Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)
SAINTEKS 2020
ISBN: 978-602-52720-7-3
Februari 2020
Hal 409-414

Pengamanan File DOCX Menerapkan Algoritma *Simplified Data Encryption Standart* (DES)

Kristina Pakpahan, Surtini Samosir, Joni Alpensius Simatupang

Program Studi Teknik Informatika, STMIK Budi Darma, Medan Indonesia
Email: [1]Kristina.pakpahan1357@gmail.com, [1]Surtinisamosir@gmail.com, [1]JoniAlpen@gmail.com

Abstrak−Pengamanan suatu data maupun informasi sangat penting. Sering terjadi data maupun informasi tidak sampai kepada penerima atau pihak lain yang ingin melakukan penggandaan atau pemalsuan. Aplikasi pengamanan data sangat penting untuk menghindari orang lain yang tidak berhak mengakses data atau informasi kita. Untuk menghindari hal tersebut, maka penulis bermaksud mengamankan suatu data dengan mengenkripsi plainteks menjadi cipherteks. Data yang akan dienskripsikan disini adalah file DOCX. Salah satu metode yang dapat mengamankan file DOCX yaitu menggunakan metode algoritma kriptografi simplified DES (*Data Encryption Standard*) atau sering disebut simple DES. Algoritma ini digunakan untuk melakukan enskripsi data sehingga data asli hanya bisa dibaca seseorang yang mempunyai kunci enkripsi tersebut.

Kata Kunci: Kriptografi, DOCX, Simplified DES, Enkripsi

1. PENDAHULUAN

Kemajuan teknologi sekarang berkembang cepat, seperti penggunaan komputer dalam kegiatan sehari-hari, baik dalam pendidikan dan dunia kerja. Banyak jenis *software* yang ada pada komputer, salah satunya adalah Microsoft office word. Format penyimpanan file dokumen yang ada pada Microsoft office word versi 2007 dan diatasnya adalah DOCX [1]. Manusia sangat membutuhkan teknologi sekarang ini baik personal atau bahkan organisasi. Setiap Organisasi membutuhkan komputerisasi untuk menjalankan setiap aktivitasnya. Dari maraknya penggunaan komputer itu, maka dibuatlah sebuah pengamanan setiap aset-aset, terutama file DOCX berbentuk rahasia atau hanya boleh diketahui si pemilik. Demi keamanan file DOCX tersebut, muncul tuntutan untuk adanya suatu system pengamanan untuk menjaga file DOCX agar lebih aman, dan tidak di gunakan oleh orang-orang yang ingin merusak atau menyalahgunakan.

Terdapat beberapa cara untuk mengamankan file DOCX, yakni teknik penyamaran (kriptografi), dan teknk penyembunyian (steganografi). Pada kriptografi, file DOCX yang dikirimkan akan disamarkan sedemikian rupa, hingga orang lain tidak akan mengerti apa isi file DOCX tersebut.

Pada kriptografi, terdapat 2 konsep utama yakni dekripsi dan enkripsi. Enkripsi adalah suatu teknik mengubah bentuk data yang akan dikirim sehingga sulit dipahami [2]. Dekripsi adalah mengubah kembali data yang disamarkan sebelumnya ke data asli. Data yang masih asli dan belum disandikan dinamakan *plaintext.* Sedangkan setelah data disamarkan dengan katasandi *plaintext* ini disebut dengan *chipertext* [3]. Proses pengamanan file DOCX dilakukan dengan cara mengenpriksikan isi file DOCX menggunakan metode algoritma yang bisa menjaga keamanan tanpa diketahui pihak asing. Salah satu metode algoritma nya adalah simplified DES (*Data Encryption Standard*). Alasan penulis memilih simplified DES (*Data Encryption Standard*) dalam menjaga keamanan file DOCX, dikarenakan simplified DES merupakan hasil sederhana dari DES dan perhitungan nya lebih mudah dan singkat.

Algoritma simplified DES (*Data Encryption Standard*) mempunyai panjang kunci 10 bit, *chipertext* 8bit, *plaintext* 8 bit, perputaran kuncinya menghasilkan pergeseran kiri. Dalam algoritma simplified DES, dekripsi dan ekripsi sama, hanya urutan dalam memasukkan round key dibalikkan. Algoritma ini memiakai lima fungsi, yakni Operasi Expand(permutasi), subsitusi, dan xor, Switch (SW) Initial Permutation (IP), dan Inver initial Permutation (IP^{-1}).

Berdasarkan uraian yang sudah dijelaskan diatas, penulis melakukan penelitian lebih jauh lagi dengan mengangkat judul dengan menerapkan metode kriptografi simplified DES (*Data Encryption Standard*) yaitu "Pengamanan File DOCX menerapkan simplified DES (*Data Encryption Standard*)".

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi merupakan suatu metode pengamanan untuk melindungi data maupun informasi dengan penyandian yang hanya bisa diketahui orang yang berhak mengakses data atau informasi tersebut. Sebenarnya, metode algoritma yang paling sering digunakan dalam melindungi berbagai jenis data atau informasi sering disebut dengn *encryption,* yaitu proses pengkonversian sebuah pesan *plaintext* menjadi *chipertext* yang bisa dikembalikan ke bentuk asli disebut juga dengan *decoding* (*decryption*) [1].

Dalam artikel ini, enkripsi yang diterapkan terhadap suatu file DOCX dengan mengganti bentuknya menjadi tida dikenali. Setiap file DOCX yang dienkripsian mempunyai kunci saat proses penyandian. Kemudian file DOCX tersebut dapat dikembalikan atau didekripsikan seperti semula dengan kunci yang dimiliki setiap file DOCX yang dapat membuka system penyandian enkripsi, agar keamanan file DOCX dapat terjaga dengan baik tanpa harus diketahui pihak yang tidak berwenang [2].

2.2 Algoritma *Simplified Data Encryption Standart*

Data Encryption Standard (DES) adalah sebuah algoritma kunci simetri yang dirancang IBM pada tahun 1970. Karena saat ini DES dianggap kurang aman dan sudah jarang digunakan, namun dalam belajar kriptografi, algoritma ini masih digunakan.

ISBN: 978-602-52720-7-3
Februari 2020
Hal 409-414

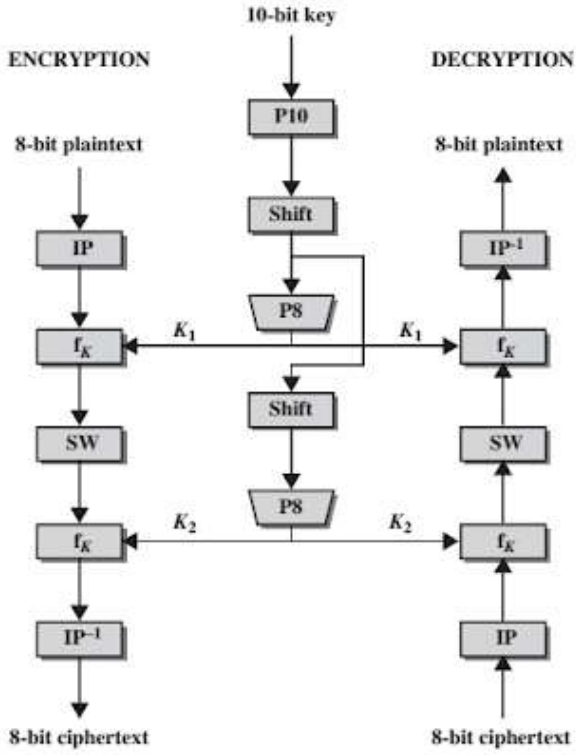
Ini terjadi karena setelahnya banyak algoritma kunci dikembangkan dan didesain berdasarkan prinsip yang digunakan pada DES. *Simplified* DES (SDES) diperkenalkan oleh Schaefer, sebagai pembelajaran algoritma DES bagi mahasiswa yang memilih mata kuliah kriptologi. *Simplified* DES memiliki struktur yang sama dengan DES, namun simplified DES sudah disederhanakan sehingga pehitungan enkripsi dan dekripsinya lebih mudah untuk diselesaikan [3].

Tabel 1. Perbedaan parameter DES dan *Simplified* DES

Karakteristik	DES	SDES
Panjang kunci	64 bit	10 bit
Panjang blok	64 bit	8 bit
Panjang knci internal	56 bit	8 bit
Jumlah matriks subsitusi	8 buah	2 buah
Jumlah putaran	16 putaran	2 putaran
Jumlah kunci internal	16 buah	2 buah
Ukuran matriks substitusi	4 x 16	4 x 4

Pada proses enkripsi, *Simplified* DES mendapatkan blok *plaintext* yang ukuran 8bit dan kunci 10bit untuk menghasilkan blok *ciphertext* yang ukurannya 8 bit. Sebaliknya proses dekripsi mendapatkan blok *ciphertext* yang ukurannya 8bit dan kunci 10bit untuk menghasilkan blok *plaintext* yang ukuranya 8 bit. Algoritma enkripsi maupun dekripsi pada *Simplified* DES terdapat lima fungsi dan dioperasikan secara berurut [4]:

1. Permutasi awal (*initial permutation*-IP)
2. Fungsi f_K berisi operasi permutasi dan substitusi,
3. Fungsi permutasi sederhana (*switches*-SW)
4. Fungsi f_K
5. Fungsi permutasi (IP^{-1}) yang merupakan invers dari *initial permutation*.



Gambar 1. Proses enkripsi, dekripsi dan pembangkitan kunci *Simplified* DES [4].

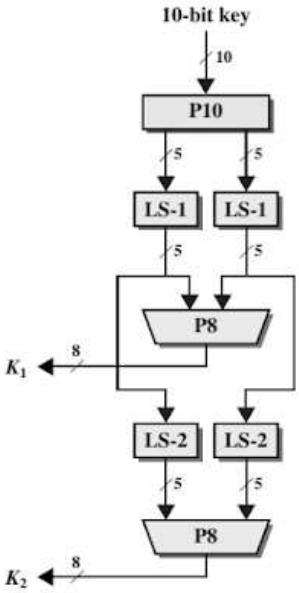
2.2.1 Proses Pembangkitan Kunci Internal

Pada *Simplified* DES proses pembangkitan kunci internal dilakukan dengan langkah-langkah berikut ini:

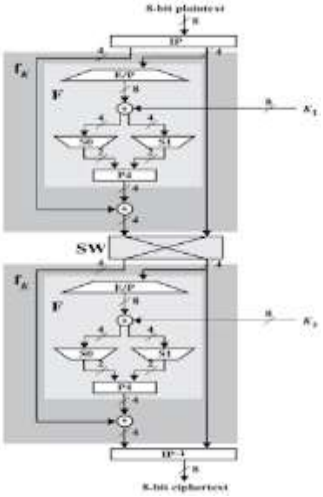
1. Masukan proses sebanyak 10bit kunci eksternal.
2. Proses permutasi P10 diterapkan pada 10bit kunci. Permutasi ini dilakukan dengan menukar posisi bit kunci eksternal. Secara matematis dapat ditulis dengan persamaan dibawah:
   $P10 = (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}) = (k_3, k_5, k_2, k_7, k_4, k_{10}, k_1, k_9, k_8, k_6)$
3. Kemudian bit-bit kunci eksternal dibagi menjadi 2 bagian, 5bit bagian kiri dan 5bit bagian kanan.
4. Setiap bagian digeser secara berurutan sejauh 1bit kesebelah kiri (*left shift*).
5. Hasil pergeseran pada langkah 4 digabungkan, lalu dikenakan proses permutasi P8. Prosespermutasi ini menerima 10 bit masukan, mendapatkan 8 bit keluaran disebut kunci internal (K_1). Secara matematis dapat ditulis dengan :
   $P8 = (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}) = (k_6, k_3, k_7, k_4, k_8, k_5, k_{10}, k_9)$
6. Hasil langkah 3 dilakukan pergeseran secara berurutan sebanyak 2bit ke sebelah kiri.

ISBN: 978-602-52720-7-3
Februari 2020
Hal 409-414

7. Hasil pergeseran dari langkah 6 digabungkan, lalu dikenakan proses permutasi P8. Proses permutasi ini menerima sebanyak 10 bit masukan dan menghasilkan sebanyak 8 bit keluaran kunci internal (K_2).



Gambar 2. Rinci roses pembangkitan kunci [2].



Gambar 3. Rinci proses enkripsi [2].

2.2.2 Proses Enkripsi

Pada *Simplified*DES dilakukan dengan dua putaran. Langkah-langkah proses enkripsi, yaitu [5] :

1. Masukan 8bit *plaintext* yan dikenakan proses *initial permutation* (IP). Secara matematis dapat ditulis kedalam persamaan:
   $IP = (p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8) = (p_2, p_6, p_3, p_1, p_4, p_8, p_5)$
2. Hasil permutasi langkah 1 dibagi menjadi dua bagian, 4bit bagian sebelah kiri (*Left*) dan 4bit bagian sebelah kanan (*Right*).
3. Ekspansi/permutasi (E/P) yang dikenakan pada 4bit bagian kanan. Kemudian hasilnya akan menerima 4bit masukan dan menghasilkan 8bit keluaran. Secara natenatis, dapat ditulis ke persamaan:
   $E/P = (pr_1, pr_2, pr_3, pr_4) = (pr_4, pr_1, pr_2, pr_3, pr_2, pr_3, pr_4, pr_1)$
4. Pada putaran pertama, hasil operasi ekspansi/permutasi (E/P) yang dikenakan operasi XOR pada kunci internal K_1.
5. Hasil operasi XOR langkah diatas dibagi dalam dua bagian, 4bit bagian pertama dan 4bit bagian kedua.
6. Setiap bagian dipakai operasi substitusi melalui kotak S-box, dimana 4bit bagian pertama akan disubstitusi pada S0 dan 4bit bagian kedua disubstitusi pada S1. S-box menerima 4bit masukan dan menghasilkan 2bit keluaran.

ISBN: 978-602-52720-7-3
Februari 2020
Hal 409-414

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

7. Bit yang pertama dan bit yang keempat dari 4bit masukan menjelaskan nomor baris S-box. Sedangkan bit kedua dan bit ketiga menjelaskna nomor kolom S-box. Posisi matriks merupakan perpotongan antara nomor baris dan kolom tersebut merupakan hasil keluaran dari S-box.
8. Kemudian hasil operasi dari S-box digabung kembali 2bit dari S0 dan 2bit dari S1, kemudian dikenakan oleh operasi permutasi P4. Operasi permutasinya dapat ditulis dengan:
   $P_4 = (p_1, p_2, p_3, p_4) = (p_2, p_4, p_3, p_1)$
9. Hasil operasi pada langkah diatas, dimana operasi XOR dengan 4bit bagian kiri dari langkah 2
10. Hasil operasi pada langkah diatas digabung kembali dengan 4bit bagian langkah 2.
11. Kemudian, dilakukan operasi *switch* (SW), dimana posisi-posisi bit dilakukan penukaran dari langkah 10. Posisi 4 bit bagian kiri akan dilakukan penukaran juga dengan posisi 4 bit bagian kanan.Secara matematis dapat ditulis dengan :
    $SW = (P_{L1}, P_{L2}, P_{L3}, P_{L4}, P_{R1}, P_{R2}, P_{R3}, P_{R4}) = (P_{R1}, P_{R2}, P_{R3}, P_{R4}, P_{L1}, P_{L2}, P_{L3}, P_{L4})$
12. Hasil operasi pada langkah diatas adalah masukan putaran kedua.
13. Proses di putaran kedua kembali diulang langkah 3 sampai langkah 10, kecuali pada langkah 4, K_2 adalah kunci internal yang digunakan.
14. Langkah terakhir yaitu operasi permutasi IP^{-1} dimana mengikuti persamaan dibawah ini :
    $IP^{-1} = (p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8) = (p_4, p_1, p_3, p_5, p_7, p_2, p_8, p_6)$
15. Hasil operasi pada langkah 14 merupakan blok *chipertext* 8 bit.

2.2.3 Proses Dekripsi

Proses dekripsi *Simplified* DES dijalankan dengan urutan yang sama contohnya pada proses enkripsi. Perbedaannya ada pada urutan kunci internal yang digunakan. Pada proses enkripsi, kunci internal K_1 digunakan untuk putaran pertama, sedangkan K_2 digunakan untuk putaran kedua. Sedangkan pada proses dekripsi, putaran pertama yang digunakan adalah kunci K_2, dan putaran keduayang digunakan adalah kunci K_1 [5].

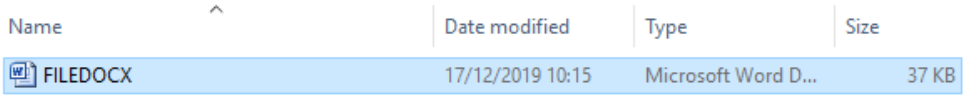
3. ANALISA DAN PEMBAHASAN

Keamanan suatu data merupakan salah satu hal yang sangat penting dalam kemajuan teknologi sekarang ini. Perkembangan teknologi zaman sekarang ini menimbulkan ide-ide dan teknik baru, bahkan tidak sedikit yang menyalah gunakan sehingga mengancam dan merugikan pemilik informasi. Secara umum, data dibagi menjadi dua, yakni data yang bersifat tidak rahasia dan data bersifat rahasia. Data yang sifatnya tidak rahasia, biasanya tidak terlalu penting dan dijaga. Sebaliknya data yang sifatnya rahasia yang isinya hanya diketahui oleh pihak pemilik data dan tidak boleh diketahui oleh pihaklain. Untuk mengatasi keamanan suatu data yang bersifat rahasia ini maka teknik kriptografi penguncian bisa digunakan.

Adapun Algoritma yang digunakan dalam pengamanan file DOCX pada artikel ini adalah Algoritma *Simplified* DES (*Data Encryption Standard)*. Pada proses enkripsi, *Simplified* DES mendapatkan blok *plaintext* yang ukuran 8bit dan kunci 10bit untuk menghasilkan blok *ciphertext* yang ukurannya 8 bit. Sebaliknya proses dekripsi mendapatkan blok *ciphertext* yang ukurannya 8bit dan kunci 10bit untuk menghasilkan blok *plaintext* yang ukuranya 8bit.

Untuk mengamankan file DOCX maka diperlukannya analisa terhadap file DOCX yang akan diamankan, agar dalam proses pengamanan file DOCX bisa diselesaikan. Adapun analisa terhadap file DOCX yang akan diamankanyaitu:

1. Memilih file DOCX yang akan diamankan, dalam hal ini *plainteks* file DOCX dapat dilihat pada gambar 4.



Gambar 4. *Plaintext* file DOCX

Selanjutnya dilakukan ekstraksi pada file DOCX yang akan diamankan tersebut guna mengetahui kunci yang terdapat pada file DOCX yang akan diamankan tersebut.

2.3 Analisa Algoritma *Simplified* DES

Kunci: 50, 4b, 6e, 20, a2, 28, a0, 54, 70, 65
Biner: 1010000 1001011 1101110 100000 10100010 101000 10100000 1010100 1110000 1100101

Kunci inilah yang disandikan guna untuk mengamankan file DOCX tersebut dengan menggunakan algoritma *Simplified* DES. Selanjutnya adalah melakukan proses permutasi P10 diterapkan pada 10bit kunci. Permutasi ini dilakukan dengan menukar posisi bit kunci eksternal.
Input: 1010000 1001011 1101110 100000 10100010 101000 10100000 1010100 1110000 1100101

ISBN: 978-602-52720-7-3
Februari 2020
Hal 409-414

Output: 1101110 10100010 1001011 10100000 100000 1100101 1010000 1110000 101000

Kemudian hasil permutasi langkah 1 dibagi menjadi dua bagian, 4bit bagian sebelah kiri (*Left*) dan 4bit bagian sebelah kanan (*Right*).
Input: 1010000 1001011 1101110 100000
Output: 1001011 1101110 100000 1010000

Hasil pergeseran pada langkah diatas digabungkan, lalu dikenakan proses permutasi P8. Proses permutasi ini menerima 10 bit masukan, mendapatkan 8 bit keluaran disebut kunci internal (K_1).
Input: 1010000 1001011 1101110 100000 10100010 101000 10100000 1010100 1110000 1100101
Output: 101000 1101110 10100000 100000 1010100 10100010 1100101 1110000

Kemudian hasil pergeseran dari langkah diatas digabungkan, lalu dikenakan proses permutasi P8. Proses permutasi ini menerima sebanyak 10 bit masukan dan menghasilkan sebanyak 8 bit keluaran kunci internal (K_2).
Input: 101000 1101110 10100000 100000 1010100
Output: 10100000 100000 1010100 101000 1101110

2.3.1 Proses Enkripsi

Pada *Simplified* DES dilakukan dengan dua putaran. Langkah-langkah proses enkripsi, yaitu:
Putaran 1:
Input: 101000 1101110 10100000 100000 1010100 10100010 1100101 1110000
Output: 1101110 10100010 10100000 1010100 101000 100000 1110000 1100101
Putaran 2:
Input: 101000 1101110 10100000 100000
Output: 100000 101000 1101110 10100000 10100000 10100000 100000 101000

Selanjutnya, pada putaran pertama, hasil operasi ekspansi/permutasi (E/P) yang dikenakan operasi XOR pada kunci internal K_1.

```
1101110 10100010 10100000 1010100   101000   100000  1110000  1100101
 101000  1101110 10100000  100000  1010100 10100010  1100101  1110000 ⊕
-------------------------------------------------------------------------
1111110 00110000          01000101 01000111  0100000 10001010 10010101
```

Setiap bagian dipakai operasi substitusi melalui kotak S-box, dimana 4bit bagian pertama akan disubstitusi pada S0 dan 4bit bagian kedua disubstitusi pada S1. S-box menerima 4bit masukan dan menghasilkan 2bit keluaran.

```
S0 = 11111100 [ 01000101 01000111 10100000 10001010 ]
     00110000 [ 00110000 11111100 01000101 01000101 ]
     01000101 [ 01000101 01000101 00110000 11111100 ]
     01000101 [ 10101000 10100010 11001011 01110000 ]
              [ 01000101 00110000 01000101 00110000 ]

S1 = 10100000 [ 11111100 00110000 01000101 01000101 ]
     11001010 [ 00110000 11111100 01000101 01000101 ]
     01000101 [ 11111100 01000101 11111100 01000101 ]
     01100101 [ 01000101 01000111 10100000 10001010 ]
              [ 01000101 00110000 01000101 00110000 ]
```

Bit yang pertama dan bit yang keempat dari 4bit masukan menjelaskan nomor baris S-box. Sedangkan bit kedua dan bit ketiga menjelaskna nomor kolom S-box. Posisi matriks merupakan perpotongan antara nomor baris dan kolom tersebut merupakan hasil keluaran dari S-box. Kemudian hasil operasi dari S-box digabung kembali 2bit dari S0 dan 2bit dari S1, kemudian dikenakan oleh operasi permutasi P4. Operasi permutasinya dapat ditulis dengan:
input: 11111100 01000101 11111100 01000101
output: 01000101 01000101 11111100 11111100

Hasil operasi pada langkah diatas digabung kembali dengan 4bit bagian langkah 2. Kemudian, dilakukan operasi *switch* (SW), dimana posisi-posisi bit dilakukan penukaran dari langkah diatas. Posisi 4 bit bagian kiri akan dilakukan penukaran juga dengan posisi 4 bit bagian kanan.Secara matematis dapat ditulis dengan :
Input: 11111100 01000101 11111100 01000101 01000101 01000101 11111100 11111100
Output: 01000101 01000101 11111100 11111100 11111100 01000101 11111100 01000101

Hasil operasi pada langkah diatas adalah masukan putaran kedua. Yang terakhir yaitu operasi permutasi IP^{-1}:
Input: 11111100 01000101 11111100 01000101 01000101 01000101 11111100 11111100
Output: 01000101 01000101 01000101 11111100 11111100 01000101 11111100 01000101

2.3.2 Proses Dekripsi

Proses dekripsi *Simplified* DES dijalankan dengan urutan yang sama contohnya pada proses enkripsi. Perbedaannya ada pada urutan kunci internal yang digunakan. Pada proses enkripsi, kunci internal K_1 digunakan untuk putaran pertama, sedangkan K_2 digunakan untuk putaran kedua. Sedangkan pada proses dekripsi, putaran pertama yang digunakan adalah kunci K_2, dan putaran keduayang digunakan adalah kunci K_1.

ISBN: 978-602-52720-7-3
Februari 2020
Hal 409-414

Putaran 1:
Input: 1101110 10100010 10100000 1010100 101000 100000 1110000 1100101
Output: 101000 1101110 10100000 100000 1010100 10100010 1100101 1110000
Putaran 2:
Input: 101000 1101110 10100000 100000
Outpu: 100000 101000 1101110 10100000 10100000 10100000 100000 101000

Selanjutnya, pada putaran pertama, hasil operasi ekspansi/permutasi (E/P) yang dikenakan operasi XOR pada kunci internal K_2.

$$\begin{array}{r} 101110\ 10100010\ \ 10100000\ \ 1010100\ \ 101000\ \ 100000\ 1110000\ \ 1100101 \\ 1111110\ 00110000\ \ 01000101\ 01000111\ 10100000\ 10001010\ 10010101010\ \oplus \\ \hline 1010000\ 1001011\ 1101110\ 100000\ 10100010\ 101000\ 10100000\ 1010100\ 1110000 \end{array}$$

Hasil Dekripsinya adalah:
Biner: 1010000 1001011 1101110 100000 10100010 101000 10100000 1010100 1110000 1100101
Heksadesimal: 50, 4b, 6e, 20, a2, 28, a0, 54, 70, 65

3 KESIMPULAN

Simplified DES (SDES) adalah salah satu algoritma penyandian dan sudah disederhanakan sehingga pehitungan enkripsi dan dekripsinya lebih mudah untuk diselesaikan. Pada proses enkripsi, *Simplified* DES mendapatkan blok *plaintext* yang ukuran 8bit dan kunci 10bit untuk menghasilkan blok *ciphertext* yang ukurannya 8bit. Sebaliknya proses dekripsi mendapatkan blok *ciphertext* yang ukurannya 8bit dan kunci 10bit untuk menghasilkan blok *plaintext* yang ukuranya 8bit.

REFERENCES

[1] Y. Maryono dan B. P. Istana, Teknologi informasi dan komunikasi, Jakarta: Yudhistira, 2007.
[2] A. A. M. Khalaf, M. S. A. El-Karim dan H. F. A. Hamed, "Proposed Triple Hill Cipher Algorithm for Increasing the Security Level of Encrypted Binary Data and Its Implementation Using FPGA," dalam International Conference on Advanced Communications Technology (ICACT 2015), Phoenix Park, PyeongChang, South Korea, 2015.
[3] N. C dan R. , "Advanced Rail Cipher Algorithm," International Journal of Pharmacy and Technology, vol. VIII, no. 3, pp. 16539-16545, 2016.
[4] H. Kurniadi, Pengantar Ilmu Kriptografi, Bandung: Informatika Bandung, 2015.
[5] S. Kromodimoeljo, Teori dan Aplikasi Kriptografi, Bandung: SPK IT Consulting, 2010.
[6] R. Sadikin, Kriptografi Untuk Keamanan Jaringan, Yogyakarta: Andi Offset, 2012.
[7] R. Munir, Kriptografi, Bandung: Informatika Bandung, 2006.
[8] Y. Kurniawan, Kriptografi Keamanan Internet dan Jaringan Komunikasi, Bandung: Informatika, 2017.
[9] N. Kaur dan R. Mahajan, "An Improved Scheme of Embedded Extended Visual Cryptography," International Journal of Computer Engineering & Science (IJCES), vol. IV, no. 2, pp. 69-73, 2014.
[10] N. K. Pareek, "Design and Analysis of a Novel Digital Image Encryption Shceme," International Journal of Network Security and Its Application (IJNSA), vol. II, no. 4, pp. 93-108, 2012.