Informatyka, studia dzienne semestr III
Podstawy kryptografii **2018/2019**
Prowadzący: prof. dr hab. Volodymyr Yemyets piątek, 8:30

Data oddania: _____ Ocena: _____

Bartłomiej Jencz 216783
Sylwester Dąbrowski 216743

Zadanie 1: DES (Data Encryption Standard)

Streszczenie

Celem zadania jest przygotowanie zestawu narzędzi do generowania kluczy, szyfrowania wiadomości za pomocą klucza i odczytywania szyfrogramów za pomocą klucza w oparciu o algorytm DES

1. Wstęp

DES powstał w latach siedemdziesiątych i został przyjęty jako standard szyfrowania przez Amerykański Narodowy Instytut Standaryzacji (ang. American National Standards Institute – ANSI) 23 listopada 1976 roku

DES jest szyfrem blokowym, pracującym na 64-bitowych pakietach danych. Zarówno do szyfrowania, jak i deszyfrowania stosuje się ten sam algorytm. Klucz jest 64-bitowy, przy czym informacja użyteczna zajmuje 56 bitów (co ósmy bit w ciągu klucza jest bitem parzystości). Całe bezpieczeństwo spoczywa właśnie na nim. Algorytm DES to kombinacja dwu podstawowych technik: mieszania i rozpraszania.

Aktualnie standard DES nie jest już uważany za dostatecznie silny mechanizm kryptograficzny dla większości zastosowań, jednak wciąż jest bardzo często demonstrowany jako bardzo reprezentatywny przykład algorytmu symetrycznego szyfrowania

2. Implementacja

Nasz algorytm działa w trybie ECB (wyjaśnienie poniżej)

Algorytm szyfrowania danych jest następujący: na początku tekst jawny, który ma zostać zaszyfrowany , dzielony jest na bloki 64-bitowe. Następnie dla każdego bloku wykonywane są następujące operacje:

- dokonywana jest permutacja początkowa bloku przestawiająca bity w pewien określony sposób – nie zwiększa ona bezpieczeństwa algorytmu, a jej początkowym celem było ułatwienie wprowadzania danych do maszyn szyfrujących używanych w czasach powstania szyfru

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	5	37	29	21	13	5	63	55	47	39	31	23	15	7

Rysunek 1 - Permutacja początkowa IP

- blok wejściowy rozdzielany jest na dwie 32-bitowe części: lewą oraz prawą
- wykonywanych jest 16 cykli tych samych operacji, zwanych funkcjami Feistela, podczas których dane łączone są z kluczem (Ad1). Operacje te wyglądają następująco:
    - bity klucza są przesuwane, a następnie wybieranych jest 48 z 56 bitów klucza
    - prawa część danych rozszerzana jest do 48-bitów za pomocą permutacji rozszerzonej

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	12	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Rysunek 2 - Permutacja z rozszerzeniem

- rozszerzona prawa połowa jest sumowana modulo 2 z wybranymi wcześniej (i przesuniętymi) 48 bitami klucza
- zsumowane dane dzielone są na osiem 6-bitowych bloków i każdy blok podawany jest na wejście jednego z Sbloków (pierwszy 6-bitowy blok na wejście pierwszego S-bloku, drugi 6-bitowy blok na wejście drugiego S-bloku, itd.). Pierwszy i ostatni bit danych określa wiersz, a pozostałe bity kolumnę S-BOXa. Po wyznaczeniu miejsca w tabeli, odczytuje się wartość i zamienia na zapis dwójkowy. Wynikiem działania każdego S-bloku są 4 bity wyjściowe – tworzą one 32-bitowe wyjście S-bloków. Każdy S-Blok ma inną strukturę
- wyjście S-bloków poddawane jest permutacji w P-blokach

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Rysunek 3 - Permutacja P-bloku

- bity tak przekształconego bloku sumowane są z bitami lewej połowy danych
- tak zmieniony blok staje się nową prawą połową, poprzednia prawa połowa staje się natomiast lewą połową – cykl dobiega końca

- po wykonaniu 16 cykli operacji prawa i lewa połowa danych jest łączona w 64-bitowy blok
- dokonywana jest permutacja końcowa

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Rysunek 4 - Permutacja końcowa IP-1

Deszyfrowanie

Operacje deszyfrowania kryptogramu uzyskanego algorytmem DES są realizowane za pomocą tej samej sieci (sieci Feistela rys. 8) co operacje szyfrowania bloku tekstu

jawnego. Różnica polega jedynie na tym, iż klucze stosowane są w kolejności odwrotnej od K_{16} do K_1

Jak powstaje klucz (Ad1)?

Ponieważ klucz jest 64-bitowy, redukowany jest do klucza 56 bitów przez pominięcie co ósmego bitu parzystości. Tak przygotowany ciąg bitów poddawany jest permutacji wejściowej.

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Rysunek 5 - Permutacja klucza

Po czym dzielony jest na dwa podciągi 28-bitowe. Następnie połowy te przesuwane są w lewo o jeden lub dwa bity, zależnie od numeru cyklu.

NR ITERACJI I	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Liczb. Przes.	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

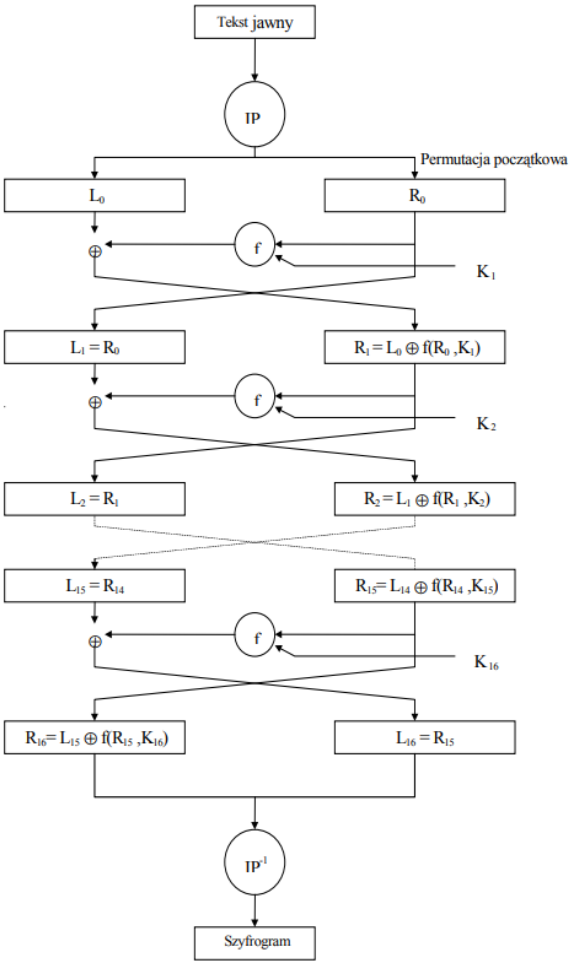
Rysunek 6 - Przesunięcia połówek klucza

Po połączeniu nowo powstałych ciągów wybiera się 48 z 56 bitów (permutacja z kompresją)

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Rysunek 7 - Permutacja z kompresją

Tak otrzymujemy klucz dla i-cyklu (gdzie i jest numerem cyklu), i = 1, ...,16.



Rysunek 2 - Schemat blokowy algorytmu DES

3. Dyskusja

Algorytm na pierwszy do zaimplementowania jest bardzo trudny. Dużą trudność sprawiło nam dobre zaimplementowanie algorytmu mianowicie kompresja SBoxów oraz alogrytm rund.

Nasz tryb działania jest dość trywialny w porównaniu np. do CBC

Z informacji znalezionych na stronie instytutu informatyki Politechniki Śląskiej dowiedzieliśmy się że DES jest algorytmem, który powstał z myślą o implementacjach sprzętowych Na początku jego istnienia układ zbudowany z 50 tysięcy tranzystorów, który zawierał zespół bramek realizujących tryby:

ECB (tryb elektronicznej książki kodowej (Electronic Codebook – ECB)

CBC (tryb wiązania bloków zaszyfrowanych (Cipher Block Chaining – CBC).

szyfrował i deszyfrował dane z szybkością 1 Gbit/s, co jest równoważne 15,6 milionom bloków na sekundę. Jest to imponująca liczba.

Implementacje programowe są znacznie wolniejsze i przegrywają w konkurencji z rozwiązaniami sprzętowymi (w tamtych czasach).

Odporność algorytmu

Algorytm DES aktualnie jest już nie używany w jego pierwotnej postaci między innymi przez odkrycie metody kryptoanalizy różnicowej oraz najzwyczajniej moc komputerów.

Jedną z wad algorytmu są również tak zwane klucze słabe tzn. że klucz użyty w jednym cyklu algorytmu będzie taki sam we wszystkich pozostałych, a co za tym idzie tekst jawny nie zostanie zaszyfrowany.

Pierwotny ciąg słabego klucza	Faktyczny ciąg klucza
0101 0101 0101 0101	0000000 0000000
FEFE FEFE FEFE FEFE	FFFFFFF FFFFFFF
1F1F 1F1F 1F1F 1F1F	0000000 FFFFFFF
E0E0 E0E0 F1F1 F1F1	FFFFFFF 0000000

Istnieją również pary kluczy, które szyfrują tekst jawny do jednakowych szyfrogramów. Innymi słowy, jeden klucz z pary może służyć do deszyfrowania wiadomości zaszyfrowanej drugim kluczem z tej pary. Zamiast generować 16 różnych podkluczy, generowane są dwa. Każdy z nich jest wykorzystywany 8 razy w algorytmie. Klucze takie nazywamy kluczami półsłabymi

01FE	01FE	01FE	01FE
1FE0	1FE0	0EF1	0EF1
01E0	01E0	01F1	01F1
1FFE	1FFE	0EFE	0EFE
011F	011F	010E	010E
E0FE	E0FE	F1FE	F1FE
FE01	FE01	FE01	FE01
E01F	E01F	F10E	F10E
E001	E001	F101	F101
FE1F	FE1F	FE0E	FE0E
1F01	1F01	0E01	0E01
FEE0	FEE0	FEF1	FEF1

Algorytm DES był przez wiele lat bezpieczny. Ze względu na złożoność obliczeniową kryptoanalizy, przy dostępnej mocy obliczeniowej, proces odnajdywania klucza metodą przeszukiwania wyczerpującego był wystarczająco nieefektywny, by uczynić ataki nieopłacalnymi. Jednak w 1998 r. algorytm DES z kluczem 56b został złamany w 56 godzin kryptoanalizy metodą przeszukiwania wyczerpującego. Koszt sprzętu (EFF DES Cracker) wówczas szacowano na 250 tys. USD. Rok później zajęło to już 22 godziny. Dziś to kwestia minut.

Spis literatury

[1] http://wazniak.mimuw.edu.pl/
[2] http://www.zo.aei.polsl.pl/