

Podstawy Kryptografii sem. V

Krzysztof Barden 210139
Przemysław Fortuna 210176
Kacper Hałaszczak 210197

ZADANIE 1 ZESTAW I

1. Wstęp

Celem zadania było napisanie programu szyfrującego/deszyfrującego dane wprowadzone przez użytkownika z wykorzystaniem algorytmu DES.

2. Opis algorytmu

Algorytm DES (Data Encryption Standard) – symetryczny szyfr blokowy zaprojektowany w 1975 przez IBM pracujący na 64-bitowych pakietach danych. Zarówno do szyfrowania jak i deszyfrowania stosuje się ten sam algorytm. Klucz jest 64-bitowy ale użyteczne informacje zajmują 56 bitów (pomija się co ósmy bit który jest bitem parzystości).

2.1 Działanie algorytmu

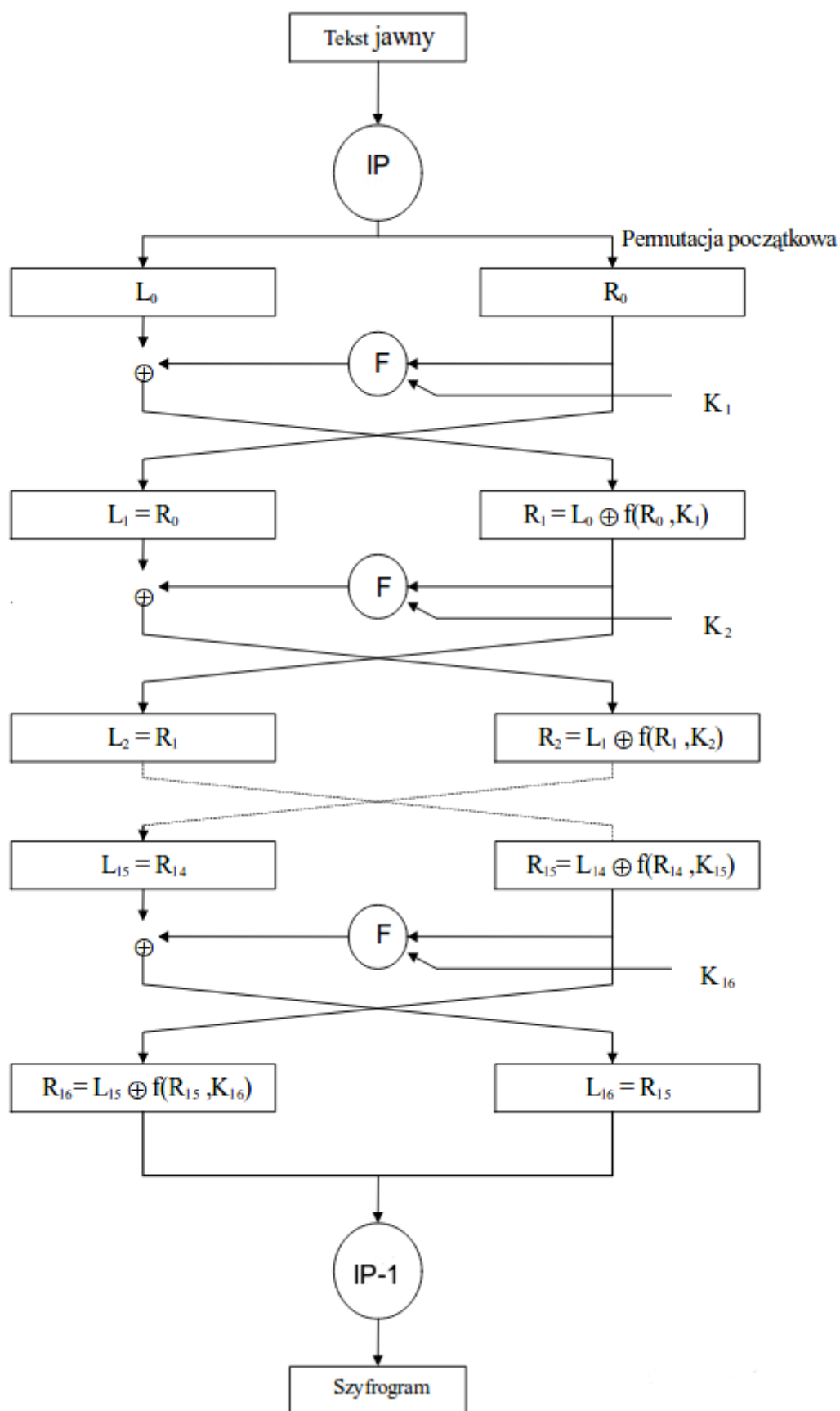
Tekst jawny (64-bitowy blok) poddawany jest wstępnej permutacji używając bloku permutacji początkowej (Tabela 1. blok IP). Potem dzielony jest na dwa podciągi 32-bitowe (Rysunek 1.). Następnie wykonywanych jest 16 cykli jednakowych operacji nazywanych funkcjami F. Po ostatnim cyklu lewa i prawa strona są łączone i poddawane permutacji końcowej używając bloku permutacji końcowej (Tabela 2. blok IP-1).

| | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|---|----|----|----|----|----|----|----|---|
| 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 |

Tabela 1. Blok IP

| | | | | | | | | | | | | | | | |
|----|---|----|----|----|----|----|----|----|---|----|----|----|----|----|----|
| 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 |

Tabela 2. Blok IP-1



Po zredukowaniu klucza do 56 bitów poprzez pominięcie bitów parzystości ciąg bitów poddawany jest permutacji wejściowej (tabela 3), 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 (tabela 4). Po połączeniu nowo powstałych ciągów wybiera się 48 z 56 bitów (tabela 5, permutacja z kompresją). Tak otrzymujemy klucz dla i -cyklu (gdzie i jest numerem cyklu), $i = 1, \dots, 16$.

| | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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 |

Tabela 3. Permutacja klucza PC-1

| | | | | | | | | | | | | | | | | |
|---------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| NR ITERACJI | 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 |

Tabela 4. Tablica przesunięć połówek klucza

| | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|
| 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 |

Tabela 5. Permutacja klucza PC-2 (permutacja z kompresją)

2.3 Funkcja F

W funkcji F (Rysunek 2.) prawa połowa bloku danych jest poddawana permutacji z rozszerzeniem (Tabela 6.), czyli z 32 do 48 bitów. Następnie, nowo powstały podciąg bitów, łączony jest za pomocą poelementowej sumy modulo 2 z 48 bitami przesuniętego i spermutowanego klucza. Otrzymany ciąg dzielony jest na 8 części i wprowadzany do skrzynek S-boxów (Tabela 8.), gdzie z 6-bitowych podciągów na wyjściu otrzymujemy 4-bitowe podciągi, które łączymy ze sobą. Powstały ciąg jest na wyjściu poddany permutacji (Tabela 7.).

| | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|
| 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 |

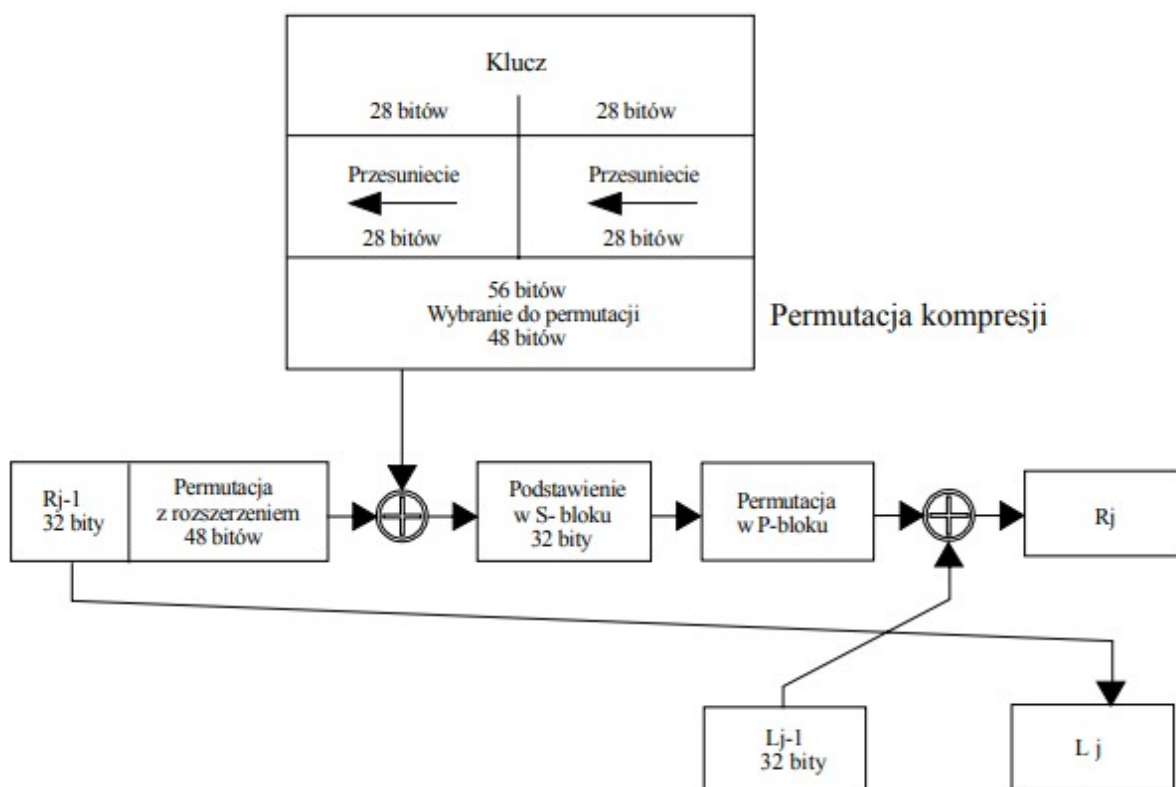
Tabela 6. Permutacja rozszerzenia (E)

| | | | | | | | | | | | | | | | |
|----|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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 |

Tabela 7. Permutacja P-bloku

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | |
|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 | S1 |
| 1 | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 | |
| 2 | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 | |
| 3 | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 | |
| 0 | 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 | S2 |
| 1 | 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 | |
| 2 | 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 | |
| 3 | 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 | |
| 0 | 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 | S3 |
| 1 | 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 | |
| 2 | 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 | |
| 3 | 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 | |
| 0 | 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 | S4 |
| 1 | 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 | |
| 2 | 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 | |
| 3 | 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 | |
| 0 | 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 | S5 |
| 1 | 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 | |
| 2 | 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 | |
| 3 | 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 | |
| 0 | 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 | S6 |
| 1 | 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 | |
| 2 | 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 | |
| 3 | 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 | |
| 0 | 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 | S7 |
| 1 | 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 | |
| 2 | 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 | |
| 3 | 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 | |
| 0 | 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 | S8 |
| 1 | 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 | |
| 2 | 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 | |
| 3 | 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 | |

Tabela 8. S-boksów



Rysunek 2. Wyznaczanie wartości funkcji F dla DES

Deszyfrowanie polega na zastosowaniu tych samych operacji w odwrotnej kolejności (różni się od szyfrowania tylko wyborem podkluczy, który teraz odbywa się od końca).

3. Implementacja

Program został zaimplementowany w technologii WPF w oparciu o język C# oraz .Net Framework. Aplikacja pozwala na wprowadzenie tekstu jawnego wiadomości w formacie znaków UTF8 poprzez wpisanie w podane pole lub poprzez wybór pliku .txt oraz wpisanie klucza poprzez wpisanie w podane pole.

4. Bibliografia

- [1]http://sun.aei.polsl.pl/~kfrancik/bsk/dokumenty/opis_DES.pdf
- [2]https://pl.wikipedia.org/wiki/Data_Encryption_Standard
- [3]https://en.wikipedia.org/wiki/Data_Encryption_Standard
- [4]http://wazniak.mimuw.edu.pl/images/0/0f/Bsi_04_wykl.pdf
- [5]https://pl.wikipedia.org/wiki/Dane_tabelaryczne_algorytmu_DES#Permutacja_rozszerzona