**Laboratorijska vežba 3: Knapsack i RSA**

|  |  |
| --- | --- |
|  |  |

**Poštovani studenti**,

Na ovoj stranici su prikazani zadaci za treću (od četiri) laboratorijsku vežbu. Ponovo ćete imati šest zadataka od kojih se tri se bave Knapsack, a tri RSA algoritmom.

Takođe, nismo izgubili entuzijazam u smišljanju interesantnih načina za određivanje rednog broja zadatka koji treba da radite. Naravno.

E, pa ovako. Uzmite vaš redni broj u grupi i vaš broj indeksa i označite ih sa r i b respektivno.

Ukoliko niste upisani ni u jednu grupu, r = b mod 23.

Ukoliko je r deljivo sa 7, uvećajte ga za 1.

Ukoliko je r < 8, onda r uvećajte za 7; a ako je r > 10, onda ga umanjite za 4. Nakon toga, redni broj zadatka, označite ga sa z, koji radite izračunaćete po formuli:

**z = rb mod 7**

Ukoliko dobijete z = 0, onda radite prvi zadatak.

Loše određen broj vežbe koju treba raditi povlači gubitak dva poena (od 5).

**Zadaci:**

1. Knapsack. Napisati kod koji služi za generisanje ključeva, kodovanje i dekodovanje po ovom algoritmu. Korisnik treba da zada prvi član supperrastućeg niza kao i broj članova niza, a da program na osnovu njega predloži neki superrastući niz i generiše ključ po Knapsack algoritmu. Ukoliko korisnik želi, može da promeni broj članova niza, u tom slučaju program treba da preračuna ključeve, M i N ponovo (ako je nova dimenzija niza manja od početne program samo treba da odbaci nepotrebne članove).  Treba omogućiti korisniku da može da promeni i svaki od članova niza pojedinačno, i u tom slučaju takođe treba preračunati ključeve.

1. Knapsack. Napisati kod koji za zadati superrastući niz, M i N  računa javni i privatni ključ po Knapsack algoritmu, i koji je u stanju da kriptuje i dekriptuje bilo kakve fajlove po ovom algoritmu. Fajl učitati kao niz bajtova. Rezultat kodiranja upisati u tekstualni fajl kao niz celih brojeva odvojenih blanko znakom. Pomenuti tekstualni fajl početi ekstenzijom kodiranog fajla praćenom blanko znakom kako bi mogao ispravno da se dekodira. Kod dekodiranja učitati tekstualni fajl koji sadrži kodovane podatke, napraviti novi fajl sa odgovarajućom ekstenzijom i u njega upisivati dekodovane podatke bajt po bajt.

1. Knapsack. Napisati kod koji za zadati superrastući niz, M i N  računa javni i privatni ključ po Knapsack algoritmu, i koji je u stanju da kriptuje i dekriptuje bilo kakve fajlove po ovom algoritmu. Fajl učitati kao niz bajtova (M-ovi). Rezultat svakog kodiranja (C), kovertovati u niz bajtova i upisati u izlazni fajl. Kod dekodiranja učitati kodirani fajl, transformisati odgovarajuće grupe bajtova u odgovarajuće C vrednost i onda njih dekodovati u upisati u fajl.

1. RSA. Napisati kod koji za zadato p, q i e, računa javni i privatni ključ po RSA algoritmu, i koji je u stanju da kriptuje i dekriptuje bitmap fajlove (\*.bmp). Vrednosti p i q unositi tako da dobijeno N bude manje od 256. Bitmap sliku učitati iz fajla kao niz bajtova, a rezulata kodovanja upisati u drugi fajl. Kod učitavanja bitmap slike voditi računa o sledećem:
   1. bitmap slike imaju na početku fajla zaglavlje, koje NE treba kodirati već samo prepisati u izlazni fajl
   2. kodirati samo bajtove koji definišu sliku
   3. ako učitavate bajtove jedan po jedan iz bitmap fajla obeležavajući njihove redne brojeve sa 0, 1, 2 itd, bajtovi sa rednim brojevima 10, 11, 12 i 13 nam trebaju da odredimo mesto odakle počinju bajtovi koji nose informaciju o slici na sledeći način:

            long pos = bajt[10] 256 \* (bajt[11] 256 \* (bajt[12] 256 \* bajt[13]));

Dakle, ako brojač učitanih bajtova obeležimo sa i, za i < pos, samo upisujemo bajtove u izlazni fajl, dok u suprotnom ih kodujemo pa upisujemo.

            Isto pravilo važi i za dekodiranje.

1. RSA u CBC modu. Napisati kod koji za zadato p, q i e, računa javni i privatni ključ po RSA algoritmu, i koji je u stanju da kriptuje i dekriptuje bilo kakve fajlove po RSA algoritmu u CBC modu. Fajl učitati kao niz bajtova. Rezultat kodiranja upisati u tekstualni fajl kao niz celih brojeva odvojenih blanko znakom. Pomenuti tekstualni fajl početi ekstenzijom kodiranog fajla praćenom blanko znakom kako bi mogao ispravno da se dekodira. Kod dekodiranja učitati tekstualni fajl koji sadrži kodovane podatke, napraviti novi fajl sa odgovarajućom ekstenzijom i u njega upisivati dekodovane podatke bajt po bajt.

1. RSA u CTR modu. Napisati kod koji za zadato p, q i e, računa javni i privatni ključ po RSA algoritmu, i koji je u stanju da kriptuje i dekriptuje bilo kakve fajlove po RSA algoritmu u CTR modu. Fajl učitati kao niz bajtova (M-ovi). Rezultat svakog kodiranja (C), kovertovati u niz bajtova i upisati u izlazni fajl. Npr, za N = 777, svaki početni bajt biće kodiran sa dva bajta.Kod dekodiranja učitati kodirani fajl, transformisati odgovarajuće grupe bajtova u odgovarajuće C vrednost i onda njih dekodovati u upisati u fajl.