
DOKUMENTÁCIA [KOKKE] – Študijné materiály

Autor: Martin Janitor

Bakalárska práca: RSA s výplňovou schémou OAEP

Dátum: 05.06.2022

Verzia: 1.0

Štruktúra kryptografickej knižnice KOKKE:

KOKKE

|---------- bnc

|---------- bn.h

|---------- changes.txt

|---------- source.txt

EXTENSIONS_KOKKE

|---------- **include**

|---------- ext_file.h

|---------- ext_rsa.h

|---------- **src**

|---------- ext_file.c

|---------- ext_rsa.c

|---------- **TESTS**

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

|---------- test_vect.c

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

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

|---------- rsa_private_1024

|---------- rsa_public_1024

|---------- rsa_private_2048

|---------- rsa_public_2048

|---------- rsa_private_4096

|---------- rsa_public_4096

OPIS KRYPTOGRAFICKEJ KNIŽNICE KOKKE

Link na pôvodnú implementáciu: https://github.com/kokke/tiny-bignum-c

Kryptografická knižnica KOKKE obsahuje algoritmus pre výpočet modulárneho umocnenia s veľkými číslami, ktorý sa využíva v RSA algoritme. Knižnica primárne nedisponuje generovaním RSA kľúčov. Pre realizáciu šifrovania a dešifrovania v rámci RSA algoritmu som implementoval funkcie, ktoré dôkazu načítavať RSA kľúče zo súborov vo špecifickom formáte, ktorý bol opísaný v dokumentácii ku kryptografickej knižnici STUDENT. Pre vhodné aplikovanie RSA algoritmu je nutné vygenerovať RSA kľúče knižnicou STUDENT a následne ich využiť v knižnici KOKKE, ktoré je priamo optimalizovaná pre takýto formát. Implementácia obsahuje aj možnosť využitia výplňovej schémy OAEP v spojení s RSA algoritmom. Implementácia výplňovej schémy OAEP sa nachádza v adresári /OAEP. Implementácia výplňovej schémy OAEP využíva hashovacie funkcie SHA-1, SHA-256 a SHA-512, ktoré sú implementované v adresári /HASH.

Formát reprezentujúci BN číslo:

```
struct bn {
    DTYPE array[ BN_ARRAY_SIZE ];
};
```

Typ **DTYPE** je definovaný v súbore bn.h a definuje s akou šírkou slova sa budú vykonávať matematické operácie. Sú dostupné tri typy (1, 2 a 4 bajty). Základnou hodnotou pre **DTYPE** je hodnota 4.

OPIS SÚBOROV

---

bn.c, bn.h

- Implementácie základných matematických operácii s využitím veľkých čísel.
- Funkcie na konverizu a porovnanie veľkých čísel.

ext_file.c, ext_file.h

- Pridanie funkcií pre prácu so súbormi.
- Načítavanie RSA kľúčov zo súboru.
- Načítavanie a zápis správy do súboru.

ext_rsa.c, ext_rsa.h

- Implementácia funkcií pre šifrovanie a dešifrovanie s využitím algoritmu RSA.
- Využitie implementácie výplňovej schémy OAEP z projektu, ktorý je realizovaný v adresári **/OAEP**.

changes.txt - Opis zmien v bn.h .

source.txt - Odkaz na pôvodnú implementáciu.

TESTY

---

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

test02 Načíta 1024-bitové RSA kľúče zo súboru. Zašifruje a dešifruje správu s využitím RSA a výplňovej schémy OAEP + meranie času šifrovania a dešifrovania. Taktiež overí pôvodnú správu s dešifrovanou správou.

test03 Načíta 2048-bitové RSA kľúče zo súboru. Zašifruje a dešifruje správu s využitím RSA a výplňovej schémy OAEP + meranie času šifrovania a dešifrovania. Taktiež overí pôvodnú správu s dešifrovanou správou.

test04 Načíta 4096-bitové RSA kľúče zo súboru. Zašifruje a dešifruje správu s využitím RSA a výplňovej schémy OAEP + meranie času šifrovania a dešifrovania. Taktiež overí pôvodnú správu s dešifrovanou správou.

test_vect Otestovanie RSA + OAEP s testovacími vektormi dostupných na stránke [https://www.inf.pucrs.br/~calazans/graduate/TPVLSI_I/RSA-oaep_spec.pdf] . Požadovane RSA kľúče sú načítavane zo súborov.

MAKEFILE

Vopred preddefinované MAKRA (možnosť využitia pri testoch)

- **DPRINT** [Výpis jednotlivých elementov pri generovaní RSA kľúčov, šifrovaní a dešifrovaní. Napríklad: prvočísla p a q, modulus ...]
- **DTEST_VECT** [Pridanie do projektu testovacie vektory, ktoré sú zadané „napevno“ a sú priradené pri kompilácií projektu, ak je vopred zadefinované makro TEST_VECT.

  Testovacie vektory: https://www.inf.pucrs.br/~calazans/graduate/TPVLSI_I/RSA-oaep_spec.pdf]

- **DMOD_LEN=[NUMBER]** [Definuje maximálnu veľkosť statického poľa pre uloženie BN čísla. Napríklad zadefinovaním MAKRA DMOD_LEN=1024, definujeme dĺžku statického poľa 1024 bitov. Maximálne číslo uložené v tejto premennej bude dosahovať hodnotu 2^1024 – 1.]
- **TEST_VECTOR_PRINT** [Spojenie MAKIER DTEST_VECT a DPRINT]

Kompilácia testu:

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