Za projekat iz Zaštite informacija implementiraćete 4 kripto algoritma i 4 dodatne metode.

Iz svake grupe radićete po jedan zadatak čiji je broj jednak (broj_indeksa) % 5 + 1 (npr. moj broj indeksa je bio 9479 i za mene bi to izgledalo ovako 9479 % 5 + 1 = 5)

Zadaci A1-A4 vrede po 4 poena. Zadaci B1-B3 vrede po 3 poena, a zadatak B4 vredi 5 poena.

Za svaki od algoritama implemetirati metodu za kriptovanje i metodu za dekriptovanje.

Algoritmi treba da kriptuju fajl (tekstualni ili binarni, u zavisnosti od konstrukcije algoritma) i rezultat treba da bude takodje fajl. Algoritmi treba da budu u stanju da dekriptuju kriptovani fajl i kao rezultat daju fajl identičan polaznom koji se može otvoriti iz iste aplikacije.

Kao dodatak treba implementirati i metodu za kriptovanje 24-bitnih BMP fajlova. Kriptovani fajl treba da bude takav da može da se otvori iz nekog od programa za obradu slike. U svakoj kategoriji postoji bar jedan algoritam koji je prikladan da se upari sa ovom metodom.

Sledeći korak je implementacija crypto hash funkcije koju ćete koristiti da uporedite polazni fajl i fajl koji je rezultat dekriptovanja.

Na kraju, probaćete da paralelizujete čitanje, kodiranje i upis u kodirani fajl koristeći više paralelnih niti (čiji broj ćete proslediti kao parametar funkcije), za jedan od algoritama iz A1-A4 po vašem izboru.

Zadatak A1

1. One-time-pad
2. A5/2
3. RC6
4. A5/1
5. RC4

Zadatak A2

1. Foursquare cipher (http://practicalcryptography.com/ciphers/four-square-cipher/
2. Railfence cipher (https://web.archive.org/web/20120105152732/http://cryptogram.org/cdb/aca.info/aca.and.you/chapter_09.pdf#RAILFE)
3. Bifid (http://practicalcryptography.com/ciphers/classical-era/bifid/)
4. Playfair cipher (https://www.geeksforgeeks.org/playfair-cipher-with-examples/ )
5. Enigma (http://practicalcryptography.com/ciphers/mechanical-era/enigma/)

Zadatak A3

1. XXTEA
2. XTEA
3. Knapsack
4. RSA
5. TEA

Zadatak A4 (mod kodera primenjen na bilo koji od algoritama)

1. OFB
2. PCBC
3. CTR
4. CFB
5. CBC

Zadatak B1 (primenjivo na A1-A4)

Metoda za učitavanje niza bajtova/karaktera iz fajla.

Metoda za upis niza bajtova/karaktera u fajl.

Zadatak B2 (primenjivo na A1-A4)

Metoda za učitavanje podataka iz BMP 24-bit slike.

Metoda za kreiranje 24-bit BMP slike kao rezultat kriptovanja.

Zadatak B3 (crypto hash za proveru validnosti fajla)

1. SHA1
2. MD5
3. Tiger hash
4. SHA2
5. CRC

Zadatak B4 (25.12.2020)

Paralelizacija učitavanja, upisa i kriptovanja.