Kryptografia i bezpieczeństwo

Laboratorium - lista nr 11, do 29 I

Zadanie 1 (10 pkt) Zmodyfikuj implementację RSA (z listy 8), aby była odporna na timing-attacks. Wykonaj to na oba sposoby:

1. poprzez maskowanie (a'la blind signatures – zobacz [Koc96]),
2. poprzez modyfikację implementacji na "constant-time" (zobacz [Por, Sch, GGO$^+$])

Zadanie 2 (10 pkt) Przygotuj politykę bezpieczeństwa dla (do wyboru): produktu, który realizujesz na programowaniu zespołowym (możecie przygotować wspólnie jeden dokument); dla legitymacji studenckiej (pamiętać należy o warstwie wizualnej i elektronicznej).

Literatura

[GGO$^+$] Vinodh Gopal, James Guilford, Erdinc Ozturk, Wajdi Feghali, Gil Wolrich, and Martin Dixon. Fast and constant-time implementation of modular exponentiation. `https://www.cse.buffalo.edu/srds2009/escs2009_submission_Gopal.pdf`.

[Koc96] Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. pages 104–113. Springer, Berlin, Heidelberg, 1996.

[Por] Thomas Pornin. BearSSL a smaller SSL/TLS library. `https://www.bearssl.org/ctmul.html`.

[Sch] Peter Schwabe. Timing attacks and countermeasures. `http://summerschool-croatia.cs.ru.nl/2016/slides/PeterSchwabe.pdf`.