Zadání semestrální práce Y2KK/ZS 2010

Téma: Symetrické blokové šifry Skipjack a Serpent

Na konci 90. let odtajnila americká NSA po sérii výrobních neúspěchů šifrovacího hardware svoji šifru označovanou kódem *Skipjack*. Tato šifra je první veřejně analyzovatelnou symetrickou blokovou šifrou z dílny NSA.

Jedním z neúspěšných finalistů volby nového algoritmu AES byla šifra *Serpent*, kterou odborníci považují za konzervativnější a bezpečnější, než je současné AES/Rijndael (ovšem za ceny podstatně vyšší výpočetní složitosti).

Prozkoumejte blíže oba tyto algoritmy a porovnejte je s šiframi DES a AES. U obou uveďte popis rundové funkce a mechanismus přípravy dílčích rundových klíčů.

Rozsah zprávy: alespoň 10 stran včetně obrázků, dvanáctibodové písmo, řádkování 1.

Literatura:

1. `http://en.wikipedia.org/wiki/Skipjack_%28cipher%29`
2. Vladimír Klíma: Šifru v pytli neutajíš ... CHIP 1/1999, pp. 46–47. `http://crypto-world.info/klima/1999/chip-1999-01-46-47.pdf`
3. R. Chung-Wei Phan: Cryptanalysis of full Skipjack block cipher. IEEE Electronics Letters 38(2), pp. 69–71.
4. `http://en.wikipedia.org/wiki/Serpent_%28cipher%29`
5. Ross Anderson, Eli Biham, Lars Knudsen: SERPENT – A Candidate Block Cipher for the Advanced Encryption Standard. `http://www.cl.cam.ac.uk/~rja14/serpent.html`