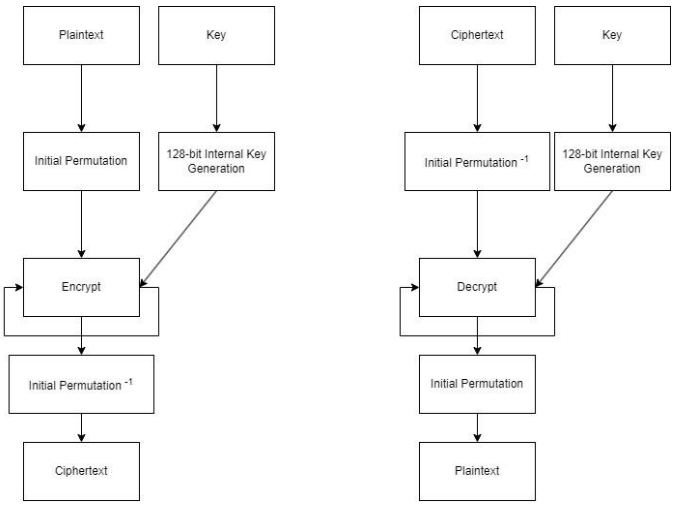
algoritma khusus untuk dekripsi. Kemudahan inilah yang membuat Feistel Network menjadi salah satu standar yang digunakan banyak algoritma enkripsi.

F. Key-Dependent S-Box

Sesuai dengan namanya, *Key-Dependent S-Box* adalah substitution box yang dibangkitkan secara dinamis berdasarkan kunci yang dimasukkan pengguna. Hal ini dapat mengurangi adanya sebuah konstanta yang mempermudah pemecahan teknik.

III. Rancangan Algoritma

Block cipher yang dirancang memiliki panjang masing-masing blok sebesar 128-bit dan juga panjang kunci sebesar 128-bit. Kunci yang dimaksud adalah kunci eksternal yang dimasukkan oleh pengguna, yang kemudian akan digunakan untuk membangkitkan kunci internal dengan menggunakan hash md5 serta string konstan (Unique Key) di dalam algoritma.



Gambar 3.1 Skema global DAWASCrypt untuk Encrypt (kiri) dan Decrypt (kanan).

Secara global, algoritma ini memiliki skema dimana input plainteks atau cipherteks akan dibagi menjadi blok-blok yang berukuran 128-bit. Plainteks yang akan diubah menjadi cipherteks akan masuk ke dalam permutasi awal (IP) sehingga urutan bit pada plainteks masukkan menjadi acak, hal ini dilakukan dengan cara men-*shuffle* urutannya, kemudian plainteks tersebut akan masuk ke dalam proses *enciphering* sebanyak 16 putaran agar menjadi cipherteks, baru kemudian cipherteks yang telah dihasilkan akan di-*unshuffle* berdasarkan invers permutasi awal (IP^{-1}). Sementara itu, untuk cipherteks yang akan diubah menjadi plainteks akan dilakukan proses secara kebalikannya, dimana akan dilakukan "*unshuffle*" terlebih dahulu dengan (IP^{-1}), lalu dilakukan *deciphering* sebanyak 16 putaran baru kemudian dilakukan *shuffle* dengan (IP) agar mendapatkan plainteks yang sama seperti semula.

Permutasi awal (IP) dilakukan dengan cara menggunakan list yang berisi posisi *byte* pada plainteks. List ini kemudian di *shuffle* berdasarkan *seed* yang didapatkan dari kunci eksternal. Kemudian urutan plainteks disusun berdasarkan urutan list yang telah di-*shuffle*.

Pada proses *enciphering* itu sendiri akan dilakukan beberapa hal. Pertama, masing-masing blok yang sudah ada akan dibagi menjadi 2 blok (L dan R). Disinilah desain algoritma ini berbeda dengan jaringan Feistel biasa, dimana blok R akan dibagi menjadi blok LR dan RR. Ketiga blok ini akan masuk ke dalam 16 putaran enkripsi / dekripsi dan dikombinasikan dengan kunci internal sehingga menghasilkan sub-blok baru berupa LL, RL, R. Fungsi transform akan menggabungkan sub-blok masukkan dengan kunci internal yang kemudian akan di XOR-kan dengan L untuk menghasilkan sub-blok R dan dengan LR untuk menghasilkan sub-blok RL, sementara LL didapat langsung dari RR.

Untuk menyembunyikan keterhubungan antara plainteks, kunci dan cipherteks dilakukanlah substitusi dengan menggunakan Sbox, ada 8 buah Sbox berbeda yang masing-masing memiliki 16 nilai berisi integer 0-15, dimana urutan dari masing-masing Sbox diacak berdasarkan kunci eksternal. Hasil substitusi tersebut kemudian ditransposisi dengan cara digeser sebanyak 4 bit ke kiri agar hasil cipher semakin teracak.

Seluruh proses *enciphering* ini dilakukan sebanyak 16 kali, dimana kunci yang digunakan untuk setiap putarannya berbeda-beda, dan nilai key tersebut didapatkan dari kunci eksternal yang dimasukkan oleh pengguna.

Sementara itu, untuk melakukan *deciphering*, cipherteks yang telah dibagi menjadi blok-blok masing-masing dibagi juga menjadi blok L dan R. Namun, jika pada *enciphering* blok R dibagi menjadi 2, kini pada *deciphering*, blok L yang dibagi 2 menjadi LL dan RL. Proses selanjutnya bisa terbilang sama dengan proses *enciphering*, namun dengan urutan yang terbalik, sehingga proses terakhir yang dilakukan pada *enciphering* sekarang dilakukan pertama dan begitu juga sebaliknya. Proses ini akan menghasilkan sub-blok L, LR, RR dimana L didapat dari XOR R dengan fungsi transform, LR didapat dari kombinasi XOR RL dengan fungsi transform, RR didapat langsung dari LL.

Invers permutasi awal (IP^{-1}) dilakukan dengan cara menggunakan list berisi posisi setiap *byte* pada plainteks maupun cipherteks setelah di-*shuffle*, lalu dilakukan *unshuffle* dengan mencari posisi semula dari list yang telah di-*shuffle*.

Kami akan membuat 3 mode operasi block cipher, yaitu *Electronic Code Book*, *Counter*, dan *Cipher-Block Chaining*

IV. Pengujian dan Hasil Analisis

Kami melakukan beberapa pengujian terhadap beberapa kasus, di antara lain adalah

- Waktu Enkripsi dan Dekripsi

  Untuk melakukan pengujian, kami menggunakan beberapa plaintext yang akan dienkripsi, yang kemudian hasil ciphertext akan langsung didekripsi lagi. Pengujian ini akan menggunakan 3 mode berbeda, yaitu Electronic Code Block (ECB), Counter Mode, dan Cipher-Block Chaining untuk masing-masing plaintext. Pada satu sesi pengujian, *key* yang akan digunakan akan sama. Kemudian, sesi kedua kunci akan diubah dengan tambahan satu

karakter. Setelah itu, akan dibandingkan apakah hasil dekripsi sama dengan plaintext awal dan apakah ciphertext yang dihasilkan akan sama.

Plaintext 1

```
"Theories about learning with multimedia can be positioned at different levels. At a basic level, psychological theories describe memory systems and cognitive processes that explain how people process different types of information and how they learn with different senses."
```

Key 1.1

```
"ameagari no niji mo"
```

Key 1.2

```
"ameagari no niji ma"
```

Plaintext 2

```
"""if saying "I won't let you run away," this made Amane feel a little shy,
and then he put his hands behind Maui and hugged her back.
I won't run...
I want to treat her well, I want her to be happy, I want to love her. These
thoughts flew through Amane's mind as he embraced her.
"I wish for Mahiru to be happy."""
```

Key 2.1

```
"daisuki da yo"
```

Key 2.2

```
"daisuko da yo"
```

Ciphertext

1. Electronic Code Book

Plaintext 1.1.1

xpÔÏåMú‹ “ÍÔÆ;
Sêªó£°LøÁ¥¼êPáÜ°þôÙ“ñ°‹…,5L0˜^Nw
&šøLu

Encryption time: 0.15842366218566895 seconds

Theories about learning with multimedia can be positioned at different levels. At a basic level, psychological theories describe memory systems and cognitive processes that explain how people process different types of information and how they learn with different senses.

Decryption time: 0.1571967601776123 seconds

Plaintext 1.1.2

@¦nÁt
xQÏ‹ lþ”éÝ_¥¡Î´ïÏs¥~7Ô)ñëI=|˜%iíÄjÛõa{
Cuí_r

Encryption time: 0.1544663906097412 seconds

Theories about learning with multimedia can be positioned at different levels. At a basic level, psychological theories describe memory systems and cognitive processes that explain how people process different types of information and how they learn with different senses.

Decryption time: 0.15571093559265137 seconds

Plaintext 1.2.1

6J3þXÒ6Á3E
L³, ÉI©]I©K›BÅVù`NgaÙÞ¬
¤I*uvÐåñ¿ZeÂ~öØËÊzIRˆvZîiùÆ)Ï*K
Ýgåœ²²á§*§ÉÌÕno(~_ú
UZ¢Ouèô|ÛŸüƒ©õ¡Õ^ãã«ÔÄÜþXÅ{çC›
, Îvú©
8�ðÆ¾9
(é·27ÊÃ©f8ùg JYMÈÙ«FZ¨h$Ïû`
å˜o$,q‘DD±#ÜuB±¨²+O:iºKÇk®zl¶brC×
ÜñÓgõ[Í8Š5

Encryption time: 0.3971574306488037 seconds

if saying "I won't let you run away," this made Amane feel a little shy,
and then he put his hands behind Maui and hugged her back.
I won't run...
I want to treat her well, I want her to be happy, I want to love her. These thoughts flew through Amane's mind as he embraced her.
"I wish for Mahiru to be happy.

Decryption time: 0.3791921138763428 seconds

Plaintext 1.2.2

µWiÊ¨(
CcŸÔß1ÊZ»/tV;!(q»VflþTM@~ï§¼ŠàôøY
õÒÊœ§04T—ù®ÖqàÛª`ÖÇj‡”XÖ—²åÞý
q/ð‹ b‰ùàe¸W°mãWÛÔiJdN#ÿí�„, °Å/Í
…ÒPÔfûiV„“ÎŠ=
ãÍƒX

Encryption time: 0.18612217903137207 seconds

if saying "I won't let you run away," this made Amane feel a little shy,
and then he put his hands behind Maui and hugged her back.
I won't run...
I want to treat her well, I want her to be happy, I want to love her. These thoughts flew through Amane's mind as he embraced her.
"I wish for Mahiru to be happy.

Decryption time: 0.177778959274292 seconds

2. Counter

Plaintext 2.1.1

xpÔh†Pÿ+TMå×Öçj:*^4b°Ùp¢ó†r6TM©=ë
A,
Ì±>ÆÊ0jO[k¾z#ÁªH8§0ì“èÊjË³£$âåþñý
ùu° ‰F=ÇÈ´YÃËȼl_h=Íð‘¸=î�y·ÑV«ô¶
{!ä+Ó$·XAˆª‹ ÙzTJÒMExß¯;´i_|ºÝÛý®ó
R2¸ñT6
zßzÏÒlä‡‡·ÒÐ1wŒR6ÁYš>|tx¦'ÑÆ- ¼Eë
kŒ-m-1—@ð9lÅf®ìõ}è»‹ ˜ÏÕ5mHB«:¥
ÐéÕfFwãg
§{'…ùZÇ

Encryption time: 0.3322141170501709 seconds

Theories about learning with multimedia can be positioned at different levels. At a basic level, psychological theories describe memory systems and cognitive processes that explain how people process different types of information and how they learn with different senses.

Decryption time: 0.31553220748901367 seconds

Plaintext 2.1.2

ßæ›Â
ÑBÇ63˜®~˜:¸�Ë`”ÄŠÜío@
”ãá|›0¸]±à×

Encryption time: 0.1574232578277588 seconds

Theories about learning with multimedia can be positioned at different levels. At a basic level, psychological theories describe memory systems and cognitive processes that explain how people process different types of information and how they learn with different senses.

Decryption time: 0.14909577369689941 seconds

Plaintext 2.2.1

6J3þX
Ò6Á3E
ÈŒNÄÛÓEŸf^¾Ü·%u›á4½ù¯ÐTÐrö:Re
ÐoRïÛŒ¬:yFúÈHBµÓ°fWªG)a½Rb_%q
Gœ‡ªEWî„fxÙuI¹è„Í9/ô8"³oOÊCäp- t^zä¿
YÓRùÁ+wÖ±¶=F†;WvW½"n1TÃ¼vB*

Û2Þ¿[ÏÒR['9™ƒÁº±¿—\ó£ŠU²ì?çµµ,FÜ
Ÿ<, >ŒYÐ4$¬
¾ŠÎº,÷E{“ª³¼YË²äfÕÌÈ0,©‰ûÈ'o
+ŸŠ- lÅN¿´c:º5>ŒÁ}«ˆýƒF3*àÀË½6=,
)ZÌaeQ^Ú$ì^}ÎØÑ½ÄúÐ&:³`ûË'KØD95^
<°Rõ@V

Encryption time: 0.181441068649292 seconds

if saying "I won't let you run away," this made Amane feel a little shy,
and then he put his hands behind Maui and hugged her back.
I won't run...
I want to treat her well, I want her to be happy, I want to love her. These thoughts flew through Amane's mind as he embraced her.
"I wish for Mahiru to be happy.

Decryption time: 0.18868494033813477 seconds

Plaintext 2.2.2

P%›ù—2Ó¥]N-O¨MÙûwäÉ=uòÃ„WL
Îš¬
n&K  Ó[v&©
ÑÏðå‹ Áˆ…¢Þ°s°{a"¬£~$siXZ£UðÙ‘×
·~r¬_.à4ä8.- ØLp¸÷ó)ÅÙI÷œgç‡Íý˜¼áˆ·
‰âC5IIÝ.“e&ÑüRâwd¿V´7Ió¿¢[¯‘ååªö6ð
—¸MŒCQŸƒ[ðéÏ~Åv6U
{G“üÛ¿$`4›áY—>SÎÓÛeG)§Ä|"†°,
¬

Encryption time: 0.19405221939086914 seconds

if saying "I won't let you run away," this made Amane feel a little shy,
and then he put his hands behind Maui and hugged her back.
I won't run...
I want to treat her well, I want her to be happy, I want to love her. These thoughts flew through Amane's mind as he embraced her.
"I wish for Mahiru to be happy.

Decryption time: 0.19388484954833984 seconds

3. Cipher-Block Chaining

Plaintext 3.1.1

ÿf, &îj¢½5xðÛ[âÿM@u|Uy
û&SÞ)Å…~×uch×Ó%;Ó&¹mNuy4™‹ 5¸_
LÓ»ý8Úx…`þ‰Î/|OŠo‡œÈÉ¾Ô!àÅGÍjÈ÷
~dão`ÅêL`Þ0bƒ#¹ÃB´à

Encryption time: 0.16220664978027344 seconds

Theories about learning with multimedia can be positioned at different levels. At a basic level, psychological theories describe memory systems and cognitive processes that explain how people process different types of information and how they learn with different senses.

Decryption time: 0.14915847778320312 seconds

True
False

Plaintext 3.1.2

U,{,ÀË¯Â»TzÇ¸Ä9F×*FÈIg>]q)ÔH?½»

ìRÆÒjFr†Ø„=‘, DãuzkKÍs1¢ÖÄŸ#½†ËÅ
öÖaîŠ}F³3Ü¶hôC>TmñÊ, `õÂ,©VÅ,‘À.ê
g»Œ2À´øsßtxYÎZÓ‡O[¶:nH9IvŒ
AÚ4¾2àHiÅq×ë~êÛI¨ÃKuÙZäÒw[oÀûc
<wYŸî¦¹ÓCÎä(ë»

Encryption time: 0.16462445259094238 seconds

Theories about learning with multimedia can be positioned at different levels. At a basic level, psychological theories describe memory systems and cognitive processes that explain how people process different types of information and how they learn with different senses.

Decryption time: 0.15554237365722656 seconds

True
False

Plaintext 3.2.1

6J3þX
Ò6Å3E
-?·ÜI0d+(8°£aÙL_1íÝ†þQz„PîãÐ½û

```
          ®™h“Nµ
½“¹$ò‡¨4¨-9ûŸÖë!çy«W@]ªú‡Ã=ë[*Mò
PL½ûÜ!tÛŸµd:ƒ§ w°d¦LÙÓî
xd›ƒô°Ý†ÕÞ*V.ÔÆ:ì¤<6.…..%a{ýJRÏ=ò
BŠz‡Qõ?Œ@¾v+ñð
îñ#\ÖÄ±æJb'Éc:´!, W¸ái0õœ
Ôy¥ItiWÄÐ5Z³ë¦n£_Å0õp„ÖEút[4’¾VÁ
Øèä@Íƒ ÛüFýÊvÐqÕb×nëßÿÎ¹ËËÝ$ahéÚ
{=¼\ËþU3v%×µá0<, yÐrÀ’}
…ÆG

Encryption time: 0.17510175704956055
seconds

if saying "I won't let you run away," this
made Amane feel a little shy,
and then he put his hands behind Maui
and hugged her back.
I won't run...
I want to treat her well, I want her to be
happy, I want to love her. These
thoughts flew through Amane's mind as
he embraced her.
"I wish for Mahiru to be happy.

Decryption time: 0.1814267635345459
seconds

True
False
```

Plaintext 3.2.2

```
44õ{‰EŸ²?ürÍÍ´…îÐ- [ó¦Mé§Z¤¦æC]fšoöl
o :Uó®%V  mÞYPó€
"_Ó—ÿSöd

Encryption time: 0.18555164337158203
seconds

if saying "I won't let you run away," this
made Amane feel a little shy,
and then he put his hands behind Maui
and hugged her back.
I won't run...
I want to treat her well, I want her to be
happy, I want to love her. These
thoughts flew through Amane's mind as
he embraced her.
"I wish for Mahiru to be happy.
Decryption time: 0.18685221672058105
seconds

True
False
```

Melalui pengujian diatas, dapat dibilang eksekusi algoritma DAWASCrypt pada operasi enciphering dan deciphering cukup cepat, namun ada beberapa kasus dimana terjadi lonjakan atas waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi.

- *Avalanche Effect*

  Dari pengujian di atas, dapat dilihat bahwa perubahan satu karakter untuk key mengakibatkan hasil ciphertext yang sangat berbeda. Sebagai uji tambahan, kami mencoba melakukan enciphering plaintext 2 dengan kunci 2.1, dan melakukan deciphering dengan kunci 2.2 untuk menguji efeknya pada plaintext hasil deciphering. Hasil yang didapat adalah sebagai berikut:

```
zAñá!áaÈ¿JáÎÍÂôuC@‹ >K]ŠÃÞ,eœÑ‰c·Vå+çfæ-3
øq ]n^áw;Š^ê=ïËo[ÀrÍÅaF*½^chæqýAGÎ³è¡ááÈúÊ
[ä‰Ë]š¾…[x×
&öN-»ñ€þ
Šé‰zñwòonÐïƒ²±ÑáÂ8ŒoÏeÏŸh£V˜¸«YêI»þø°¨2|
#‰[‡7j“iyrúxAó“Õ¡¿¢'z_îØðn“&4Ï+U™ªÄiv”Hç§¹
á÷øÇåTÈa×cî†?¤ÏD0xÐ_- )ÑÛ1]ÃCZŒ
```

Dapat dilihat bahwa dengan mengganti 1 karakter pada kunci dapat mengakibatkan perubahan drastis pada plaintext hasil *deciphering*.

Jika plaintext 2 ditambahkan karakter ‘.’ di belakangnya, dienkripsi dengan kunci 2.2, dan menggunakan mode counter akan menghasilkan ciphertext:

```
8ªÍUG Sùl
Ã0ü‡ÞÜ\n, f.DvÑ?&dŒÇŸámÈ8,Ék‰³/Rª  ˜´hË€Ï
"ó{FNbÿH“Qãs- FÉ(yAê]è*]‡òÀ
```

Bandingkan dengan ciphertext untuk plaintext 2.2.2:

```
P%›ù—2Ó¥]N-O¨MÙûwäÉ=uòÃ„WL Î§¬
n&K€Ó[v&© ÑÏðå‹ Á^…¢Þ°s°{a"¬£~$siXZ£UðÙ·×
·~r¬_.à4ä8.- ØLp,÷ó)ÅÙI÷œgç‡Íý˜˜¼â^·‰âC5IIÝ.“e&ÑüR
âwd¿V´7Ió¿¢[˜ååªö6ð— ,MŒCQŸƒ[ðéÏ~Åv6U
{G“üÛ¿$`4›áY—>SÎÓÛeG)§Ä|"†º,          ¬
```

Dapat dilihat bahwa dengan mengganti 1 karakter pada plaintext awal dapat menghasilkan ciphertext yang sangat berbeda meski menggunakan kunci dan mode operasi yang sama. Dengan begitu, DAWASCrypt dapat menyembunyikan hubungan plaintext, ciphertext, dan kunci dengan baik.

- Analisis Ruang Kunci & Keamanan Lainnya

  Kunci internal yang dibangkitkan sebesar 128-bit, sehingga memiliki sekitar 2^{128} kombinasi untuk kunci internal. Dengan begitu, apabila diserang dengan metode *brute-force* sekalipun, waktu yang dibutuhkan untuk mencoba semua kemungkinan akan

sangat lama. Menurut kami, DAWASCrypt aman digunakan.

V. Kesimpulan dan Saran

Dari hasil pengujian yang telah dilakukan pada bagian 4, algoritma ini sudah dapat memiliki *avalanche effect* yang sangat besar pada semua mode yang ada, dimana perubahan sebuah karakter pada plainteks atau kunci memiliki dampak yang sangat besar dan bahkan dapat mempengaruhi blok lain serta karakter yang ada sebelum karakter yang diganti.

Sementara itu, dalam pengujian terhadap waktu enkripsi dan dekripsi, algoritma ini mampu melakukan enkripsi dan dekripsi dalam waktu yang cukup singkat, dimana waktu berkisar di antara 1.5 detik hingga 2 detik, namun dalam beberapa kasus kami menemukan adanya lonjakan waktu yang dibutuhkan untuk melakukan enkripsi atau dekripsi sehingga mengakibatkan diperlukannya waktu sebanyak kurang lebih 2 kali lipat dibanding waktu normal, penyebab dari pertambahan waktu ini belum kami ketahui dan terkesan terjadi secara acak. Waktu yang dibutuhkan juga tidak berubah jauh meskipun mode yang digunakan berbeda.

Untuk kunci yang digunakan di dalam algoritma ini memiliki ukuran yang sangat besar, sehingga dapat dibilang aman.

Saran pengembangan untuk kedepannya mungkin bisa dengan memperumit algoritma untuk pembuatan sbox, agar efek diffusion serta confusion semakin baik. Selain itu, dapat juga menggunakan algoritma pembangkit kunci internal yang lebih panjang dan rumit untuk membuatnya semakin mustahil untuk di-*bruteforce.*

Link Program

https://colab.research.google.com/drive/1e2olMPYvNGDg--n2w81IkNz_bYtrVO5u?usp=sharing

Referensi

[1] National Bureau of Standards, U.S. (1977). Data Encryption Standard~ Federal Information Processing Standard (FIPS), Publication 46, Department of Commerce, Washington D.C.

[2] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography.

[3] E. Biham, A. Shamir. (1993). Differential Cryptanalysis of the Data Encryption Standard. Springer Verlag, New York

[4] Munir, Rinaldi. (2023). “Slide Mata Kuliah Kriptografi”. Bandung: Teknik Informatika.

[5] Kazlauskas, Kazys & Kazlauskas, Jaunius. (2009). Key-Dependent S-Box Generation in AES Block Cipher System. Informatica, Lith. Acad. Sci.. 20. 23-34. 10.15388/Informatica.2009.235.