---

# DOKUMENTÁCIA [OpenSSL] – Študijné materiály

---

**Autor:** Martin Janitor

**Bakalárska práca:** RSA s výplňovou schémou OAEP

**Dátum:** 05.06.2022

**Verzia:** 1.0

---

## Štruktúra projektu s využitím kryptografickej knižnice OpenSSL:

**OPENSSL**

|---------- Makefile

|---------- test01.c

|---------- test02.c

|---------- test05.c

|---------- test06.c

---

## OPIS KRYPTOGRAFICKEJ KNIŽNICE OpenSSL

---

**Link na pôvodnú implementáciu:** https://www.openssl.org/source/

Kryptografická knižnica OpenSSL využíva sofistikované metódy na realizáciu a vykonávanie kryptografických algoritmov. Je optimalizovaná pre viacero operačných systémov a využíva sa v praxi na bezpečný prenos dát v komunikačnom kanáli. Knižnica obsahuje hlavičkový súbor **openssl/rsa.h** v ktorom sú implementované potrebné funkcie pre realizovanie šifrovacieho algoritmu RSA v spojení s výplňovou schémou OAEP.

Formát reprezentujúci BN číslo:

```
struct bignum_st {
        BN_ULONG *d;
        int top; /* Index of last used d +1. */
        int dmax; /* Size of the d array. */
```

```
    int neg; /* one if the number is negative */
    int flags;
};
```

---

## TESTY

---

**test01** Testuje overenie správnosti výpočtu matematickej operácie modulárneho umocnenia m^e mod n.

**test02** Generuje RSA kľúče [1024, 2048, 4096 bitov] a šifruje správy s využitím RSA a výplňovej schémy OAEP + meranie času šifrovania a dešifrovania.

**test05** Generuje RSA kľúče [1024, 2048, 4096 bitov] + meranie času generovania kľúčov.

**test06** Meranie času šifrovanie + dešifrovanie s využitím výplňovej schémy OAEP.

---

## MAKEFILE

---

Pre efektívnu kompiláciu zdrojových súborov s využitím knižnice OpenSSL bol vytvorený súbor Makefile. Makefile obsahuje preddefinované MAKRO **OpenSSL_PATH**, ktoré určuje umiestnenie knižnice OpenSSL pre operačný systém Windows. Štandardne sa OpenSSL knižnica nainštaluje do adresára **C:\Program Files\OpenSSL-Win64.** V súbore Makefile je potrebné nastaviť cestu k OpenSSL knižnici, pričom základné nastavenie v Makefile súbore je **C:/OpenSSL-Win64**. Knižnicu OpenSSL som prekopíroval do adresára **C:/OpenSSL-Win64** z dôvodu prístupových práv k adresáru Program Files.

### Kompilácia testu:

**make** test[ číslo testu ] príklad: **make** test02