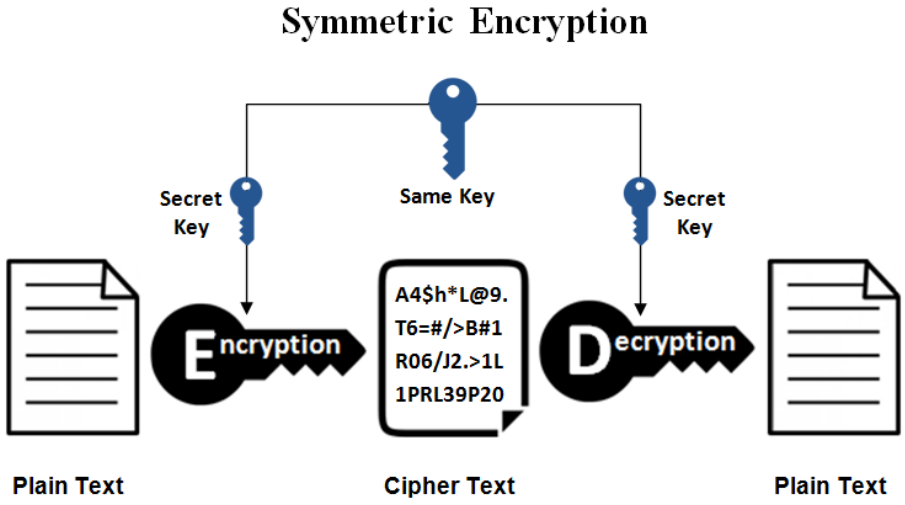
1. <u>Kriptografija, simetrična i asimetrična</u>

Kriptografija je metoda korišćenja viših matematičkih principa za prenos i skladištenje podataka u odredjenoj fromi tako da samo oni koja su ti podaci namenjeni mogu ih procesovati i čitati.

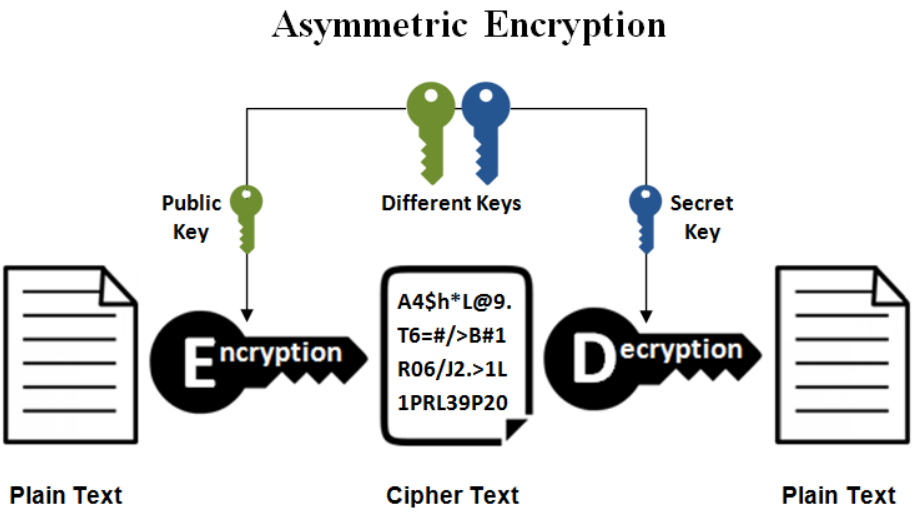
Enkripcija je ključan pojam u kriptografiji - to je proces gde se neka poruka enkoduje u formatu takvomda neko ko prisluškuje ne može da ga čita. Dekripcija je proces gde se neka enkodovana poruka prevodi u nama čitljivu formu podataka.

<u>Simetrična kriptografija</u> je jednostavan vid kriptografije, koji koristi samo jedan ključ da šifruje i dešifruje podatke. AES, Blowfish, RC4, DES, RC5 i RC6 su neki algoritmi simetrične enkripcije.



<u>Asimetrična kriptografija</u> je složeniji i noviji vid kriptografije, koji koristi 2 ključa prilikom šifrovanja i dešifrovanja. Jedan za šifrovanje, drugi za dešifrovanje.

Ovde umesto 2 tajna ključa, prilikom enkripcije se koristi javni ključ.



2. Kerckhoffs-ovi principi praktičnih šifratora

Kerckoffs-ov princip je ideja u kriptografiji, koju je Kerckoff razvio u 19om veku i koja glasi: "*Kriptosistem mora biti siguran čak i kada je sve u tom sistemu, osim ključa, poznato javnosti*".

Ostali principi su:

1. Sistem bi moralo biti praktično, čak i u nekim slučajevima matematički, nemoguće dešifrovati
2. Ne treba da zahteva tajne i ne treba da predstavlja problem ako padne u ruke nepoželjnih lica
3. Mora biti moguće komunicirati i zapamtiti ključ bez pisanja beleški, i korisnici sistema bi morali imati mogućnost da promene ili modifikuju ključ po želji
4. Mora imati mogućnost apliciranja na telegrafske komunikacije
5. Sistem mora da bude portabilan i ne sme zahtevati više ljudi da bi se upravljalo njime
6. Sistem mora biti lak za korišćenje koji ne zateva korisnike da prate ogroman set pravila

Neki od ovih principa sada su nebitni jer računari mogu da vrše kompleksnu enkripciju.

3. <u>Idealni šifrator</u>

Šest pravila koje je Kerckhoffs postavio se mogu, uz modernizaciju, primeniti na idealni šifrator:

1. Sistem bi moralo biti praktično, čak i u nekim slučajevima matematički, nemoguće dešifrovati
2. Ne treba da zahteva tajne i ne treba da predstavlja problem ako padne u ruke nepoželjnih lica
3. Mora biti moguće komunicirati i zapamtiti ključ bez pisanja beleški, i korisnici sistema bi morali imati mogućnost da promene ili modifikuju ključ po želji
4. Mora imati mogućnost apliciranja na telegrafske komunikacije
5. Sistem mora da bude portabilan i ne sme zahtevati više ljudi da bi se upravljalo njime
6. Sistem mora biti lak za korišćenje koji ne zateva korisnike da prate ogroman set pravila

4. <u>TLS/SSL protokol</u>

Transport Layer Security i njegov prethodnik Secure Socket Layer, su kriptografski protokoli koji pružaju sigurnost i integritet podataka za komunikaciju preko TCP/IP mreža, kao što je internet.

Nekoliko verzija protokola ima čestu primenu u web pretraživanju, e-mailu, instant porukama i voice-over-IP (VoIP).

TLS protokol omogućava komunikaciju preko mreže na takav način koji je dizajniran da spreči prisluškivanje. TLS koristi kriptografiju da bi obezbedio autentikaciju preko interneta.

5. <u>Kerberos protokol</u>

Kerberos protokol je mrežni autentikacioni protokol, koji dozvoljava ljudima koji komuniciraju preko nesigurne mreže da se medjusobno autentifikuju na siguran način. Dizajneri ovog protokola su ga namenili za client-server modele i on daje obostranu autentikaciju - i korisnik i server moraju identifikovati jedni druge. Poruke poslate kerberos protokolom su zaštićene od špijuniranja.

Kerberos koristi autentikaciju preuzete sa pouzdane treće strane koja deli kriptografske tajne pod pretpostavkom da paketi koji putuju nesigurnom mrežom mogu biti čitani, modifikovani i ubačeni. Kerberos gradi simetričnu kriptografiju.

6. <u>Šta je enkripcija, a šta dekripcija?</u>

Enkripcija je proces transformisanja originalne informacije u neprepoznatljiv i nečitljiv oblik. Ova nova forma informacije je potpuno drugačija od originalnog oblika. Enkripcija se obično vrši pomoću algoritma ključeva.

Dekripcija je proces transformisanja enkodovane/enkriptovane informacije u oblik koji je čitljiv ljudima ili računaru. Dekripcija se vrši tako što se "odenkriptuje" tekst manuelno ili korišćenjem ključa koji je korišćen pri enkriptovanju.

7.<u>Infrastruktura javnih ključeva (PKI sistem)</u>

Public Key Infrastructure (PKI) je set pravila, zakona, hardvera, softvera i procedura koje su potrebne da se kreiraju, održavaju, distribuiraju, koriste i izbacuju digitalni sertifikati i da se radi sa enkripcijom pomoću javnih ključeva.

Digitalni sertifikati se koriste da bi se ustanovilo da li neki javni ključ pripada nekom telu. PKI pravi digitalne sertifikate koji povezuju javne ključeve sa telima, bezbedno skladišti te sertifikate u centralnom direktorijumu i briše ih (izbacuje iz upotrebe) ako je potrebno.

PKI se sastoji iz:

- Autoriteta za sertifikate (CA) koji skladište, izdaju i potpisuju digitalne sertifikate
- Registracionog autoriteta (RA) koji verifikuje identitet tela koji zahtevaju da se njihovi digitalni sertifikati skladište u CA
- Centralni direktorijum, tj. mesto gde se skladište ključevi
- Sistem za menadžment sertifikata
- Pravilnik PKI

8. <u>Digitalni potpis</u>

Digitalni potpis ili šema digitalnog potpisa jeste tip asimetrične kriptografije. Za poruke koje se šalju kroz nesigurnu mrežu, dobra implementacija algoritma digitalnog potpisa bila bi ona koja primaoca "ubedjuje" da je poruka poslata od pravog pošiljaoca i tako poruki će se dati neko poverenje.

Digitalni potpisi koji su pravilno implementarini su mnogo teži za kopiranje od ručnih potpisa.

Digitalni potpisi imaju 2 algoritma:

- Potpisujući algoritam koji kao ulaz ima poruku i privatni ključ da bi izlaz bio potpis
- Verifikujući algoritam koji kada se kao ulaz uzme poruka, javni ključ i potpis, odlučuje da li će tu poruku odbaciti ili prihvatiti

9. HASH funkcija

HASH funckija je funkcija. Kada je kompjuterski program napisan, obično, velik0a količina podataka mora biti skladištena. Oni su obično smešteni u heš tabele. Da bi se podatak našao, računa se neka vrednost. Gleda se da podaci ne budu iste heš vrednosti.

Kriptografksa heš funkcija je heš funkcija koja uzima neku ulaznu vrednost (poruku) i kao izlaz daje neku vrednost fiksirane dužine bajtova. Idealna heš funckija ima 3 stavke:

- Ekstemno lako je izračunati heš za bilo koji podatak
- Ekstremno je teško kompjuterski izračunati hešovan alfanumerički tekst
- Ekstremno je retko da će dve različite poruke imati isti heš

Kriptografska heš funkcija bi se trebala ponašati što je nasumičnije moguće, a da je pri tome deteministička i komputabilna. Idealno, trebalo bi biti nemoguće naći dve poruke čiji je heš sličan, tadkoje, bilo bi poželjno da napadač ne nauči ništa od hešovanog dela poruke.

10. SHA algoritam

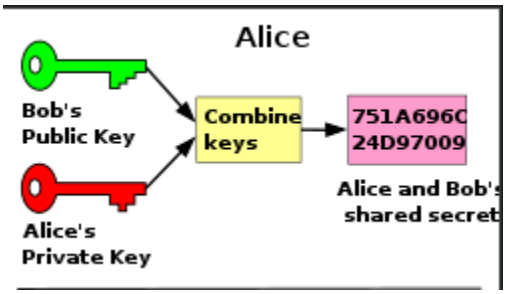
Secure Hash Algorithm (SHA) jeste porodica kriptografskih funkcija koju izdaje Nacionalni Institut Standarda i Tehnologije (NIST), postoji 4 vrste SHA algoritama i to:

- SHA-0: 160-bitna heš funkcija koja je objavljena u 1993. sa imenom "SHA", ubrzo je povučena iz upotrebe zbog nedostataka
- SHA-1: 160-bitna heš funkcija, koja je takodje imala otkrivene slabosti, nakon 2010. ovaj algoritam se više ne koristi
- SHA-2: Ovo je porodica 2 slična algoritma koji koriste različitu veličinu blokova, pa tako imamo: SHA-256 i SHA-512. SHA-256 koristi 32-bitne reči, dok SHA-512 koristi 64-bitne.
- SHA-3: Heš funkcija koja se zvala Keccak, je izabrana 2012. nakon javnog takmičenja izmedju ljudi koji nisu članovi NSA (National Security Agency). Struktura ovog algoritma odstupa dosta od SHA porodice, ali on podržava dužinu heša kao i SHA-2.

11. Diffie-Hellman-ov protokol za razmenu ključeva

Diffie-Hellman-ova razmena ključeva je metoda bezbednog razmenivanja kriptografskih ključeva preko javnih kanala i ovo je bio prvi protokol za javne ključeve. DH je jedan od najranijih praktičnih primena javne razmene ključeva implementirane u polju kriptografije. DH dozvoljava da 2 partije, koje nemaju ranije znanje jedna o drugoj, implementiraju jedan zajednički tajni ključ preko nesigurne mreže. Ovaj ključ može da se koristi da enkriptuje komunikaciju korišćenjem simetričnog šifratora.

DH se koristi da osigura razne usluge interneta, ali u oktobru 2015. nagovestilo se da parametri koje DH koristi nisu dovoljno jaki da spreče dobro finansirane napadače.



12. Šta je kriptoanaliza?

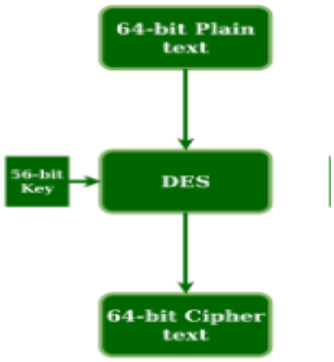
Kriptoanaliza je studija šifrovanog teksta, šifratora i kriptosistema sa ciljem da se razume kako oni funkcionišu. Pri tome teži se pokušaju nalaženja i poboljšavanja tehnika za razbijanjem ili oslabljenjem tih šifratora. Na primer, ljudi koji rade u polju kriptoanalize pokušavaju da dektriptuju šifrovani tekst bez znanja izvora tog teksta, enkripcionog ključa ili algoritma koji je iskorišćen da bi se enkriptovao taj tekst. Ti ljudi ciljaju na siguran hešing, digitalne potpise i kriptografske algoritme.

13. Cezarovo šifrovanje

Cezarovo šifrovanje je prastar način zamene mesta slova rečenice.
Da bi se neka poruka enkriptovala u Cezarovom šifratoru, svako slovo je promenjeno jednostavnim pravilom: pomeranjem u desno za 3 slova u abecedi: A postaje D, B postaje E, itd.
Možemo abecedu zamisliti kao krug pa će tako W postati Z, a X postati A, Y postaje B, Z postaje C. Da bi se ova poruka dešifrovala samo se vrati svako slovo, u šifrovanoj poruci, za 3 mesta u abecedi.
Ovaj algoritam je jako lako razbiti čak i kad se promeni broj slova za koji se pomera u neku stranu, ali Julije Cezar je koristio 3 pa se zato ovaj algoritam zove Cezarov.

14. DES algoritam

Data Encryption Standard (DES) algoritam jeste šifrator koji ima ključ u 56 bitova i koji je postao zastarao zbog njegove slabosti protiv jakih napada. Zbog slabosti razvijen je 3DES.
DES je blok šifrator koji radi u 64 bita, što znači da 64 bita teksta se uzima kao ulaz u DES, koji zatim na izlazu ima 64 bita šifrovanog teksta. Isti algoritam se koristi za šifrovanje i dešifrovanje, sa malim razlikama.
Ključ se u početku sastoji iz 64 bita, ali pre nego što DES enkripcija počne svaki 8mi bit se odbacuje, pa su tako bitovi na pozicijama 8, 16, 24, ..., 64 odbačeni.
DES radi u 16 koraka.



15. AES algoritam

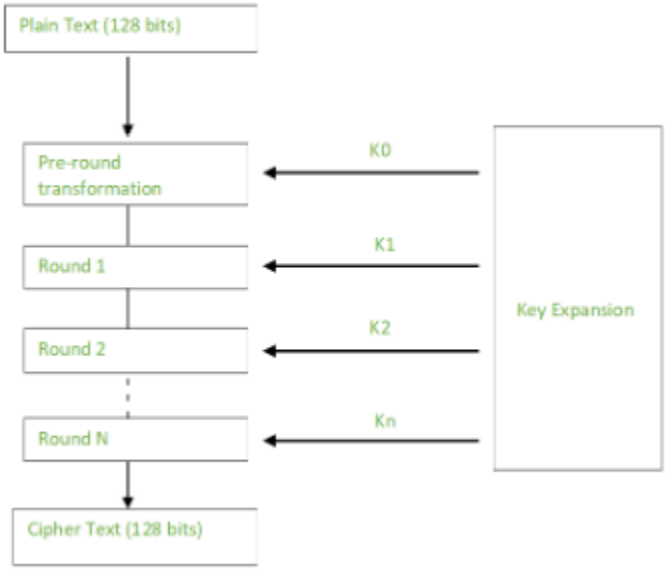
Advanced Encryption Standard (AES) je specifikacija za enkripotvanje elektronskih podataka koji je razvijen 2001. i koji ima široku primenu danas jer je mnogo jači od DES i 3DES iako je teži za implementaciju.

AES je blok šifrator, njegovi ključevi mogu da budu 128/192/256-bitni, a enkripcija se vrši u blokovima od 128 bitova svaki. Ovo znači da je ulaz AES 128-bitni tekst i na izlazu je 128-bitni enkriptovani tekst.

AES je baziran na seriji povezanih operacija koje uključuju menjanje i mešanje podataka.

AES radi tako što operacije vrši na bajtovima, umesto bitovima, pošto je blok 128 bitova, šifrator procesuje 16 bajtova.

Za 128 bitova, šifrator prolazi 10 koraka, za 192 - 12, a za 256 - 14.



16. RSA algoritam

RSA algoritam je asimetrični kriptografski algoritam. Asimetrični znači da radi sa dva različita ključa - privatnim i javnim. Javni je dostupan svima, a privatni se čuva privatno.

Asimetrična kriptografija radi na sledećem principu: Klijent pošalje javni ključ serveru zahtevajući neke podatke, zatim server enkriptuje podatke koristeći javni ključ klijenta i pošalje enkriptovane podatke, da bi klijent primio šifrovane podatke i dekriptovao ih.

RSA je baziran na činjenici da je teško faktorijalizovati veliki broj. Javni ključ se ovde sastoji iz 2 broja gde je jedan broj proizvod dva velika prosta broja, a privatni ključ je nasledjen iz tih brojeva. Tako da, ako neko uspe da faktorijalizuje veliki broj, privatni ključ će biti poznat. Zbog toga jačina enkripcije leži u veličini ključa i ako ključ pomnožimo sa 2 ili 3, jačina tog ključa raste eksponencijalno. RSA ključevi su obično 1024 ili 2048-bitni, ali stručnjaci nagoveštavaju da će u bliskoj budućnosti 1024-bitni ključ biti moguće razbiti, ali za sada taj zadatak je gotovo nemoguć.

17. Virus

Virus je računarski program koji može sebe kopirati kada je pokrenut. Obično, virusi se pokreću kao deo nekog drugog programa, svaki program koji je pogodjen virusom naziva se "inficiranim" ili "zaraženim". Biološki virusi rade na isti način, oni kopiraju sebe kao deo drugih organizama, tako je kompjuterski virus dobio ime.

Osim što može sebe da kopira, računarski virus može da izvrši naredbe koje dovode do štete, zbog ovih razloga virusi narušavaju bezbednost. Oni su deo malware-a.

Ponekad, izraz virus se koristi i za ostale vidove malware-a, kao što su: crvi, trojanski konji itd. Iako je ovo netačno, teško je reći o kom malware-u je obično reč, jer se ponekad oni realizuju grupno.

Postoji više vrsta kompjuterskih virusa i to:

- Makro-virus (script virus), ovi virusi su programirani sa skriptovanim funkcijama koji se nalaze u sklopu drugih programa
- Boot Sector virusi, oni inficiraju boot sektor flopi diskova, hard diskova i ostalih medija
- Pokretljive datoteke (executable files) i virusi operativnog sistema, ovo uključuje programe koji se pokreću automatski kada se medijum ubaci u slot (kao npr USB fleš)
- XSS (Cross Site Scripting), skripte na web stranicama koje se repliciraju na drugim stranicama

18. Crv

Kompjuterski crv je malware koji može kopirati sebe i proširiti se. Za razliku od kompjuterskih virusa, ovo se radi bez promene datoteka na računaru i bez promene boot sektora medija. Crvima ne treba ljudska pomoć da bi se razmnožili. Oni se šire preko mreža ili na medijumu kao što je USB fleš.

Njima obično treba pomoćni program da bi pristupili na mrežu ili koji se pokreće kada se neki novi medijum ubaci. Na taj način, crvi mogu pokrenuti program da pošalju e-mail i da proslede sebe na dosta različitih e-mail adresa. ILOVEYOU je poznati crv.

Crvi obično ne prave direktnu štetu sistemu, ali oni crpe memorijski prostor i brzinu mrežnog saobraćaja i tako usporavaju računar.

19. Trojanski konj

Trojanski konji (ili trojanci) su malware koji se predstavljaju kao da imaju neku drugu svrhu. Ponekad trojanci rade upravo ono što je i rečeno, ali pored toga rade i nešto drugo. Ovo je zato što prava svrha je skrivena - radjenje štetnih operacija u pozadini, kao na primer, pravljenja linije izmedju korisnika i nekog drugog, kome je možda omogućeno da čita i menja informacije na kompjuteru. U nekim situacijama, korisnik može da prepozna da ima trojanca, dok u drugim to nije moguće.

Mnogi moderni trojanci služe da naprave backdoor (zadnja vrata) preko kojih je moguće prisluškivanje.

Trojanci se obično šire tako što se neki korisnik **ZAJEBE**(ovo sam jebeno prevodio 2 minuta) i klikne na popup, email, prilog koji ide uz tekst, reklame itd.

Trojanski konj je nazvan po priči iz grčke mitologije.

20. Phishing napad

Fišing jeste način na koji kriminalci dobijaju sensitivne i privatne informacije (kao što su korisničko ime i lozinka). Ovo je metoda društvenog inženjerstva.

Obično, fišing se obavlja preko mail-a, moguće je da mail izgleda kao da je pošiljalac banka ili neki druga ustanova koja pruža usluge. Sadržaj maila može biti, na primer, da je došlo do neke promene pa tako korisnici moraju da se verifikuju, zajedno sa tim tekstom dolazi i link (koji je drugačiji od prave banke) identičnog sajta kao i prava banka.

Fišing dozvoljava kriminalcima da pristupe nalozima banaka, ili drugim kao što su nalozi za kupovinu, aukciju ili za igrice. Može se takodje koristiti i za kradju identiteta.

Fišing se nije mnogo menjao tokom godina, samo što se sada može obavljati i preko fejsbuka, instagrama itd.

21. <u>Generalna podela napada</u>

Postoji mnogo podela napada, ali najčešći napadi su:
- Malware (Ransomware, trojans, spyware, worms)
- DDoS (Distributed Denial-of-Service)
- Phishing
- SQL Injection Attacks
- XSS (Cross-Site Scripting)
- Botnets

22. <u>Firewall</u>

Firewall je, u računarstvu, mrežni sigurnosni sistem koji nadgleda i kontroliše ulazeći i izlazeći internet saobraćaj u odnosu na sigurnosna predefinisana pravila. Firewall obično uspostavlja barijeru izmedju sigurne (onoj kojoj možemo verovati) i nesigurne mreže (internet).
Firewall i Firewall-i sledeće generacije se fokusiraju na blokiranju malware-a i aplikacijskih slojevitih napada, kao i na blokiranju integrisanog sistema upadanja, Firewall-i sledeće generacije mogu odreagovati brzo i bez velikog "truda" detektovati i shodno tome odrediti šta da se radi prilikom spoljašnjeg napada na mrežu.

23. <u>Cross-Site Scripting (XSS)</u>

XSS je client-side injekcioni napad. Napadač cilja da izvrši zlonamerne skripte na web browseru žrtve tako što uključi neki kod (skriptu).
XSS napadač koristi web stranice sa slabom sigurnošću da bi isporučio Javascript korisniku. Korisnički pretraživač izvrši taj JS kod na kompjuteru.
Istraživanja su pokazala da 1 u 3 web sajtova imaju lošu sigurnost što se tiče XSS.
XSS napadi se dešavaju u web pretraživaču, moguće je da će takav napad uticati na ceo sajt, kao i na ceo pretraživač. Na primer, napadač može da ukrade korisničke podatke i da se uloguje na taj sajt. Ako je korisnik administrator, može se preuzeti kontrola nad celim sajtom
Da bi se zaštitili od XSS web sajt se mora skenirati svaki put nakon menjanja koda, da bi se otklonile sve moguće opasnosti za zlonamernu upotrebu skripti, firewall ne sprečava XSS - on ga samo čini težim za izvršavanje.