
DOKUMENTÁCIA [HASH] – Študijné materiály

Autor: Martin Janitor

Bakalárska práca: RSA s výplňovou schémou OAEP

Dátum: 05.06.2022

Verzia: 1.0

Štruktúra projektu s hashovacími funkciami:

HASH

|---------- **EXTENSIONS**

|---------- ext_sha.c

|---------- ext_sha.h

|---------- **SHA_1**

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

|---------- sha1.c

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

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

|---------- **SHA_256**

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

|---------- sha256.c

|---------- sha256.h

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

|---------- **SHA_512**

|---------- fixedint.h

|---------- sha512.c

|---------- sha512.h

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

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

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

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

OPIS IMPLEMENTÁCIE HASHOVACÍCH FUNKCIÍ

Link na pôvodnú implementáciu:

- SHA-1, SHA-256: https://github.com/B-Con/crypto-algorithms
- SHA-512: https://github.com/orlp/ed25519

Porovnanie hashovacích funkcií:

HASHOVACIE FUNKCIE			
	SHA-1	SHA-256	SHA-512
Výstup v bitoch	160	256	512
Dĺžka správy v bitoch	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$
Dĺžka slova v bitoch	32	32	64

OPIS SÚBOROV

---

sha1.c, **sha1.h**

- Zdrojové súbory pre hashovaciu funkciu SHA-1.

sha256.c, **sha256.h**

- Zdrojové súbory pre hashovaciu funkciu SHA-256.

sha512.c, **sha512.h**, **fixedint.h**

- Zdrojové súbory pre hashovaciu funkciu SHA-512.

TESTOVANIE HASHOVACÍCH FUNKCIÍ

V rámci testovania hashovacích funkcií bol vytvorený test, ktorý realizuje korektnosť výpočtu hashovacích funkcií. Testovacie vektory pre realizáciu testu sú dostupné na stránke: https://www.di-mgt.com.au/sha_testvectors.html

test01 Overenie korektnosti hashovacích funkcií pomocou testovacích vektorov.

Kompilácia testu (pomocou vopred pripraveného Makefile súboru):

make test01