Zadání semestrální práce Y2KK/ZS 2010

Téma: Symetrické blokové šifry Blowfish a Twofish

V době exportních omezení USA na šifrovací technologii DES a patentové ochrany dalších bezpečných šifer (RC5, IDEA) navrhl Bruce Schneier alternativní volně dostupný šifrovací algoritmus, jenž nazval *Blowfish*. Nástupce tohoto algoritmu s kódovým názvem *Twofish* byl jedním z finalistů soutěže na výběr algoritmu šifry AES.

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/Blowfish_%28cipher%29`
2. Bruce Schneier: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), `http://www.schneier.com/paper-blowfish-fse.html`
3. Vincent Rijmen: Cryptanalysis and Design of Iterated Block Ciphers. Ph.D. thesis, KU Leuven, 1997. `http://www.cosic.esat.kuleuven.be/publications/thesis-4.ps`
4. `http://en.wikipedia.org/wiki/Twofish`
5. Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson: The Twofish Encryption Algorithm. 1998. `http://www.schneier.com/paper-twofish-paper.html`
6. David Wagner: Better algorithm: Rijndael or TwoFish? USENET discussion group sci.crypt, 2004. `http://groups.google.com/group/sci.crypt/browse_thread/thread/7834ad13db22e207/6f6e157149330057`