# Implementacija RSA algoritma

U postavci zadatka je implementirano segmentovanje i en(de)kodovanje teksta. Zadatak je dodati funkcionalnost kako bi se postiglo enkriptovanje i dekriptovanje tekstualne datoteke. Pre toga je neophodno generisati javni i privatni ključ kojima će se vršiti kriptografke operacije. Neki delovi algoritma koji nisu vezani za kriptografiju su već implementirani:

- generisanje prostih brojeva (generate_primes)
- računanje najmanjeg zajedničkog sadržalaca (calculate_lcm)
- računanje najvećeg zajedničkog delilaca (calculate_gcd)
- računanje inverzne modularne multiplikacije (inverse)

## 1. Implementacija generisanja ključeva

Proširiti funkciju `make_key_pair` tako da vrati objekte klasa `PublicKey` i `PrivateKey` koji zajedno čine uređeni par RSA ključeva.

Algoritam za generisanje ključeva:

1. Izabrati dva prosta broja $p$ i $q$ tako da vazi:
   - $n = p * q$
   - $n\_min < n < n\_max$
2. $l$ je NZS od $p - 1$ i $q - 1$
3. Izabrati $e$, tako da je $3 \leq e < l$ i da su $e$ i $l$ uzajamno prosti (NZD je 1)
4. $d = e^{-1} \bmod l$ (inverzna modularna multiplikacija)

## 2. Implementacija enkripcije i dekripcije

Proširiti funkcije `encrypt` i `decrypt` implementacijom odgovarajućih kriptografskih operacija. Operacije enkripcije i dekripcije se vrše slično, sa razlikom da se koriste različiti eksponenti.

Parametri funkcije `encrypt` su objekat klase `PublicKey` i segment teksta koji se enkriptuje. Kod `decrypt` funkcije, javni ključ je zamenjen privatnim.

Za enkripciju se koristi $e$ kao eksponent:

$$c = m^e \bmod n$$

Za dekripciju se koristi $d$:

$$m = c^d \bmod n$$

## Testiranje

Nakon što se skripta pokrene, na ulazu se očekuje komanda. Dozvoljene komande su genkey, encrypt i decrypt.

**Genkey**

Komanda za generisanje para ključeva koja nakon toga očekuje dužinu ključa u bitovima. Preporučena vrednost je 48. Veće vrednosti troše velike količine memorije.

**Encrypt/Decrypt**

Komande za kriptografijske operacije dodatno očekuju imena ulazne i izlazne datoteke. Kao primer uz zadatak postoji datoteka input sa kojom se može testirati program.