
DOKUMENTÁCIA [MCRYPTO] – Študijné materiály

Autor: Martin Janitor

Bakalárska práca: RSA s výplňovou schémou OAEP

Dátum: 05.06.2022

Verzia: 1.0

Štruktúra kryptografickej knižnice MCRYPTO:

MCRYPTO

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

|---------- bigdigits.h

|---------- hash.h

|---------- mcrypto.h

|---------- md5.h

|---------- pkcs1-rsa.h

|---------- sha1.h

|---------- sha2.h

|---------- **src** [ZDROJOVÉ SÚBORY PRE MATEMATICKÉ OPERÁCIE +

KÓDOVANIE V RADIX-64 FORMÁTE + RSA A OAEP IMPLEMENTÁCIA]

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

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

EXTENSIONS_MCRYPTO

|---------- extensions_mcrypto.c

|---------- extensions_mcrypto.h

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

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

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

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

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

|---------- test03.c

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

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

OPIS KRYPTOGRAFICKEJ KNIŽNICE MCRYPTO

Link na pôvodnú implementáciu: https://code.google.com/archive/p/libmcrypto/downloads

Kryptografická knižnica MCRYPTO obsahuje implementáciu šifrovacieho algoritmu RSA s výplňovou schémou OAEP. Testovanie prvočíselnosti je realizované pomocou Miller-Rabinovho testu prvočíselnosti s parametrom **t = 200**, ktorý určuje počet iterácii testu prvočíselnosti.

Pôvodná implementácia obsahuje aj šifrovací algoritmus s využitím eliptických kriviek, Galoisové polia.

Knižnica obsahuje možnosť výberu pre generovanie náhodných čísel. V súbore mcrypto.h sa nachádza MAKRO **STRONG_RANDOM**, ktoré ma základné nastavenie na hodnotu 1. hodnota je znamená využitie generovania kryptograficky bezpečných náhodných čísel. Hodnota 0 znamená generovanie pseudonáhodných čísel s využitím funkcie rand().

Knižnica realizuje generovanie kryptograficky bezpečných náhodných čísel:

- Operačný systém Windows: využitá je funkcia rand_s()
- Operačný systém Linux: náhodné čísla sú načítavané zo súboru /dev/urandom

Formát reprezentujúci BN číslo:

```
#define MAX_DIG_LEN 64                /* 2048 bits */

typedef uint32_t DIGIT_T;

DIGIT_T BN_NUM[ MAX_DIG_LEN ];
```

OPIS SÚBOROV

---

bigdigits.h

- Matematické operácie s BN číslami, zadefinovanie typu pre veľkosť vektora v poli.

mcrypto.h

- Definície generátorov náhodných čísel.

md5.h, sha1.h, sha2.h, hash.h

- Implementácie hashovacích funkcií.

pkcs1-rsa.h

- Šifrovací algoritmus RSA s výplňovou schémou OAEP.

extensions_mcrypto.c, extensions_mcrypto.h

- Zápis RSA kľúča do súboru.
- Definícia štruktúry súboru pre zápis RSA kľúčov, zápis načítanie správy zo súboru.

changes.txt - Opis vykonaných zmien v mcrypto.h, bigdisits.h.

source.txt - Odkaz na pôvodnú implementáciu.

TESTY

---

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

test02 Generuje RSA kľúč 1024 bitov a šifruje správu s využitím RSA a výplňovej schémy OAEP + meranie času šifrovania a dešifrovania.

test03 Generuje RSA kľúč 2048 bitov a šifruje správu s využitím RSA a výplňovej schémy OAEP + meranie času šifrovania a dešifrovania.

test04 Generuje RSA kľúč 4096 bitov a šifruje správu 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.

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

MAKEFILE

Vopred preddefinované MAKRA (možnosť využitia pri testoch)

- **DMCRYPTO_DEBUG** [Výpis jednotlivých elementov pri generovaní RSA kľúčov, šifrovaní a dešifrovaní. Napríklad: prvočísla p a q, modulus, zašifrovaná správa, dešifrovaná správa]
- **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.]
- **DEBUG_INF** [Spojenie MAKIER DTEST_VECT a DMCRYPTO_DEBUG]

Kompilácia testu:

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

FORMÁTY PRE NAČÍTANIE A ZÁPIS DO SÚBOROV

FORMÁT (správa):

1. Hlavička: **----------BEGIN MSG----------** .

2. Dĺžka správy: [ČÍSLO]
3. Postupnosť čísel reprezentujúca BN číslo: MSB bajt správy .... LSB bajt správy zakódovane v radix-64 formáte.
4. Päta: **----------END OF MSG---------- .**

FORMÁT (RSA kľúče):

1. Hlavička**: ----------BEGIN PKCS#1 SECRET KEY----------** (pre súkromný kľúč) alebo **----------BEGIN PKCS#1 PUBLIC KEY----------** (pre verejný kľúč).
2. Dĺžka BN čísla modulusu n: [číslo]. Napríklad pre 2048 bitový modulus je dĺžka 2048/32= 64. Konštanta 32 definuje počet bitov pre uloženie jedného vektora do statického poľa v jazyku C.
3. Postupnosť čísel reprezentujúca BN číslo (modulus): MSB bajt .... LSB bajt zakódovane v radix-64 formáte.
4. Postupnosť čísel reprezentujúca BN číslo (verejný exponent): MSB bajt .... LSB bajt zakódovane v radix-64 formáte.
5. V prípade zápisu súkromného kľúča je zapísaný do súboru aj súkromný exponent d. Postupnosť čísel reprezentujúca BN číslo (súkromný exponent): MSB bajt .... LSB bajt zakódovane v radix-64 formáte.
6. Päta: **----------BEGIN PKCS#1 PUBLIC KEY----------** (verejný kľúč) alebo **----------END OF PKCS#1 SECRET KEY----------** (súkromný kľúč).