*Notatki z Kryptografii* 21 lutego 2001

# (DATA ENCRYPTION STANDARD)

1977 -National Bureau of Standards

IIUWr. II rok informatyki. Przygotował: Krzysztof Loryś

- Użytkownik wybiera klucz $K$ złożony z 56 losowych bitów.
  $K$ jest pamiętany razem z bitami parzystości na pozycjach $8, 16, ..., 64$.
  Bity losowe klucza $K$ (tj. bity o numerach $1, .., 7, 9, .., 15, .., 57, .., 63$) służą do wyznaczenia 48-bitowych kluczy $K_1, ..., K_{16}$.

- Wyznaczanie kluczy $K_1, ..., K_{16}$.

  (a) Tworzenie 28-bitowych bloków $C_0, D_0, ..., C_{16}, D_{16}$ z bitów losowych klucza $K$.

  $$C_0 = \begin{array}{ccccccc} 57 & 49 & 41 & 33 & 25 & 17 & 9 \\ 1 & 58 & 50 & 42 & 34 & 26 & 18 \\ 10 & 2 & 59 & 51 & 43 & 35 & 27 \\ 19 & 11 & 3 & 60 & 52 & 44 & 36 \end{array} \qquad D_0 = \begin{array}{ccccccc} 63 & 55 & 47 & 39 & 31 & 23 & 15 \\ 7 & 62 & 54 & 46 & 38 & 30 & 22 \\ 14 & 6 & 61 & 53 & 45 & 37 & 29 \\ 21 & 13 & 5 & 28 & 20 & 12 & 4 \end{array}$$

  Dla $n = 1, 2, ..., 16$

  $$C_n = LS_n(C_{n-1}) \qquad D_n = LS_n(D_{n-1}),$$

  gdzie $LS_n$ jest przesunięciem cyklicznym w lewo o 1 lub 2 bity (dokładniej: $LS_n$ jest przesunięciem o 1 bit dla $n = 1, 2, 9, 16$; dla pozostałych $n$-ów jest przesunięciem o dwa bity).

  (b) $\forall_{n=1,2,..,16}$ spośród 56-ciu bitów $C_nD_n$ wybieramy następujących 48 bitów

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

  i w ten sposób otrzymujemy klucz $K_n$.

- W schemacie kodowania używana jest funkcja $f(R_{n-1}, K_n)$, której pierwszy parametr jest 32-bitowym ciągiem (jego definicja będzie dalej), a drugi jest jednym z kluczy zdefiniowanych powyżej.

- Obliczanie $f(R_{n-1}, K_n)$.

  (a) $R_{n-1}$ rozszerzane jest do 48-iu bitów wg tabeli:

$$E(R_{n-1}) = \begin{array}{cccccc} 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \end{array}$$

(b) Obliczana jest różnica symetryczna $E(R_{n-1}) \oplus K_n$.
Niech $E(R_{n-1}) \oplus K_n = B_1 B_2 ... B_8$, gdzie $B_1, ..., B_8$ są ciągami 6-bitowymi.

(c) $B_1, ..., B_8$ zamieniane są na $\hat{B}_1, ..., \hat{B}_8$.
Do tego celu używamy tablic $S_1, ..., S_8$: array$[0..3, 0..15]$ of $0..15$. (Tablice te podane są na oddzielnej kartce. Zwróć uwagę, że ich elementami są liczby 4-bitowe.)
Jeśli $B_i = b_1 b_2 b_3 b_4 b_5 b_6$ to $\hat{B}_i = S_i[b_1 b_6, b_2 b_3 b_4 b_5]$.
Tak więc skrajne bity $B_i$ określają numer wiersza a środkowe - numer kolumny tablicy $S_i$, z których należy odczytać $\hat{B}_i$.

(d) Ostatecznie $f(R_{n-1}, K_n) = P(\hat{B}_1, ..., \hat{B}_8)$, gdzie $P$ jest następującą permutacją:

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

- **KODOWANIE**

(a) Tekst jawny dzielony jest na bloki 64-bitowe.

(b) Blok tekstu przekształcany jest permutacją IP:

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

Oznaczmy pierwsze 32 bity otrzymanego ciągu przez $L_0$, a ostatnie 32 bity przez $R_0$.

(c) Obliczane są ciągi bitów $L_n, R_n$ dla $n = 1, 2, ..., 16$.
$L_n = R_{n-1}$
$R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$

(d) Kod bloku= $IP^{-1}(R_{16}L_{16})$.

- **TABLICE** $S_1, S_2, ..., S_8$

$$S_1 = \boxed{\begin{array}{cccccccccccccccc}
14 & 4 & 13 & 1 & 2 & 15 & 11 & 8 & 3 & 10 & 6 & 12 & 5 & 9 & 0 & 7 \\
0 & 15 & 7 & 4 & 14 & 2 & 13 & 1 & 10 & 6 & 12 & 11 & 9 & 5 & 3 & 8 \\
4 & 1 & 14 & 8 & 13 & 6 & 2 & 11 & 15 & 12 & 9 & 7 & 3 & 10 & 5 & 0 \\
15 & 12 & 8 & 2 & 4 & 9 & 1 & 7 & 5 & 11 & 3 & 14 & 10 & 0 & 6 & 13
\end{array}}$$

$$S_2 = \boxed{\begin{array}{cccccccccccccccc}
15 & 1 & 8 & 14 & 6 & 11 & 3 & 4 & 9 & 7 & 2 & 13 & 12 & 0 & 5 & 10 \\
3 & 13 & 4 & 7 & 15 & 2 & 8 & 14 & 12 & 0 & 1 & 10 & 6 & 9 & 11 & 5 \\
0 & 14 & 7 & 11 & 10 & 4 & 13 & 1 & 5 & 8 & 12 & 6 & 9 & 3 & 2 & 15 \\
13 & 8 & 10 & 1 & 3 & 15 & 4 & 2 & 11 & 6 & 7 & 12 & 0 & 5 & 14 & 9
\end{array}}$$

$$S_3 = \boxed{\begin{array}{cccccccccccccccc}
10 & 0 & 9 & 14 & 6 & 3 & 15 & 5 & 1 & 13 & 12 & 7 & 11 & 4 & 2 & 8 \\
13 & 7 & 0 & 9 & 3 & 4 & 6 & 10 & 2 & 8 & 5 & 14 & 12 & 11 & 15 & 1 \\
13 & 6 & 4 & 9 & 8 & 15 & 3 & 0 & 11 & 1 & 2 & 12 & 5 & 10 & 14 & 7 \\
1 & 10 & 13 & 0 & 6 & 9 & 8 & 7 & 4 & 15 & 14 & 3 & 11 & 5 & 2 & 12
\end{array}}$$

$$S_4 = \boxed{\begin{array}{cccccccccccccccc}
7 & 13 & 14 & 3 & 0 & 6 & 9 & 10 & 1 & 2 & 8 & 5 & 11 & 12 & 4 & 15 \\
13 & 8 & 11 & 5 & 6 & 15 & 0 & 3 & 4 & 7 & 2 & 12 & 1 & 10 & 14 & 9 \\
10 & 6 & 9 & 0 & 12 & 11 & 7 & 13 & 15 & 1 & 3 & 14 & 5 & 2 & 8 & 4 \\
3 & 15 & 0 & 6 & 10 & 1 & 13 & 8 & 9 & 4 & 5 & 11 & 12 & 7 & 2 & 14
\end{array}}$$

$$S_5 = \boxed{\begin{array}{cccccccccccccccc}
2 & 12 & 4 & 1 & 7 & 10 & 11 & 6 & 8 & 5 & 3 & 15 & 13 & 0 & 14 & 9 \\
14 & 11 & 2 & 12 & 4 & 7 & 13 & 1 & 5 & 0 & 15 & 10 & 3 & 9 & 8 & 6 \\
4 & 2 & 1 & 11 & 10 & 13 & 7 & 8 & 15 & 9 & 12 & 5 & 6 & 3 & 0 & 14 \\
11 & 8 & 12 & 7 & 1 & 14 & 2 & 13 & 6 & 15 & 0 & 9 & 10 & 4 & 5 & 3
\end{array}}$$

$$S_6 = \boxed{\begin{array}{cccccccccccccccc}
12 & 1 & 10 & 15 & 9 & 2 & 6 & 8 & 0 & 13 & 3 & 4 & 14 & 7 & 5 & 11 \\
10 & 15 & 4 & 2 & 7 & 12 & 9 & 5 & 6 & 1 & 13 & 14 & 0 & 11 & 3 & 8 \\
9 & 14 & 15 & 5 & 2 & 8 & 12 & 3 & 7 & 0 & 4 & 10 & 1 & 13 & 11 & 6 \\
4 & 3 & 2 & 12 & 9 & 5 & 15 & 10 & 11 & 14 & 1 & 7 & 6 & 0 & 8 & 13
\end{array}}$$

$$S_7 = \boxed{\begin{array}{cccccccccccccccc}
4 & 11 & 2 & 14 & 15 & 0 & 8 & 13 & 3 & 12 & 9 & 7 & 5 & 10 & 6 & 1 \\
13 & 0 & 11 & 7 & 4 & 9 & 1 & 10 & 14 & 3 & 5 & 12 & 2 & 15 & 8 & 6 \\
1 & 4 & 11 & 13 & 12 & 3 & 7 & 14 & 10 & 15 & 6 & 8 & 0 & 5 & 9 & 2 \\
6 & 11 & 13 & 8 & 1 & 4 & 10 & 7 & 9 & 5 & 0 & 15 & 14 & 2 & 3 & 12
\end{array}}$$

$$S_8 = \boxed{\begin{array}{cccccccccccccccc}
13 & 2 & 8 & 4 & 6 & 15 & 11 & 1 & 10 & 9 & 3 & 14 & 5 & 0 & 12 & 7 \\
1 & 15 & 13 & 8 & 10 & 3 & 7 & 4 & 12 & 5 & 6 & 11 & 0 & 14 & 9 & 2 \\
7 & 11 & 4 & 1 & 9 & 12 & 14 & 2 & 0 & 6 & 10 & 13 & 15 & 3 & 5 & 8 \\
2 & 1 & 14 & 7 & 4 & 10 & 8 & 13 & 15 & 12 & 9 & 0 & 3 & 5 & 6 & 11
\end{array}}$$