Symetrické kryptosystémy

Definice. *Symetrický kryptosystém* $\mathcal{S}$ je pětice konečných množin $(\mathcal{P}, \mathcal{C}, \mathcal{K}, e, d)$, kde

$\mathcal{P}$ je množina otevřených textů (plaintextů)

$\mathcal{C}$ je množina zašifrovaných textů (ciphertextů)

$\mathcal{K}$ je prostor klíčů

$e : \mathcal{P} \times \mathcal{K} \to \mathcal{C}$ je šifrovací zobrazení

$d : \mathcal{C} \times \mathcal{K} \to \mathcal{P}$ je dešifrovací zobrazení

Pro každý plaintext $x \in \mathcal{P}$ a každý klíč $K \in \mathcal{K}$ musí platit: $d(e(x, K), K) = x$, neboli v jiné verzi značení: $d_K \circ e_K = \mathrm{Id}_{\mathcal{P}}$.

Budeme se zabývat pouze *endomorfními* kryptosystémy, tedy kryptosystémy, ve kterých je $\mathcal{P} = \mathcal{C}$. Pro každý klíč $K \in \mathcal{K}$ pak musí být $e_K : \mathcal{P} \to \mathcal{P}$ bijekce ($\mathcal{P}$ je konečná množina) a $d_K = e_K^{-1}$. Endomorfní kryptosystém můžeme zapisovat jako trojici $(\mathcal{P}, \mathcal{K}, e)$.

Od starověku lidstvo používá dva základní typy šifrovacích algoritmů: substituční a permutační šifry. Tyto šifry slouží jako stavební kameny i v moderních kryptosystémech.

Definice. *Substituční šifra* nad abecedou A je endomorfní kryptosystém $(\mathcal{P} = A,\ \mathcal{K} = \mathrm{S}_A,\ e)$, kde S_A je symetrická grupa na množině A a pro $x \in \mathcal{P}$ a $\pi \in \mathcal{K}$ je $e(x, \pi) = \pi(x)$, tedy $e_\pi = \pi$.

Jako historický příklad substituční šifry můžeme uvést *posunutí*. Jde o substituční šifru nad n-prvkovou abecedou $A = \mathbb{Z}_n$ s tvarem šifrovacího klíče $\pi(x) = (x + b) \bmod n$ pro pevné $b \in A$. Posunutí o tři znaky latinské abecedy je známé jako Caesarova šifra. *Multiplikativní šifra* nad A má tvar klíče $\pi(x) = ax \bmod n$ pro pevné $a \in A$, $\mathrm{NSD}(a, n) = 1$. Rozšířením obou kryptosystémů je *afinní šifra* s tvarem šifrovacích klíčů $\pi(x) = (ax + b) \bmod n$ pro pevně zvolené $a, b \in A$, $\mathrm{NSD}(a, n) = 1$.
Jako další příklad můžeme zmínit hebrejskou šifru Atbash, kde tajná permutace abecedy byla složením disjunktních transpozic: první a poslední znak (aleph $\leftrightarrow$ tav), druhý a předposlední znak (beth $\leftrightarrow$ shin), ...

Definice. Pro abecedu A a $m \in \mathbb{N}$ definujeme *permutační šifru* jako endomorfní kryptosystém $(\mathcal{P} = A^m,\ \mathcal{K} = \mathrm{S}_m,\ e)$, kde pro $x = (x_1, \ldots, x_m) \in \mathcal{P}$ a $\pi \in \mathcal{K}$ je $e(x, \pi) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(m)})$.

Historickým příkladem permutační šifry je řecká šifra Skytalé jejímž tajným klíčem byl hranol, který se při šifrování šroubovitě ovinul pásem papyru a na jeho boky pak byla zapsána zpráva.

Definice. *Hillova šifra* je kryptosystém $(\mathcal{P} = \mathbb{Z}_n^m,\ \mathcal{K} = \mathrm{GL}_m(\mathbb{Z}_n),\ e)$, kde $\mathrm{GL}_m(\mathbb{Z}_n)$ je grupa invertibilních matic řádu m nad $\mathbb{Z}_n$ a pro $x \in \mathcal{P}$ a $M \in \mathcal{K}$ je $e(x, M) = M \cdot x$.

Hillovu šifru můžeme chápat jako rozšíření permutační šifry, která je jejím podsystémem se stejnou množinou plaintextů a reprezentací klíčů permutačními maticemi.

Při kryptoanalýze moderních symetrických šifer předpokládáme, že útočník zná použitý kryptosystém (takzvaný Kerckhoffův princip), a útoky rozlišujeme podle možností útočníka:

- útok pouze se znalostí zašifrovaného textu (ciphertext only attack)
- útok se znalostí otevřeného textu (known plaintext attack)
- útok s volbou otevřeného textu (chosen plaintext attack)

Pokud substituční šifra nahrazuje krátké bloky otevřeného textu, obvykle stačí malý objem zašifrovaného textu k úspěšnému ciphertext only útoku (frekvenční analýza ciphertextu s využitím statistických vlastností předpokládaného typu otevřeného textu).

V případě *known plaintext* útoku musí mít útočník možnost pasivního sledování vstupu (a výstupu) šifry, která mu stačí k nasbírání množiny vzorků $\{(x, e(x))\}$ s potřebnými parametry. Zde předpokládáme, že vstupy šifry jsou dostatečně náhodné. Pokud jsou požadavky útoku takové, že pravděpodobnost výskytu potřebných vzorků při šifrování s náhodným vstupem neumožňuje získat požadovanou množinu vzorků, musí útočník aktivně do vstupu šifry zasahovat a mluvíme o *chosen plaintext* útoku.

Permutační resp. Hillova šifra jsou při vhodné volbě parametrů (dostatečně velké m, náhodně zvolený klíč) ciphertext only útokům odolné. K odhalení klíče Hillovy šifry však stačí získat množinu dvojic $\{(x, e(x))\}$ takovou, že příslušné plaintexty generují $\mathbb{Z}_n^m$ (jako modul nad $\mathbb{Z}_n$). Je-li chování vstupů šifry dostatečně náhodné, pak lze takovou množinu pozorováním vstupů snadno získat. Například v případě tělesa, kdy potřebujeme získat m nezávislých vektorů v $\mathbb{F}^m$, je pravděpodobnost, že náhodný vektor bude nezávislý na dosud získaných vektorech, alespoň $\frac{|\mathbb{F}|-1}{|\mathbb{F}|}$. Totiž počet různých posunutí nadroviny generované $m-1$ nezávislými vektory je $|\mathbb{F}|$ (velikost přímky). Složitost takového known plaintext útoku pak bude srovnatelná se složitostí šifrování (bude polynomiální ve složitosti šifrování).

Moderní kryptosystémy musí být odolné proti known plaintext i chosen plaintext útokům. Mezi hlavní metody útoků na symetrické kryptosystémy patří lineární kryptoanalýza, kterou lze považovat za known plaintext útok. Diferenční kryptoanalýza patří díky svým specifickým požadavkům na vztahy mezi plaintexty potřebných vzorků mezi chosen plaintext útoky. Oběma těmto metodám se budeme věnovat později.

Definice. Pro kryptosystémy $\mathcal{S}_1 = (\mathcal{P}, \mathcal{K}_1, e_1)$ a $\mathcal{S}_2 = (\mathcal{P}, \mathcal{K}_2, e_2)$ se stejnou množinou plaintextů definujeme *produktový kryptosystém* $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2 = (\mathcal{P}, \mathcal{K} = \mathcal{K}_1 \times \mathcal{K}_2, e)$, kde pro $x \in \mathcal{P}$ a $(K_1, K_2) \in \mathcal{K}$ je $e(x, (K_1, K_2)) = e_2((e_1(x, K_1)), K_2)$. Šifrovací zobrazení pak můžeme zapsat jako $e_{(K_1,K_2)} = {e_2}_{K_2} \circ {e_1}_{K_1}$.

Definice. Kryptosystém $\mathcal{S}_1 = (\mathcal{P}, \mathcal{K}_1, e_1)$ *lze převést* do kryptosystému $\mathcal{S}_2 = (\mathcal{P}, \mathcal{K}_2, e_2)$, pokud existuje zobrazení $t : \mathcal{K}_1 \to \mathcal{K}_2$ takové, že pro všechny $x \in \mathcal{P}$ a všechny $K \in \mathcal{K}_1$ platí $e_1(x, K) = e_2(x, t(K))$.

Definice. Kryptosystémy $\mathcal{S}_1$ a $\mathcal{S}_2$ jsou *ekvivalentní*, pokud je lze navzájem do sebe převést. V tomto případě píšeme $\mathcal{S}_1 \sim \mathcal{S}_2$.

Definice. Kryptosystémy $\mathcal{S}_1$ a $\mathcal{S}_2$ *komutují*, pokud platí $\mathcal{S}_1 \times \mathcal{S}_2 \sim \mathcal{S}_2 \times \mathcal{S}_1$.

Definice. Kryptosystém $\mathcal{S}$ je *idempotentní*, pokud platí $\mathcal{S}^2 = \mathcal{S} \times \mathcal{S} \sim \mathcal{S}$.

Z definice substituční i permutační šifry plyne idempotence těchto kryptosystémů. Jako příklad komutujících kryptosystémů můžeme uvést posunutí a multiplikativní šifru nad stejnou abecedou: posunutí $\times$ multiplikativní šifra $\sim$ multiplikativní šifra $\times$ posunutí $\sim$ afinní šifra.

Produkt kryptosystémů je asociativní binární operace na kryptosystémech s danou množinou plaintextů. Tyto kryptosystémy tak tvoří pologrupu a ekvivalence kryptosystémů je kongruencí této pologrupy. Faktorizací podle $\sim$ dostaneme konečnou pologrupu ($\mathcal{P}$ je pevná konečná množina a můžeme ztotožnit klíče, které dávají stejná šifrovací zobrazení). Pro každý kryptosystém $\mathcal{S}$ tedy existují čísla $k, l \in \mathbb{N}$, $k < l$, pro která je $\mathcal{S}^k \sim \mathcal{S}^l$. Cyklická pologrupa generovaná $\mathcal{S}$ pak má ve faktoru podle $\sim$ nejvýše $l - 1$ prvků. Při návrhu kryptosystému je žádoucí, aby příslušná cyklická pologrupa byla dostatečně velká.

Moderní symetrické blokové šifry jsou obvykle produktem svých kol - tedy přesněji mocninou svého kolového kryptosystému. Cyklická pologrupa generovaná kolovým kryptosystémem musí být tedy dostatečně velká, abychom iterací kola mohli získávat komplexnější šifrovací zobrazení. Speciálně nesmí být kolový kryptosystém idempotentní. Kolo je obvykle produktem několika vrstev, které bývají idempotentní (např. substituční šifra, permutační šifra, Hillova šifra). Přitom platí, že produkt idempotentních komutujících kryptosystémů je opět idempotentní. Návrh kola šifry tedy musí obsahovat nekomutující vrstvy.

Symetrická šifra AES pracuje se 16-bytovými bloky. Její kolové klíče jsou prvky $\mathbb{F}_2^{128}$ a označíme-li e šifrovací zobrazení kola AES, lze dokázat, že platí

$$\langle \{ e_K \,;\; K \in \mathbb{F}_2^{128} \} \rangle \;=\; \mathrm{A}_{\mathbb{F}_2^{128}}$$

Tedy množina kolových šifrovacích zobrazení pro všechny hodnoty klíčů generuje celou alternující grupu na množině plaintextů. Počet různých šifrovacích zobrazení l-té mocniny kola AES je nejvýše $(2^{128})^l$. Velikost alternující grupy můžeme odhadnout jako $|A_{2^{128}}| > 2^{2^{128}}$. Abychom l-tou mocninou kola AES mohli získat celou alternující grupu, musí platit $l \sim 2^{128}$. Pologrupa generovaná kolem AES má tedy alespoň 2^{128} prvků.

Definice. Ať jsou $\mathcal{S} = (\mathcal{P}, \mathcal{K}, e)$ a $\bar{\mathcal{S}} = (\mathcal{P}, \bar{\mathcal{K}}, \bar{e})$ kryptosystémy se stejnou množinou plaintextů a $N \in \mathbb{N}$. Mějme dále převod kryptosystému $\bar{\mathcal{S}}$ do kryptosystému $\mathcal{S}^N$:

$$\bar{\mathcal{S}} \longrightarrow \mathcal{S}^N$$
$$\bar{\mathcal{K}} \xrightarrow{t} \mathcal{K}^N$$

V této situaci říkáme, že $\bar{\mathcal{S}}$ je *iterovaný kryptosystém*, $\mathcal{S}$ je *kolo* $\bar{\mathcal{S}}$, N je počet kol. Zobrazení t se nazývá *algoritmus přípravy klíčů* (key schedule), obraz v t je příslušná N-tice kolových klíčů.

Substitučně-permutační síť (SPN). Popíšeme konkrétní příklad iterovaného kryptosystému. Mějme $l, m \in \mathbb{N}$, $\pi_{\mathrm{S}} \in \mathrm{S}_{\mathbb{F}_2^l}$ a $\pi_{\mathrm{P}} \in \mathrm{S}_{lm}$. Označme σ konkatenaci m permutací π_{S}. Tedy $\sigma \in \mathrm{S}_{\mathbb{F}_2^{lm}}$, obraz v σ je konkatenací obrazů l-bitových bloků vstupního vektoru v π_{S}.
Položme $\mathcal{P} = \mathbb{F}_2^{lm} = \mathcal{K}$, kde $\mathcal{P}$ je množina plaintextů a $\mathcal{K}$ je prostor kolových klíčů (algoritmus přípravy klíčů ponecháme nyní stranou). Definujme následující kryptosystémy:

$\mathcal{S}_1 = (\mathcal{P}, \mathcal{K}, e_1),\ e_1(x, K) = x + K$ (součet vektorů v $\mathbb{F}_2^{lm}$)

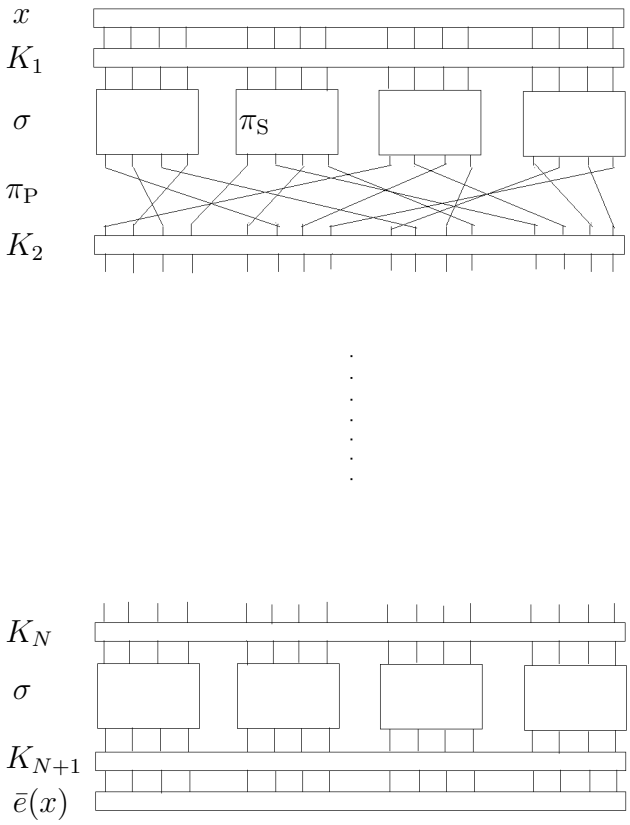
$\mathcal{S}_2 = (\mathcal{P}, \{\sigma\}, e_2),\ e_2$ je šifrovací zobrazení substituční šifry s jediným klíčem σ

$\mathcal{S}_3 = (\mathcal{P}, \{\pi_{\mathrm{P}}\}, e_3),\ e_3$ je šifrovací zobrazení permutační šifry s jediným klíčem π_{P}

Kolový kryptosystém SPN je produkt $\mathcal{S}_1 \times \mathcal{S}_2 \times \mathcal{S}_3$. Kolo má tedy tři vrstvy: přičtení kolového klíče, substituční vrstvu $\mathcal{S}_2$ a permutační vrstvu $\mathcal{S}_3$. Vyjímkou je poslední kolo, které má tvar $\mathcal{S}_1 \times \mathcal{S}_2 \times \mathcal{S}_1$. Celý N-kolový kryptosystém má tvar:

$$(\mathcal{S}_1 \times \mathcal{S}_2 \times \mathcal{S}_3)^{N-1} \times (\mathcal{S}_1 \times \mathcal{S}_2 \times \mathcal{S}_1)$$

Počet kolových klíčů v N-kolovém kryptosystému SPN je tedy $N + 1$. Tyto kolové klíče jsou odvozené algoritmem přípravy klíčů ze šifrovacího klíče, který je jedinou tajnou informací tohoto kryptosystému. Šifrovací algoritmus včetně pevně zvolených permutací π_S a π_P i algoritmus přípravy klíčů jsou veřejně známé.



Poznámky. 1) Kryptosystému $\mathcal{S}_2$ se říká *vrstva* S-*boxů*, π_S je l-bitový S-box (substitution-box).

2) Návrh SPN se blíží návrhu šifry AES. V kolovém kryptosystému AES je navíc lineární vrstva (MixColumns), která byla přidána kvůli zvýšení odolnosti proti lineárním a diferenčním útokům.

3) V návrhu SPN je určitá odchylka od definice iterovaného kryptosystému. Pokud bychom se přesně drželi definice, dostali bychom kryptosystém ve tvaru $(\mathcal{S}_1 \times \mathcal{S}_2 \times \mathcal{S}_3)^N$. Tím bychom ale útočníkovi usnadnili jeho úlohu - mohl by přejít s ciphertexty přes známé vrstvy $\mathcal{S}_3$ a $\mathcal{S}_2$ a útočit pouze na zkrácený kryptosystém. Přičtení dalšího kolového klíče v závěru šifrování je standardní obrana proti zkrácení kryptosystému (key whitening).
Samotné přidání další vrstvy $\mathcal{S}_1$ ale nemusí stačit. Pokud by kryptosystém $\mathcal{S}_1$ komutoval se sousední veřejně známou vrstvou, opět by bylo možné šifrování o tuto vrstvu zkrátit. To je případ kryptosystému $(\mathcal{S}_1 \times \mathcal{S}_2 \times \mathcal{S}_3)^N \times \mathcal{S}_1$. Totiž $e_{\pi_P}(x) + K = e_{\pi_P}(x + e_{\pi_P^{-1}}(K))$, kde e je šifrovací zobrazení permutační šifry. Tedy kryptosystémy $\mathcal{S}_1$ a $\mathcal{S}_3$ komutují.

4) Při implementaci dešifrování v SPN můžeme komutování $\mathcal{S}_1$ a $\mathcal{S}_3$ využít. Totiž po přehození vnitřních vrstev $\mathcal{S}_1$ se sousedními vrstvami $\mathcal{S}_3$ (a příslušném přepermutování klíčů) bude pořadí dešifrovacích kroků stejné jako při šifrování.

Podívejme se, jak je to s komutováním dalších vrstev kola SPN.

Lemma. Kryptosystémy $\mathcal{S}_1$ a $\mathcal{S}_2$ komutují právě když je S-box π_S afinní zobrazení.

Důkaz. Z konstrukce substituční vrstvy je snadno vidět, že π_{S} je afinní právě když σ je afinní. Je-li tedy σ afinní, pak $\sigma(x) = g(x) + v$, kde $g : \mathbb{F}_2^{lm} \to \mathbb{F}_2^{lm}$ je lineární a $v \in \mathbb{F}_2^{lm}$ je pevný vektor. Platí $\sigma(x + K) = g(x + K) + v = (g(x) + v) + g(K) = \sigma(x) + g(K)$.
Ať naopak $\mathcal{S}_1$ a $\mathcal{S}_2$ komutují. Pro vektory $v_1, v_2, w_1, w_2 \in \mathbb{F}_2^{lm}$ takové, že $v_1 + v_2 = w_1 + w_2$, označme $K = v_1 + v_2$. Z komutování musí existovat klíč K' tak, že $\sigma(v_1 + K) = \sigma(v_1) + K'$ a $\sigma(w_1 + K) = \sigma(w_1) + K'$. Tedy $\sigma(v_1) + \sigma(v_2) = \sigma(v_1) + \sigma(v_1 + K) = K' = \sigma(w_1) + \sigma(w_2)$. Jinými slovy: máme-li dvojice vektorů se stejnou diferencí (počítáme nad $\mathbb{F}_2$), pak jejich obrazy v σ musí mít stejnou diferenci.
Označme $\tau_{\sigma(0)}$ posunutí (translaci) o vektor $\sigma(0)$. Ukážeme, že $\tau_{\sigma(0)} \circ \sigma$ je lineární:

$$(\tau_{\sigma(0)} \circ \sigma)(v) + (\tau_{\sigma(0)} \circ \sigma)(w) = \sigma(v) + \sigma(w) = \sigma(v + w) + \sigma(0) = (\tau_{\sigma(0)} \circ \sigma)(v + w)$$

□

V návrhu SPN musí být S-box nelineární (neafinní). Při komutování substituční a permutační vrstvy rovněž dojde k degradaci kryptosystému. Pro σ a π_{P} v návrhu SPN dokonce musí platit silnější vlastnost: pro každou vrstvu l-bitových S-boxů σ' a každou permutaci složek π' je $e_{\pi_{\mathrm{P}}} \circ \sigma \neq \sigma' \circ e_{\pi'}$. Na závěr tohoto textu ukážeme, jak lze takovou substituční a permutační vrstvu zvolit.

Zaveďme kryptosystémy $\tilde{\mathcal{S}}_2$ a $\tilde{\mathcal{S}}_3$ jako rozšíření $\mathcal{S}_2$ a $\mathcal{S}_3$:

$$\begin{aligned}
\tilde{\mathcal{S}}_2 \;&=\; (\mathcal{P} = \mathbb{F}_2^{lm},\, \tilde{\mathcal{K}}_2 = (\mathrm{S}_{\mathbb{F}_2^l})^m,\, \tilde{e}_2),\\
&\quad\; \tilde{K} \in \tilde{\mathcal{K}}_2 \subseteq \mathrm{S}_{\mathbb{F}_2^{lm}} \text{ je konkatenace } m \text{ } l\text{-bitových S-boxů (mohou být různé)},\\
&\quad\; \tilde{e}_2 \text{ je šifrovací zobrazení substituční šifry s danou množinou klíčů}\\
\tilde{\mathcal{S}}_3 \;&=\; (\mathcal{P} = \mathbb{F}_2^{lm},\, \tilde{\mathcal{K}}_3 = \mathrm{S}_{lm},\, \tilde{e}_3) \;\text{ je permutační šifra}
\end{aligned}$$

Ukážeme, že pro $l, m > 1$ kryptosystémy $\tilde{\mathcal{S}}_2$ a $\tilde{\mathcal{S}}_3$ nekomutují.

Definice. Ať je $f : \prod_{i \in I} A_i \to \prod_{j \in J} B_j$ zobrazení kartézských součinů množin, I a J jsou konečné. Pro $r \in I$ a $s \in J$ řekneme, že s-tá složka obrazů f *závisí na* r, pokud existují $a, a' \in \prod_{i \in I} A_i$ takové, že $a \restriction I \setminus \{r\} = a' \restriction I \setminus \{r\}$ a přitom $f(a)_s \neq f(a')_s$. Označíme $I_{f,s} = \{r \in I\,;\, s \text{ závisí na } r\}$.

Lemma. Ve značení předchozí definice, pro každá $a, a' \in \prod_{i \in I} A_i$ platí: je-li $a \restriction I_{f,s} = a' \restriction I_{f,s}$, pak $f(a)_s = f(a')_s$. Je-li dále $I' \subseteq I$ taková, že kdykoli se $a, a' \in \prod_{i \in I} A_i$ shodují na I', pak $f(a)_s = f(a')_s$, musí být $I_{f,s} \subseteq I'$.

Důkaz. Pro $r \in I \setminus I_{f,s}$ mohu zkonstruovat $\tilde{a} \in \prod_{i \in I} A_i$ tak, že $\tilde{a} \restriction I \setminus \{r\} = a \restriction I \setminus \{r\}$ a $\tilde{a}_r = a'_r$. Musí platit $f(\tilde{a})_s = f(a)_s$. Takto mohu na indexech mimo $I_{f,s}$ postupně nahradit hodnoty a hodnotami a', přičemž hodnota $f(a)_s$ zůstane v s-té složce obrazu zachována.
Pro $r \in I_{f,s} \setminus I'$ existují $a, a' \in \prod_{i \in I} A_i$, které se shodují na $I \setminus \{r\}$ a $f(a)_s \neq f(a')_s$. To je ve sporu s vlastností I'. □

Definice. Pro $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ definujeme *stupeň difuze*:

$$\mathrm{d}(f) = \frac{|\{0 \leq s < m; |I_{f,s}| = n\}|}{m}$$

Řekneme, že f má *plnou difuzi*, pokud $\mathrm{d}(f) = 1$.

Obvyklým požadavkem na iterované kryptosystémy je, aby kryptosystém po malém počtu kol dosáhl plné difuze.

Věta. Kryptosystémy $\tilde{\mathcal{S}}_2$ a $\tilde{\mathcal{S}}_3$ pro $l, m > 1$ nekomutují.

Důkaz. Ať je $\sigma \in \tilde{\mathcal{K}}_2$ konkatenace S-boxů, pro kterou existují výstupní indexy $s \neq s'$ takové, že $I_{\sigma,s} \cap I_{\sigma,s'} \neq \emptyset$. Hodnoty na indexech různých S-boxů jsou na sobě nezávislé, tedy s a s' musí být výstupní indexy stejného S-boxu. Je-li $\pi \in \tilde{\mathcal{K}}_3$ permutace složek taková, že $\pi(s)$ a $\pi(s')$ leží v indexech různých S-boxů, pak $e_\pi \circ \sigma \neq \sigma' \circ e_{\pi'}$ pro všechny $\sigma' \in \tilde{\mathcal{K}}_2$ a $\pi' \in \tilde{\mathcal{K}}_3$ (e je šifrovací zobrazení permutační šifry, v tomto případě tedy $\tilde{e}_3$).
Totiž pro složení $e_\pi \circ \sigma$ platí $I_{e_\pi \circ \sigma,\, \pi(s)} = I_{\sigma,s}$. Tedy $I_{e_\pi \circ \sigma,\, \pi(s)} \cap I_{e_\pi \circ \sigma,\, \pi(s')} \neq \emptyset$. Naopak pro složení $\sigma' \circ e_{\pi'}$ platí $I_{\sigma' \circ e_{\pi'},\, z} = \pi'^{-1}(I_{\sigma',z})$. Indexy $\pi(s)$ a $\pi(s')$ leží v různých S-boxech, takže musí platit $I_{\sigma',\pi(s)} \cap I_{\sigma',\pi(s')} = \emptyset$. Dostáváme $I_{\sigma' \circ e_{\pi'},\, \pi(s)} \cap I_{\sigma' \circ e_{\pi'},\, \pi(s')} = \emptyset$. Zobrazení $e_\pi \circ \sigma$ a $\sigma' \circ e_{\pi'}$ se tedy nemohou rovnat. □