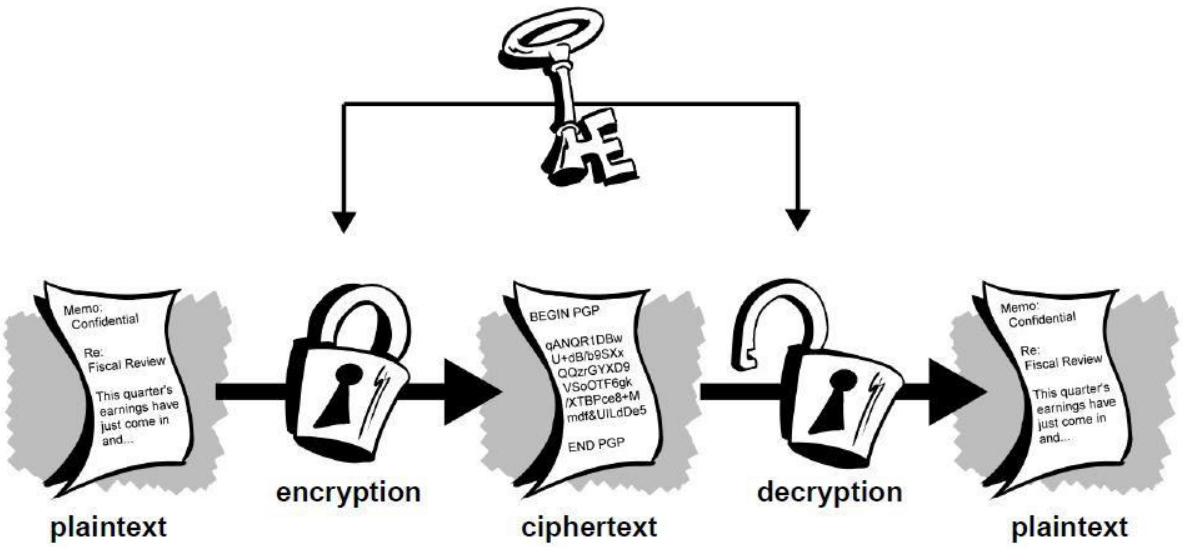
Javni i privatni ključevi u sistemima kripcije i enkripcije

Marija Popović IV_6

Kripcija (eng.encryption)

Postupak pomoću koga se izvorni tekst (Plaintext ili Cleartext) transformiše u šifrovan tekst se naziva kriptovanje (eng.encryption). Kriptovanje se koristi da bi se obezbedilo da nijedan korisnik, osim korisnika kome je poruka namenjena, ne može da sazna sadržaj poruke. Kriptovanje izvornog teksta se obavlja pomoću određenog pravila za kriptovanje odnosno kriptografskog algoritma:

- kao ulazne podatke ima izvorni tekst i ključ a kao izlaz daje kriptovani tekst.



Po definiciji, enkripcija je konverzija elektronskih podataka (plaintext) u šifrovanu formu (ciphertext) koji je nerazumljiv za sve osim za autorizovane strane koje imaju ključ za dešifrovanje. Primarna uloga enkripcije je da zaštiti poverljivost podataka koji su pohranjeni na računaru ili se distribuiraju putem interne mreže ili Interneta. Moderni algoritmi za enkripciju igraju vitalnu ulogu u bezbednosti IT sistema i komunikacije, ne samo kad je u pitanju poverljivost podataka, već i sledećim kjučnim ele-mentima sigurnosti:

- Autentifikacija: Može se verifikovati poreklo poslatog sadržaja
- Integritet: Obezbeđuje dokaz da poslati sadržaj nije izmenjen nakon slanja
- Neporecivost: Pošiljaoc ne može da porekne da je poslao sadržaj

Istorija enkripcije

Reč enkripcija potiče od grčke reči kriptos, koja znači sakriven ili tajna. Upotreba enkripcije bezmalo je stara koliko i samo umeće komunikacije. Još 1900 godina pre nove ere Egipatski pisci koristili su nestandardne hieroglife da prikriju značenje napisanog. U vreme kada većina ljudi nije znala da čita, pisanje poruka je bilo dovoljno, ali su ubrzo razvijeni šabloni za enkripciju koji su konvertovali poruke u nečitljive grupe figura kako bi sačuvali njihovu poverljivost prilikom prenošenja sa jednog na drugo mesto. Sadržaj poruka se preuređivao ili

zamenjivao sa drugim karakterima, simbolima, brojevima ili slikama u cilju prikrivanja pravog značenja.

Spartanci su, 700 godina pre nove ere, pisali poverljive poruke na kožnim trakama obmotanim oko štafeta. Kada bi se traka odmotala, ispisani karakteri bi izgubili smisao, ali sa štafetom istog prečnika primalac je mogao da dešifruje poruku. Kasnije, u doba rimljana, napravljen je Cezarov šifarnik u kome se svako slovo otvorenog teksta menjalo odgovarajućim slovom alfabeta (monoalfabetska substitucija), pomerenim za određeni broj mesta. Na primer, ukoliko je dogovoreni broj mesta 3, reč „odžačar“ u šifrovanom obliku bi bila „SFCČĐČT“. Na prvi pogled deluje komplikovano, ali prostim pomeranjem početka abecede u odnosu na poruku, brzo ćete doći do rezultata. Takođe, samoglasnici i često korišćena slova mogu se lako utvrditi analizom frekvencije ponavljanja, a te se informacije mogu koristiti u daljem dešifrovanju poruke.

Srednji vek je ispratio pojavu polialfabetskih šifarnika koji su koristili više alfabeta istovremeno i onemogućavali analizu frekvencije ponavljanja. Ovaj metod enkripcije je ostao popularan uprkos mnogim neuspelim pokušajima da se adekvatno prikrije promena šifarnika, poznatija kao progresija ključa. Verovatno najpoznatiju primenu polialfabetskog šifarnika predstavlja Enigma, elektro-mehanički šifarnik sa rotorom koji su koristili Nemci u drugom svetskom ratu.

Veliko unapređenje u enkripciji dogodilo se sedemdesetih godina prošlog veka. Do tada su svi šabloni koristili isti metod za enkripciju – jedan, simetrični ključ za šifrovanje i dešifrovanje poruka. Godine 1976, u svojoj studiji „Novi pravci u kriptografiji“, autori B. Whitfield Diffie i Martin Hellman rešili su jedan od fundamentalnih problema u kriptografiji, a to je pronalaženje bezbednog načina za distribuciju ključa za dešifrovanje. Nedugo zatim je objavljen RSA algoritam za asimetričnu kriptografiju sa javnim ključem što je, paralelno sa ekspanzijom informacionih tehnologija, najavilo novu eru u svetu enkripcije.

Savremena upotreba enkripcije

Sve do pronalaska bezbednog načina za razmenu ključeva i RSA algoritama za asimetričnu kriptografiju, države i njihove armije bili su praktično jedini korisnici enkripcije. Nakon ovih otkrića, enkripcija je doživela komercijalni procvat i širu upotrebu u zaštiti podataka, kako u procesima mrežne distribucije (data in transit), tako i u procesima skladištenja podataka na različitim medijumima (data in rest). Uređaji u svakodnevnoj upotrebi poput modema, digitalnih risivera, smart i SIM kartica koriste raznorazne protokole za enkripciju (SSH, S/MIME, SSL/TLS) u službi zaštite osetljivih informacija. Enkripcija se koristi za zaštitu podataka poslatih sa bilo kojeg uređaja i u bilo kojoj vrsti mreže, ne samo na Internetu; svaki put kada koristite bankomat, kupujete online, pozivate mobilnim telefonom ili otključavate auto daljinski ključem, enkripcija štiti razmenu informacija koja se tom prilikom ostvaruje. Digital rights management sistemi koji sprečavaju neautorizovano korišćenje i kopiranje copyright materijala takođe su klasičan primer upotrebe enkripcije.

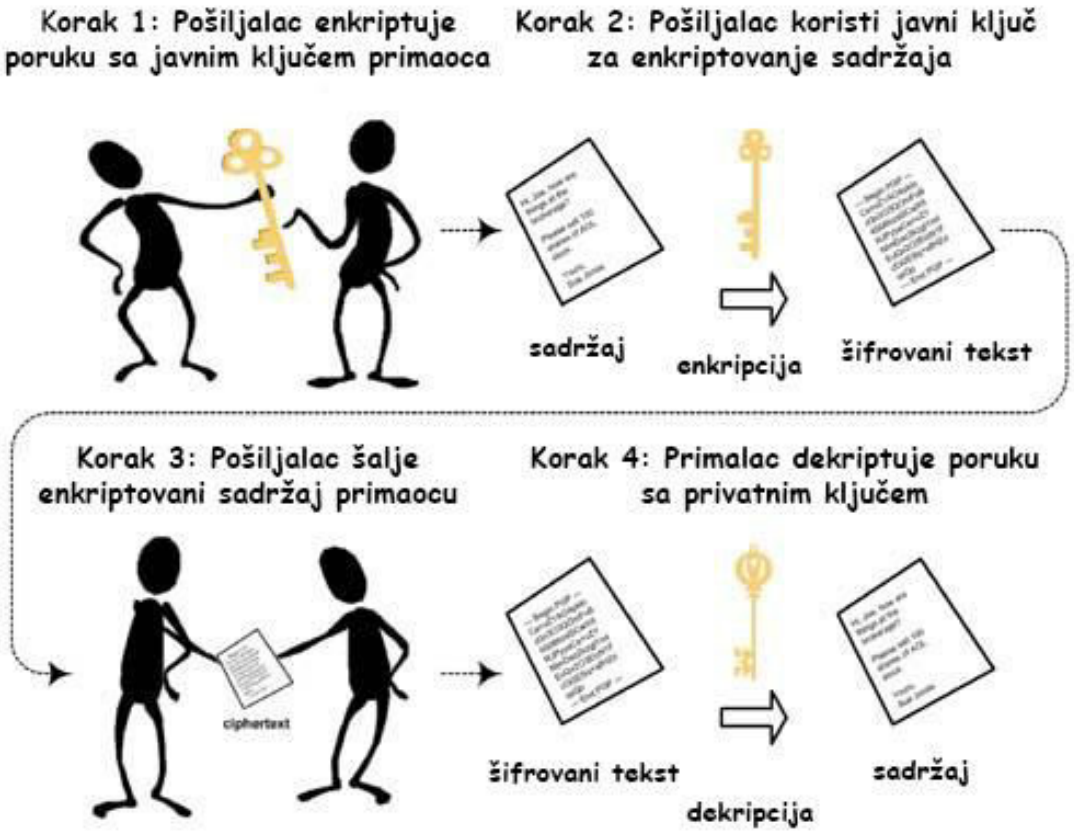
Vrste enkripcije

Postoje dve osnovne vrste enkripcije: simetrična enkripcija i asimetrična enkripcija. Kod simetrične enkripcije se i za šifrovanje i za dešifrovanje koristi ista šifra (ključ). Kod asimetrične postoji poseban ključ samo za šifrovanje i drugi koji služi samo za dešifrovanje. Ova dva ključa nazivaju se još javni i tajni ključ. Tajni ključ dodeljuje se onda kada se vrši enkripcija i na osnovu njega se generiše javni ključ, koji koristi strana koja treba da pročita podatke. Standard koji se koristi pri simetričnoj enkripciji je DES. Asimetrična enkripcija se još naziva i kriptografija javnog ključa. Za ovu vrstu enkripcije koristi se RSA algoritam.

Javni i privatni ključ

Izvorni oblik svih elektronskih podataka (data) je u tekstualnoj formi (plaintext). Enkripcija se vrši šifarnicima – algoritmima i ključevima za enkripciju. Ovaj proces generiše šifrovan tekst (ciphertext) koji može da se dekriptuje samo sa odgovarajućim algoritmom i ključem. Dekripcija je, ustvari, inverzni proces koji primenjuje korake enkripcije obrnutim redosledom. Današnji algoritmi za enkripciju podeljeni su u dve kategorije: simetrične i asimetrične.

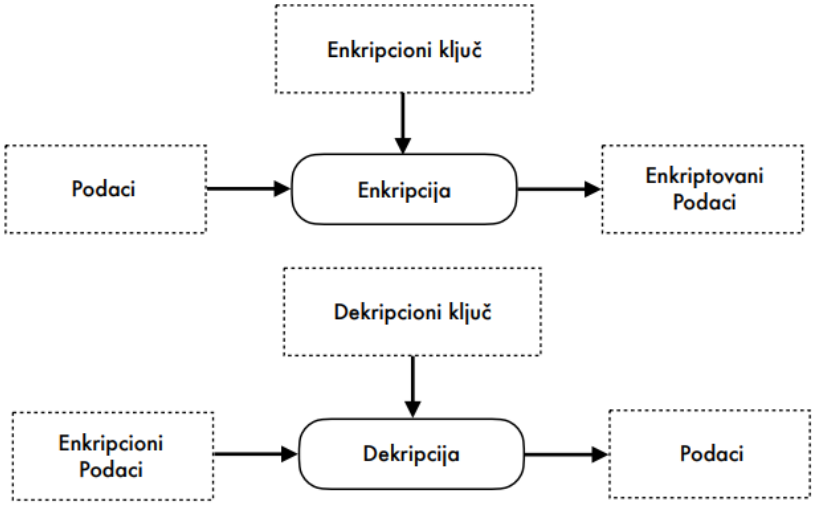
Simetrični algoritmi koriste isti ključ za enkripciju i dekripciju podataka. AES (Advanced Encryption Standard) je najčešće korišćeni simetrični algoritam, inicijalno kreiran za upotrebu u državnim institucijama za zaštitu poverljivih informacija. Simetrična enkripcija je mnogo brža u odnosu na asimetričnu, s tim da onaj koji šalje šifrirane podatke mora da razmeni ključ za dešifrovanje sa primaocem poruke. Potreba da se bezbedno distribuira veliki broj ključeva dovela je do toga da većina procesa u kriptografiji koristi simetrične algoritme za sadržaj, a asimetrične za razmenu ključeva.



Asimetrična kriptografija, poznata i kao kriptografija sa javnim ključem, koristi dva različita ali matematički povezana ključa, jedan javni i jedan privatni. Javni ključ je dostupan svima dok se privatni čuva u tajnosti. RSA (skraćenica predstavlja početna slova prezimena pronalača Rona Rivesta, Adi Shamira i Leonarda Adlema) je najšire upotrebljavan asimetrični algoritam delom zbog toga što oba ključa, i javni i privatni mogu da enkriptuju poruku; za dekripciju se koristiti ključ asimetričan onome sa kojim je izvršena enkripcija. Ova osobina je omogućila ne samo poverljivost poslatih informacija, već i proveru integriteta, autentičnost i neporecivost u elektronskoj komunikaciji i pohranjivanju podataka korišćenjem digitalnih potpisa.

Javni ključ - enkripcija, privatni ključ - dekripcija

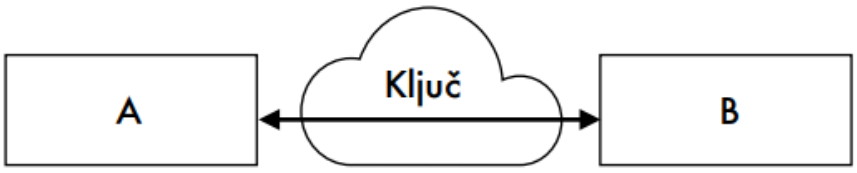
Kao što je bio slučaj i kod simetričnih šifara, enkripcija podataka podrazumeva skrivanjepodataka od svih učesnika koji nemaju ključ kojim se podaci mogu otkriti. Asimetrična kriptografija koristi javni ključ primaoca za enkriptovanje podataka a privatni ključ primaoca za dekriptovanje podataka. Iako je moguće, asimetrična enkripcija nije pogodna za enkriptovanje velike količine podataka zbog svoje brzine, za razliku od simetričnih šifara koje su i do 1000 puta brže od asimetričnih. Iz tog razloga, simetrična kriptografija se koristi u specifičnim okolnostima gde je količina podataka mala i gde osobine asimetrične kriptografije daju najveći doprinos. Čest scenario je enkripcija podataka simetričnim ključem a zatim korišćenje algoritama asimetrične kriptografije za enkripciju simetričnog ključa koji se zajedno sa enkriptovanim podacima šalje primaocu.



Dijagram asimetrične enkripcije/dekripcije

RAZMENA KLJUČA

Razmena ključa može se smatrati posebnim oblikom enkripcije, gde je cilj skriveno (nerazumljivo za ostale učesnike) dogovoriti simetrični ključ koji će se nadalje koristiti za enkripciju podataka koji se prenose između učesnika koji učestvuju u razmeni. U zavisnosti od algoritma, ključ se može preneti enkripcijom privatnim ključem od strane oba učesnika, bez potrebe dekripcije (npr. Diffie-Hellman razmena) dok se kod drugih algoritama vrši enkripcija javnim ključem primaoca i dekripcija privatnim ključem primaoca, kao što je uobičajen slučaj kod enkripcije.



Dijagram razmene ključa