Lista Nr 06, laboratorium

(wyk. 10 XII 09 r.)

1. Dla własnych liczb `rsa_p`, `rsa_q`, `e` oraz pliku `rsa_naFin` „przećwiczyć" działanie programu z wykładu Nr 11[1].

2. Jakie znaczenie ma dyrektywa preprocesora[2] `RSA_HEX`. Czy bezpiecznie jest założyć, że `sizeof(int)` wynosi `4` ?

3. Napisać program, który dla danego klucza publicznego (e, n) wyznaczy klucz prywatny (d, n).

4. Na podstawie znajomości klucza publicznego (e, n) rozszyfrować dany plik[3].

Wrocław, dnia 21/12/2009

[1] http://127.0.1.1/ tabisz/WIP/doxy-03/index.html

[2] http://www.cppreference.com/wiki/preprocessor/start

[3] Klucz publiczny jak i odpowiednio zaszyfrowany plik może być dostarczony przez prowadzącego laboratorium lub studenci zostaną podzieleni w pary do przećwiczenia *„łamania szyfru"*