

SEMESTRÁLNÍ PRÁCE Z PŘEDMĚTU KIV/BIT

IMPLEMENTACE ŠIFRY SAFER K-64

Jméno: Jakub Záruba

Osobní číslo: A13B0476P

E-mail: eflyax@students.zcu.cz

Datum: 30. dubna 2016

Obsah

1	O šifře SAFER	3
2	Popis algoritmů	4
2.1	Šifrování	4
2.2	Produkce podklíčů	6
2.3	Dešifrování	6
3	Závěr	7

1 O šifře SAFER

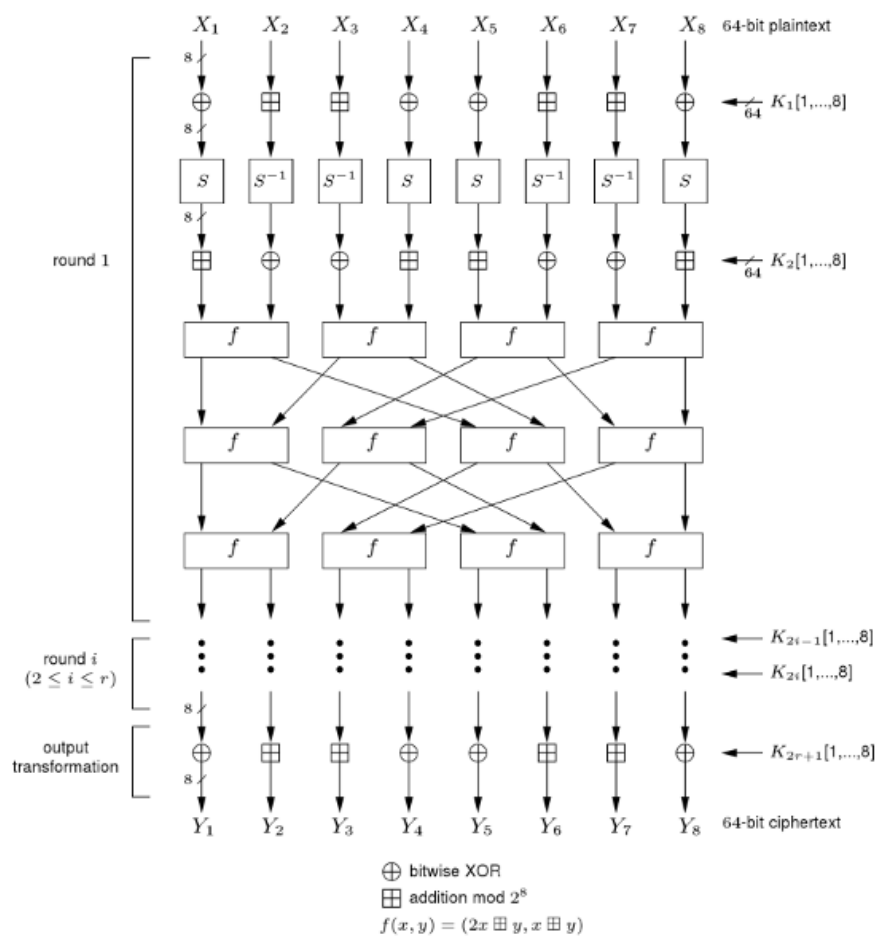
Šifra SAFER K-64 (Secure And FAST Encryption Routine, s 64bitovým klíčem), je bloková šifra s 64bitovým plaintextem. Šifra SAFER k-64 spadá do rodiny šifer SAFER, které navrhnul James Massey (jeden z návrhářů šifry IDEA). Poprvé byla publikována v roce 1993. Všechny algoritmy z rodiny SAFER jsou nepatentované a jsou k dispozici pro neomezené použití.

2 Popis algoritmů

Šifra používá r identických šifrovacích kol (rounds). Tato šifra standardně používá 6 rounds, počet může být volitelný. Maximum je však 10. Pro zadaný 64 bitový klíč se vytvoří $2r + 1$ podklíčů, které mají také 64 bitů. 2 klíče se vždy použijí v jednom šifrovacím kole ($2r$) a poslední klíč ($+1$) se použije pro výstupní transformaci. Uživatelem zvolený vstup a klíč je dlouhý 8 bajtů (64 bitů).

2.1 Šifrování

- **Vstup:** $r, 6 \leq r \leq 10$; 64 bitový text $M = m_1 \dots m_{64}$; klíč $K = k_1 \dots k_{64}$
 - **Výstup:** 64 bitový šifrovaný text (blok) $Y = (Y_1, \dots, Y_8)$
1. Výpočet podklíčů K_1, \dots, K_8 , viz kapitola xyz
 2. $(X_1, X_2, \dots, X_8) \leftarrow (m_1 \dots m_8, m_9 \dots m_{16}, \dots, m_{57} \dots m_{64})$.
 3. Pro i od 1 proved' akce: (XOR-addition, S-box, XOR-addition, 3x lineární vrstvy)
 4. (a) Pro $j = 1, 4, 5, 8$: $X_j \leftarrow X_j \oplus K_{2i-1|j|}$
Pro $j = 2, 3, 6, 7$: $X_j \leftarrow X_j \boxplus K_{2i-1|j|}$
(b) Pro $j = 1, 4, 5, 8$: $X_j \leftarrow S[X_j]$, Pro $j = 2, 3, 6, 7$: $X_j \leftarrow S_{inv}[X_j]$.
(c) Pro $j = 1, 4, 5, 8$: $X_j \leftarrow S[X_j] \boxplus K_{2i|j|}$. Pro $j = 2, 3, 6, 7$: $X_j \leftarrow X_j \oplus K_{2i|j|}$.
(d) Pro $j = 1, 3, 5, 7$: $(X_j, X_{j+1}) \leftarrow f(X_j, X_{j+1})$
(e) $(Y_1, Y_2) \leftarrow f(X_1, X_3)$, $(Y_3, Y_4) \leftarrow f(X_5, X_7)$
 $(Y_5, Y_6) \leftarrow f(X_2, X_4)$, $(Y_7, Y_8) \leftarrow f(X_6, X_8)$
Pro j od 1 do 8 proved' : $X_j \leftarrow Y_j$
(f) $(Y_1, Y_2) \leftarrow f(X_1, X_3)$, $(Y_3, Y_4) \leftarrow f(X_5, X_7)$
 $(Y_5, Y_6) \leftarrow f(X_2, X_4)$, $(Y_7, Y_8) \leftarrow f(X_6, X_8)$
Pro j od 1 do 8 proved' : $X_i \leftarrow Y_j$
 5. Výstupní transformace:
Pro $j = 1, 4, 5, 8$: $Y_j \leftarrow X_j \oplus K_{2r+1|j|}$.
Pro $j = 2, 3, 6, 7$: $Y_j \leftarrow X_j \boxplus K_{2r+1|j|}$



Obrázek 1: Schéma šifrování

2.2 Produkce podklíčů

- **Vstup:** 64 bitový klíč $K = k_1 \dots k_{64}$; počet šifrovacích kol r
- **Výstup:** 64 bitové podklíče K_1, \dots, K_{2r+1}

1. Nechť $R[i]$ představuje 8 bitové úložiště dat a nechť $B_i[j]$ představuje bajt j v B_i
2. $(R[1], R[2], \dots, R[8]) \leftarrow (k_1 \dots k_8, k_9 \dots k_{16}, \dots, k_{57} \dots k_{64})$
3. Pro i od 2 do $2r+1$ proved':
 - (a) Pro j od 1 do 8 proved': $R[j] \leftarrow (R[j] \leftarrow 3)$
 - (b) Pro j od 1 do 8 proved': $K_i[j] \leftarrow R[j] \boxplus B_i[j]$

2.3 Dešifrování

Proces dešifrování používá pro zadaný klíč K stejné hledání podklíčů, jako při šifrování. Proces začíná s se vstupní transformací s klíčem K_{2r+1} k výstupní transformaci. Veškeré modulární součty jsou nahrazeny modulárním odečítáním. Funkce f v lineárních vrstvách jsou nahrazeny jejich inverzními funkcemi: $f_{inv}(L, R) = (L - R, 2R - L)$ s odečítáním mod 256 v tříkrokových sekvencích.

3 Závěr

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas.