Kodowanie i bezpieczeństwo

Laboratorium - lista nr 7, 17 XII

Zadanie 1 (10 pkt) Zaimplementuj przedstawiony na wykładzie *timing attack* [1] na program z poprzedniej listy.

Zadanie 2 (5 pkt) Zmodyfikuj działanie programu z poprzedniej listy. Serwer ma nie wykonywać operacji na dostarczonym ciągu x, zamiast tego ma wylosować $r \in Z_N^*$, obliczyć $y = (rx)^d \bmod N$ i zwrócić jako odpowiedź: $yr^{-1} \bmod N$.

Sprawdź jak teraz wyglądają statystyki (w zadaniu 1).

Zadanie 3 (5 pkt) Zmodyfikuj działanie programu z poprzedniej listy. Zadbaj o to, aby była to implementacja typu *constant-time* [2].

Sprawdź jak teraz wyglądają statystyki (w zadaniu 1).

Literatura

[1] Paul C Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Annual International Cryptology Conference*, pages 104–113. Springer, 1996.

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