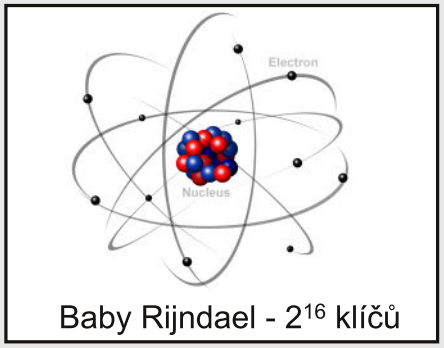
Kryptoanalýza šifry Baby Rijndael

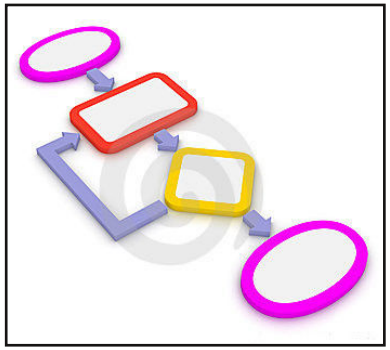
Josef Kokeš

Transformace zachovávající operace a požadované vlastnosti



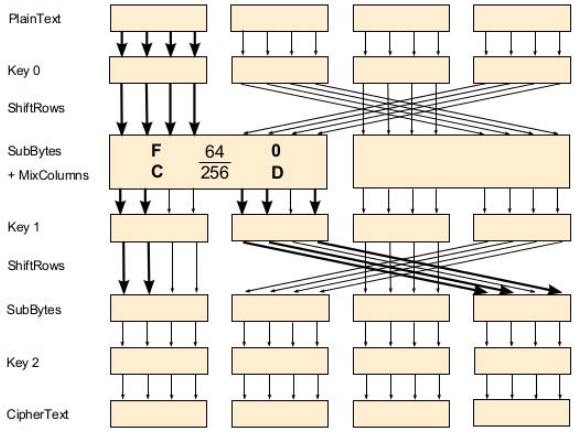
Baby Rijndael - 2^{16} klíčů

Analýza lineárních vlastností šifry



Algoritmus pro tvorbu optimálních lineárních aproximací

Ověření všech kombinací hrubou silou



Lineární aproximace pro 2, 3, 4 rundy

Aplikace na všechny kombinace klíčů a šifrových textů

	aprox. A (obr. 5.6)
Průměrná pozice správného klíče	106,54
Směrodatná odchylka správného klíče	79,99
Medián pozice správného klíče	84
Modus pozice správného klíče	256
Nejlepší pozice správného klíče	1
Nejhorší pozice správného klíče	256
Očekávaný bias	0,00390625
Průměrný skutečný bias	0,004047
Směrodatná odchylka skutečného biasu	0,002407

Dosažené výsledky

- 2 rundy - plně prolomeny
- 3 rundy - nalezena závislost mezi klíčem a schopností ho najít => možná slabina v expanzi klíče
- 4 rundy - jen mírné zlepšení vůči náhodě; zjištěna existence vztahu mezi počtem aktivních bitů a úspěšností prolomení

1) Rijndael je mnohonásobně větší, úspěšnost jeho prolomení nebude větší než u Baby Rijndael
2) identifikována potenciální slabá místa, vhodná pro další analýzu