
DOKUMENTÁCIA [OAEP] – Študijné materiály

Autor: Martin Janitor

Bakalárska práca: RSA s výplňovou schémou OAEP

Dátum: 05.06.2022

Verzia: 1.0

Štruktúra projektu OAEP:

OAEP

|---------- oaep.c

|---------- oaep.h

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

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

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

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

OPIS IMPLEMENTÁCIE OAEP

Link na pôvodnú implementáciu: https://github.com/Rupan/rsa

Implementácia realizuje šifrovanie s využitím výplňovej schémy OAEP, ktorá je definovaná v štandarde RFC 8017, ktorý je dustupný na stránke: https://datatracker.ietf.org/doc/html/rfc8017#section-7.1

Pôvodná implementácia bola rozšírená o hashovacie funkcie z projektu HASH.

Opis súborov

---

oaep.c, **oaep.h**

- Implementácia funkcií pre OAEP, šifrovanie a dešifrovanie.

changes.txt - Popis zmien v oaep.h oaep.c

source.txt - Odkaz na pôvodnú implementáciu.

TEST NA OVERENIE VÝPLŇOVEJ SCHÉMY OAEP

---

test01 Realizuje šifrovanie a dešifrovanie s využitím výplňovej schémy OAEP + meranie času procesu šifrovania a dešifrovania.

Kompilácia testu (pomocou vopred pripraveného Makefile súboru):

make test01