Szyfrowanie plików przy pomocy szyfrowania DES

(Data Encryption Standard)

Denis Wychowałek
sekcja 11
grupa GKiO 2

Założenia

- **GUI zrobione zostanie przy wykorzystaniu WinForms**
- **Przygotowanie danych do szyfrowania i deszyfrowania przygotowane zostaną w aplikacji napisanej w języku C#**
- **Dane do szyfrowania wczytywane będą w trybie binarnym**
- **Wszystkie dane zostaną podzielone na bloki gotowe do rozdziału pomiędzy wątki**
- **Przygotowanie klucza, szyfrowanie i deszyfrowanie danych wykonane będzie w asemblerze**
- **Do szyfrowania i odszyfrowania zostaną wykorzystane instrukcje wektorowe.**
- **Zwrócony zaszyfrowany lub odszyfrowany blok danych zostanie zapisany do pliku.**

Przygotowanie klucza – początkowa permutacja

• Klucz 64 bitowy jest permutowany według tablicy z następującymi wartościami.

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

Bity z początkowego klucza są umieszczane kolejno według powyżej tablicy tzn. pierwszym bitem nowego klucza jest 57 bitem klucza który został przekazany wcześniej.

Przygotowanie klucza – dzielenie, przesunięcia bitowe, finałowa permutacja

- **W następnej kolejności jest dzielony cały klucz na dwa podklucze o równej długości.**

- **Po podziale następuje szesnastokrotna iteracja w trakcie, której tworzonych jest 16 nowych kluczy.**

- **Podczas iteracji przesuwane są bity w lewo.**

Nr iteracji	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Przesunięcie o ile bitów	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

- **Wszystkie utworzone nowe klucze są poddawane ostatecznej permutacji według tabeli.**

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

Szyfrowanie

- **Tak samo jak w przypadku klucza na samym początku jest dokonywana wstępna permutacja.**

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	45	37	29	21	13	5
63	55	47	39	31	23	15	7

- **Następnie dane są dzielone na dwie równe części.**

- **Podzielone strony poddaje się szesnatokrotnej iteracji. Każda iteracja wygląda następująco:**

  $L_i = R_{i-1}$

  $R_i = L_{i-1} \text{ xor } f(R_{i-1}, K_i)$

Szyfrowanie - permutacja i xorowanie z kluczem

• Dokonywana jest permutacja, która ma na celu stworzenie z 32 bitowej strony 48 bitowy blok według tablicy.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
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

- **Następnie dane xoruje się z kluczem.**

- **Dane wdzielone są na osiem 6-bitowych bloków i każdy blok jest podawany nawejście jednego z S-bloków. Pierwszy i ostatni bit określa wiersz, a pozostałe kolumnę S-Boxa. Po wyzmaczeniu miejsca w tabeli odczytuje zawartość i jest zamieniany na zapis binarny. Wynikiem działania S-bloku są 4 bity wejściowe.**

Szyfrowanie - permutacja i xorowanie z lewą stroną

- **Dokonywana jest permutacja 4-bitowych bloków.**

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

- **Te dane w następnej kolejności są xorowane z lewą stroną.**

- **Wynik tej operacji staje się nową prawą stroną, natomiast lewą poprzedni blok prawy.**

- **Po wykonaniu 16 permutacji bloki są łączone w 64-bitowy blok.**

- **Na końcu wykonuje się ich permutację końcową.**

Szyfrowanie - permutacja końcowa i deszyfracja

- **Na koniec połączone dane są permutowane według poniższej tabeli.**

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

- **Procedura odszyfrowania danych jest podobna do szyfrowania, lecz wszystkie operacje wykonuje się w odwrotnej kolejności. Różnica polega na wyborze podkluczy.**

Dziękuję za uwagę