Kriptografske primitive

Informaciona bezbednost

FAKULTET TEHNIČKIH NAUKA

V2

Sadržaj

- Istorija
- Osnovna terminologija
- Kriptologija
- Simetrična kriptografija
- Asimetrična kriptografija
- Simetrična i asimetrična kriptografija
- Heš funkcije
- Bezbedna komunikacija

Istorija

- Cezarova šifra je jedna od najstarijih i najprostijih šifri, i pripada porodici šifre zamenjivanja. Otvoreni tekst se šifruje tako što se svaki karakter u otvorenom tekstu zameni sa karakterom koji je određen broj karaktera udaljen u alfabetu.U slučaju alfabeta, koji se sastoji od 26 karaktera, funkcija za šifrovanje jednog karaktera se matematički može opisati kao:

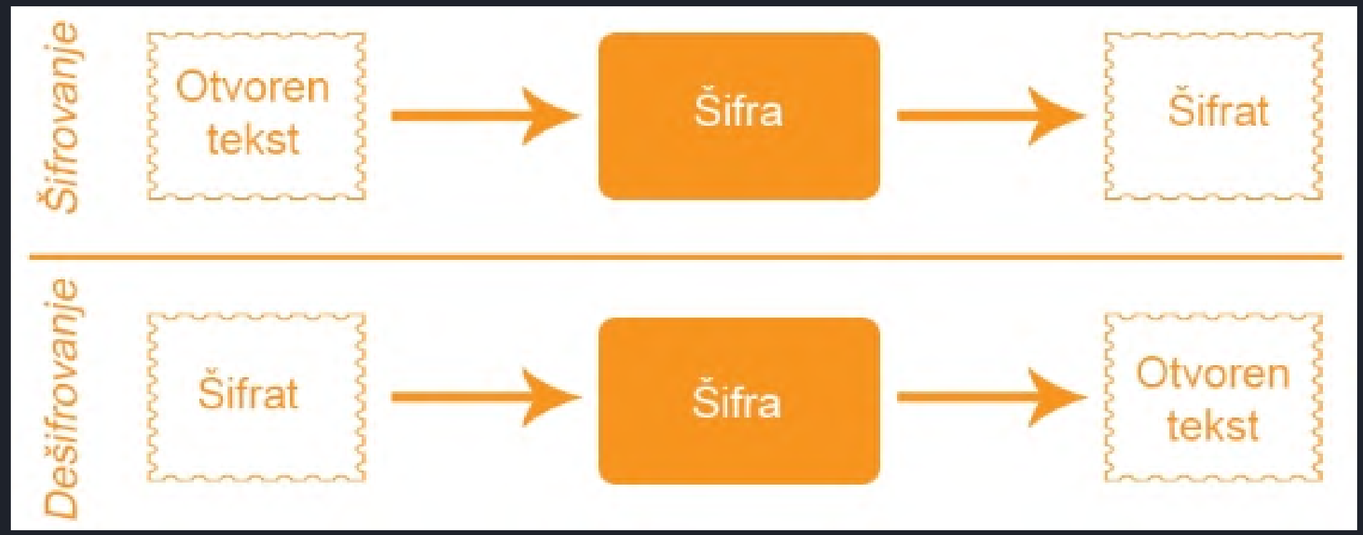
$$En(p)=(p+n)\ mod\ 26,$$

p- karakter otvorenog teksta, n-ceo broj koji predstavlja pomeraj u alfabetu putem kog se nalazi karakter šifrata.

- Posmatrajući Cezarovu šifru, moguće je uočiti sve pojmove koji igraju ulogu kako u zastarelim, tako i u modernim algoritmima za šifrovanje i dešifrovanje. Pored otvorenog teksta, šifrata i same šifre, pojavljuje se ključ, čija vrednost mora ostati tajna da bi šifrat ostao bezbedan, a to je broj n.

Osnovna terminologija

- U najprostijem obliku, kriptografski algoritam predstavlja **šifru**
- Šifra - algoritam koji vrši **šifrovanje** i **dešifrovanje**
- Šifrovanje - funkcija koja pretvara otvoreni tekst u šifrat
- Dešifrovanje - funkcija koja pretvara šifrat u originalni otvoreni tekst
- Ključ - parametar koji parametrizije funkcije šifrovanja i dešifrovanja
- Dekripcija - postupak transformisanja šifrata u otvoreni tekst (bez poznavanja ključa)



Kriptologija

KRIPTOLOGIJA

- nauka koja se bavi tehnikama **zaštite** i **napada** na tajnost i integritet poruka. Tajnost predstavlja svojstvo da se poruka može čitati samo od strane autorizovanih korisnika. Integritet je svojstvo koje obezbedjuje otkrivanje neautorizovane promene poruke ili izvora poruke.

KRIPTOGRAFIJA

- grana kriptologije koja se bavi tehnikama zaštite tajnosti (poverljivosti) i integriteta poruka

KRIPTOANALIZA

- grana kriptologije koja se bavi tehnikama napada na tajnost (poverljivost) i integritet poruka

Simetrična kriptografija

- Ključ za šifrovanje je isti kao i ključ za dešifrovanje
- Prošiljalac i primalac poruke se moraju dogovoriti oko tajnog ključa
- Ključ za dešifrovanje se može izračunati na osnovu ključa za šifrovanje i obrnuto; najčešće su ključevi jednaki

Alisa i Bob žele da razmene poruku preko interneta, koristeći simetrični šifru:

1. Alisa i Bob dogovaraju algoritam;

2. Alisa i Bob dogovore ključ;

2. Alisa šifruje poruku sa ključem K koristeći dogovoreni algoritam;

3. Alisa šalje rezultujući šifrat, preko mreže, Bobu;

4. Bob, koristeći isti kli algoritam i ključ K, dešifruje šifrat i dobija originalnu poruku.

Simetrična kriptografija

- Formalno, simetrična šifra se može definisati kao skup dve funkcije, funkcije za šifrovanje E i funkcije za dešifrovanje D. Za svaku poruku M i ključ K se može dobiti šifrat C, tako da važi:

$$C=E(M,K) \quad M=D(C,K)$$

- Postoje dve osnovne grupe simetričnih šifri, i to su:
  1. **Šifra niza** (engl. Stream) - enkripcija poruke(originala) se vrši bit po bit
  2. **Blok šifre** (engl. Block) - enkripcija se vrši po blokovima podataka

Simetrična kriptografija

ŠIFRA NIZA

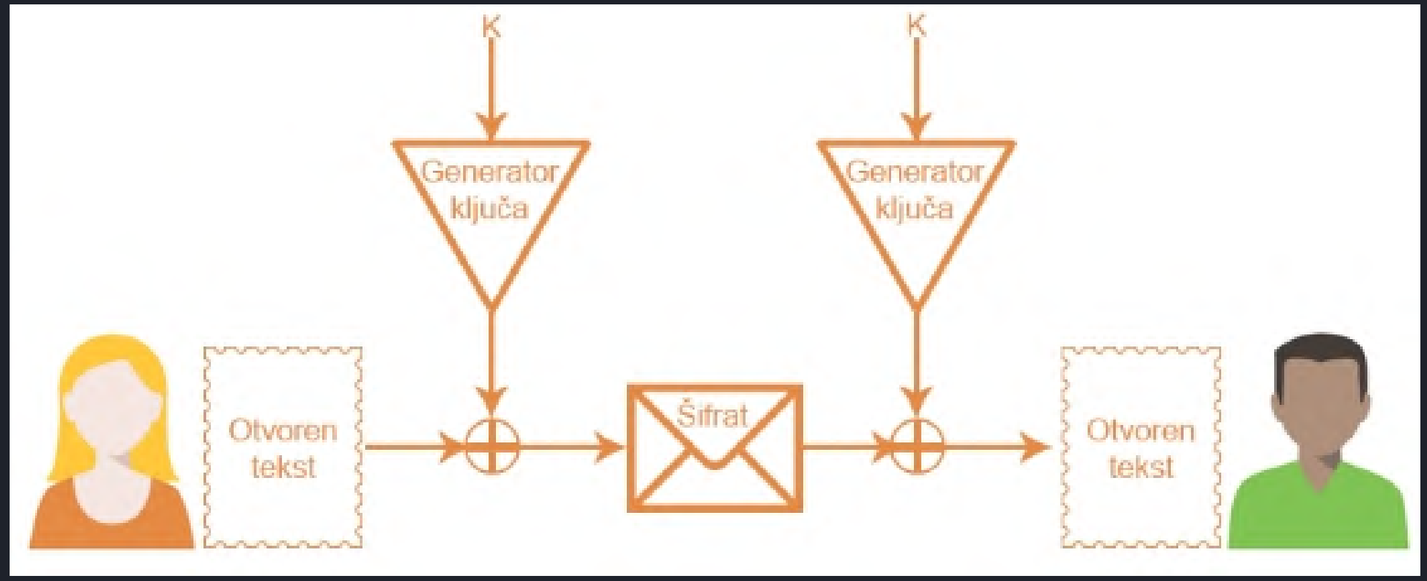
Šifre niza svoje ime dobijaju po ključu koji se generiše kao beskonačan niz bitova upotrebom generatora pseudo slučajnih brojeva

Alisa želi da pošalje šifrovanu poruku Bobu upotrebom šifre niza:

1. Alisa i Bob dogovaraju algoritam koji će da koriste, uključujući generator pseudo slučajnih brojeva koji će da generiše ključ, i početni ključ K koji će se koristiti kao nasumičan seed za generator
2. Alisa prosleđuje početni ključ generatoru pseudo slučajnih brojeva, koji potom generiše bajt za svaki bajt otvorenog teksta Alisine poruke. Putem operacije XOR se spaja bajt generisanog ključa i otvorenog teksta, čime se dobija bajt šifrata
3. Alisa prosleđuje šifrat Bobu
4. Bob upotrebom dogovorenog ključa aktivira svoj generator pseudo slučajnih brojeva i generiše identičan ključ koji je Alisa generisala. Upotrebom XOR operacije između bajtova generisanog ključa i šifrata dobija se otvoreni tekst, odnosno Alisina poruka

Simetrična kriptografija

ŠIFRA NIZA



Šifre niza pronalaze primenu zbog svoje efikasnosti. Ovi algoritmi zbog svoje jednostavnosti rade brzo i zahtevaju malo hardverskih resursa. Ključan problem predstavlja ispravna implementacija generatora slučajnih brojeva koji formiraju ključ, i mnogo algoritama iz ove grupe pati od dizajna koji nije otporan na metode kriptoanalize.

Simetrična kriptografija

BLOK ŠIFRA

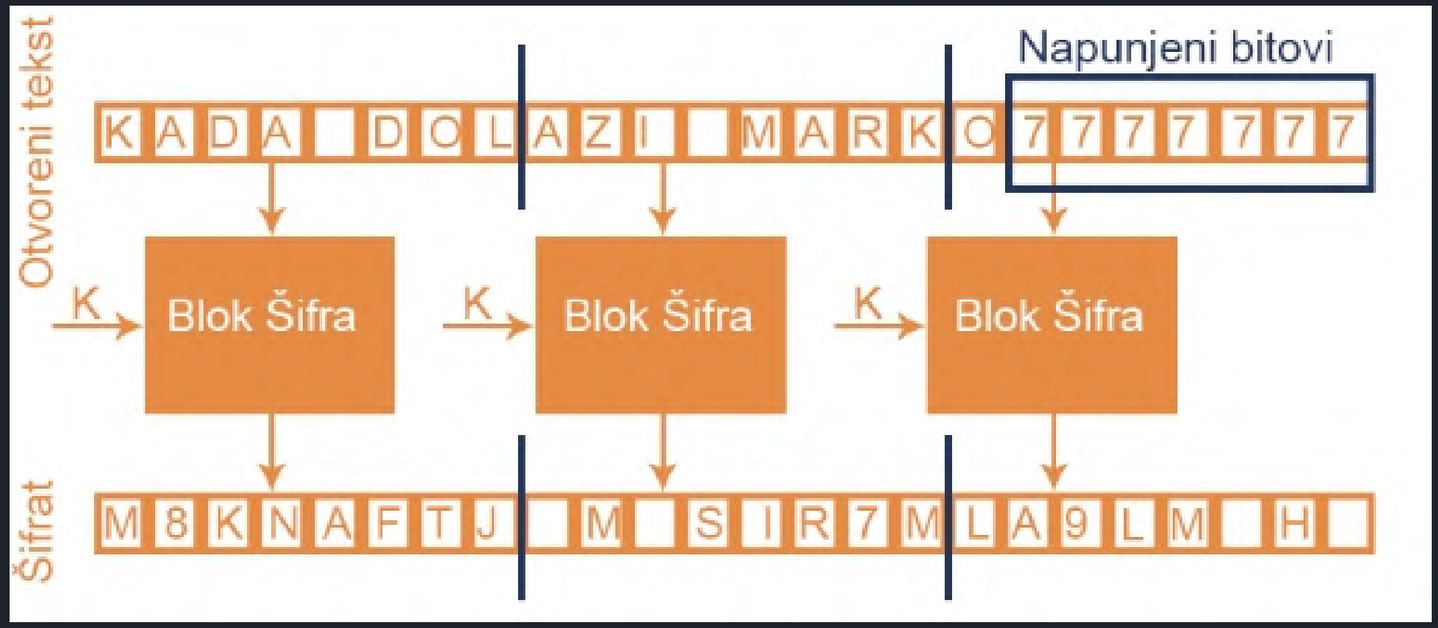
Blok šifre dele otvoren tekst u niz blokova određene dužine, gde se jedan blok otvorenog teksta prosleđuje algoritmu za šifrovanje, i pretvara u jedan blok šifrata. Ukoliko dužina otvorenog teksta nije jednaka umnošku dužine bloka, poslednji blok se dopuni sa određenim bitovima (engl. Padding). Ukoliko dužina otvorenog teksta jeste jednaka umnošku dužine bloka, kreira se još jedan blok koji će biti u potpunosti ispunjen određenim bitovima.

- Svaki blok simbola se šifruje uvek na isti način, nezavisno od mesta koje zauzima u poruci.
- Jednake poruke, šifrovane sa istim ključem, uvek daju jednake šifrovane poruke.
- Da bi se dešifrovao deo poruke, nije neophodno dešifrovati je od početka, dovoljno je dešifrovati blok koji nas interesuje.

Simetrična kriptografija

BLOK ŠIFRA

Postoji više režima (engl. Mode) u kojim blok šifra drugačije orkestrira blokove, kombinuje ih i šifruje, kako bi se povećala bezbednost same šifre. **ECB (engl. Electronic Code Book)** režim, je najprostiji oblik orkestracije ovih blokova, gde se jedan blok otvorenog teksta direktno šifruje u jedan blok šifrovanog teksta



Simetrična kriptografija

- Trenutno najsigurniju simetričnu šifru predstavlja AES (engl. Advanced Encryption Standard), koristeći ključ od 256 bita, oslanjajući se na PKCS#7 strategiju za dopunu bitova. Međutim, ovo ne znači da vremenom neće biti otkrivene ranjivosti u algoritmu, režimu rada ili strategiji za dopunu bitova. Kada se pojavi potreba za upotrebu simetrične šifre u projektu, neophodno je istražiti šta se u tom trenutku smatra za sigurnu šifru, ali i koje su najbolje prakse za konfiguraciju date šifre.

Asimetrična kriptografija

- Ključ za šifrovanje je različit od ključa za dešifrovanje
- Javni ključ se koristi za šifrovanje poruka
- Privatni ključ se koristi za dešifrovanje poruka
- ”Teško” je izračunati javni ključ na osnovu privatnog ključa (i obrnuto)
- Ne postoji problem distribucije javnih ključeva (zato što su javni ključevi javni)

Asimetrična šifra se definiše kao skup dve funkcije, funkcije za šifrovanje E i funkcije za dešifrovanje D. Za svaku poruku M i par javnog i privatnog ključa J i P se mogu se dobiti šifrati C i X, tako da važi:

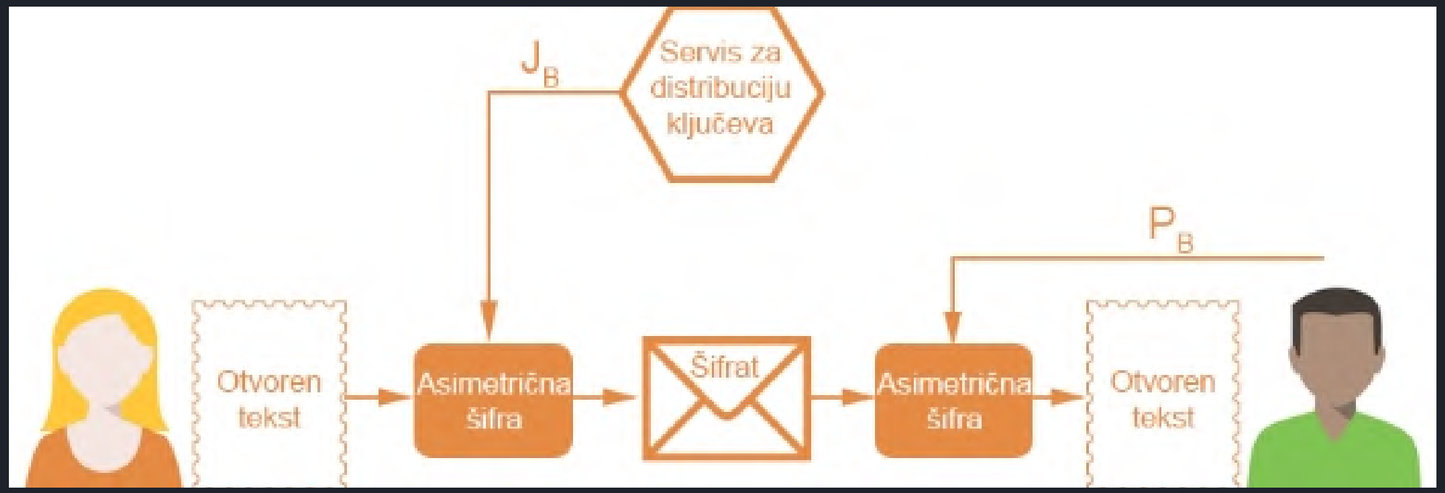
$$C=E(M,J);$$

$$M=D(C,P);X=E(M,P);M=D(X,J)$$

Asimetrična kriptografija

Alisa i Bob žele da komuniciraju upotrebom asimetrične šifre:

1. Alisa i Bob su dogovaraju algoritam;
2. Alisa i Bob razmenjuju javni ključ, putem direktne komunikacije, ili upotrebom servisa za objavu javnih ključeva
3. Alisa koristi Bobov javni ključ da šifruje poruku;
4. Alisa šalje rezultujući šifrat Bobu;
5. Bob koristi svoj privatni ključ da dešifruje poruku i pročita njen sadržaj



Asimetrična kriptografija

- Putem asimetričnih šifri moguće je otvoreni tekst šifrovati kako sa javnim, tako i sa privatnim ključem. Šifrovanje poruke sa javnim ključem znači da rezultujući šifrat može dešifrovati samo subjekt koji je u posedstvu odgovarajućeg privatnog ključa, čime se može garantovati poverljivost poruke. Sa druge strane, ako se poruka šifruje sa privatnim ključem, svako ko ima pristup javnom ključu može da dešifruje rezultujući šifrat, što je u opštem slučaju velik broj, potencijalno nepoznatih, subjekata. Ova strategija ne doprinosi poverljivosti poruke, ali dati mehanizam ima svoju upotrebu. Ako se poruka može dešifrovati nečijim javnim ključem, sledi da je ta poruka bila formirana od strane tog nekog, što je koristan podatak.

- Problem kod asimetričnih šifri jeste provera garancije da neki javni ključ stvarno pripada datoj osobi.

- Bezbednost asimetričnih šifri je garantovana matematičkim tehnikama koje se nazivaju jednosmerne funkcije sa tajnom (engl. Trapdoor function). Ideja kod ovih tehnika jeste da je računanje funkcije za neki ulaz računski jednostavno, dok je računanje inverzne funkcije izuzetno zahtevno, ukoliko se ne zna tajna informacija (engl. Trapdoor).

Asimetrična kriptografija

RSA

RSA (engl. Rivest-Sharmir-Adleman) je aktuelna asimetrična šifra, čija bezbednost se zasniva na prethodno navedenom matematičkom problemu. Koraci algoritma za kreiranje ključeva su:

1. Alisa bira dva velika prosta broja p i q, i računa proizvod n = pq i φ(n) = (p - 1)(q - 1);
2. Alisa bira broj e čiji najveći zajednički delilac sa φ(n) je 1, i izračunava d = e-1 mod φ(n);
3. Alisa objavljuje (e, n) kao svoj javan ključ, dok d predstavlja privatni ključ;
4. Kada želi da joj pošalje poruku m, Bob izračunava c = me mod n, gde je dužina od m manja od n;
5. Alisa prihvata šifrat c i dešifruje ga po formuli cd mod n.

Detaljnija analiza RSA, kao i interaktivan kalkulator za računanje ključeva i šifrovanje poruka se može naći na sledećem linku.

Asimetrična kriptografija

E C C

Aktuelna vodeća asimetrična šifra je i ECC (engl. Elliptic Curve Cryptography). ECC šifre su zasnovane na problemu diskretnog logaritma primenjenog nad eliptičnim krivama. Matematika iza algoritma je složenija od RSA, i sam algoritam je teže implementirati. Kvalitetno objašnjenje o kriptografiji nad eliptičnim krivama se može naći na sl. linku.

RSA šifre se pokazala jednostavnijom za razumeti i ispravno implementirati, ali ECC šifre nude veću sigurnost sa kraćim ključevima. Ovo smanjuje prostor potreban da se skladišti ključ i povećava brzinu operacije generisanja ključeva i digitalnog potpisivanja. ECC šifre se trenutno smatraju kao najkvalitetnijim rešenjem u domenu asimetričnih šifri. Međutim, kontroverzija prati ovu grupu šifri, uključujući i odluku NSA organizacije da izbaci ECC šifre iz upotrebe pred kraj 2015. godine

Asimetrična i simetrična kriptografija

- simetrične šifre nude veću bezbednost po bitu ključa
- simetrični šifre koriste kraće ključeve i, u opštem slučaju, rade brže i zahtevaju manje energije
- asimetrični algoritmi su i do 1000 puta sporiji od simetričnih
- asimetrične šifre ne pate od problema razmene ključeva

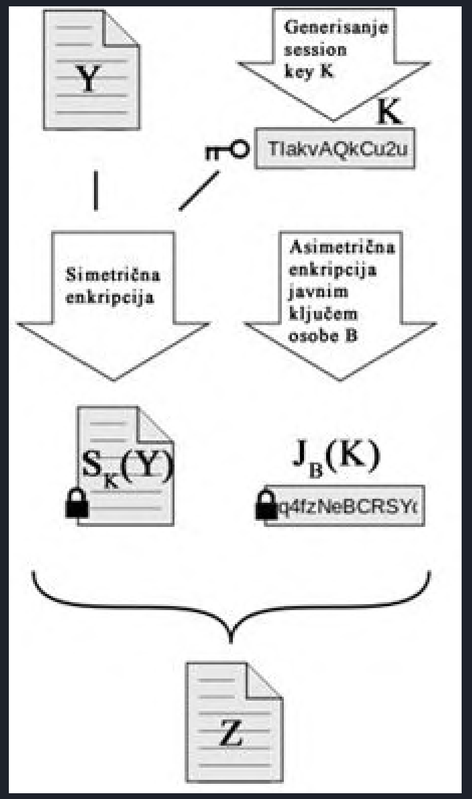
Šifrovanje poruka asimetričnim šiframa je neefikasno, pogotovo u slučaju veoma dugačkih poruka.
Upotrebom asimetrične šifre, pogotovo u kombinaciji sa simetričnom šifrom, moguće je na efikasan način omogućiti očuvanje svojstva poverljivosti poruke, i ovaj mehanizam se koristi u HTTPS protokolu da zaštiti poverljivost poruke koja se šalje sa klijenta na server.

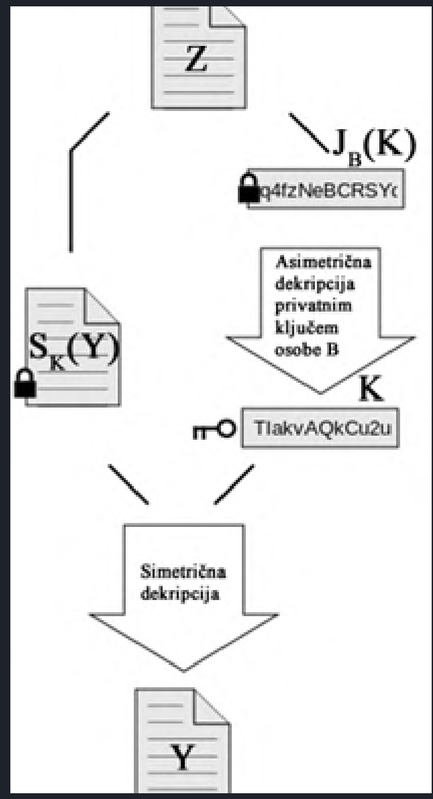
- asimetrični algoritmi se koriste za razmenu ključeva za simetrične algoritme
- ključ za simetričan algoritam se koristi samo u jednoj sesiji (session key)
- potencijalni (ali mnogo manji) problem – kompromitovanje tajnog ključa

Asimetrična i simetrična kriptografija

Alisa želi da pošalje poruku Y Bobu:

1. Alisa i Bob dogovaraju koji skup simetričnih i asimetričnih šifri će se koristiti;
2. Alisa generiše ključ K za simetričnu šifru koji će se koristiti za ovu poruku (engl. Session key);
3. Alisa šifruje poruku Y putem simetrične šifre i generisanog ključa i dobija šifrat SK(Y);
4. Koristeći asimetričnu šifru i Bobov javni ključ JB, Alisa šifruje ključ K i dobija šifrat JB(K);
5. Šifrovana poruka i šifrovan ključ se spajaju u poruku Z, koja se šalje preko mreže;
6. Sa druge strane Bob rastavlja poruku Z na šifrovanu poruku i šifrovan simetrični ključ;
7. Bob koristi svoj privatni ključ, PB, da dobije ključ K za simetričnu šifru;
8. Bob koristi ključ K da dešifruje šifrovanu poruku i dobija poruku Y.





Heš funkcije

Heš funkcije su jednosmerne funkcije koje preslikavaju otvoreni tekst proizvoljne dužine na heš fiksne dužine. Ukoliko je heš funkcija bezbedna, subjekat koji poseduje heš ne može da izračuna otvoren tekst od kog je nastao heš.

Idealna heš funkcija će ispunjavati sledeće zahteve:

- Funkcija je deterministička, gde isti tekst uvek proizvodi isti heš;
- Izračunavanje heša treba da bude brzo, ali ne previše brzo kako bi se otežao napad pogađanja;
- Nije moguće generisati originalan tekst iz heša;
- Izmena proizvoljnog bita u tekstu menja otprilike pola bitova generisanog heša (efekat lavine);
- Nije moguće, u razumnom vremenu, pronaći dve različite poruke koje proizvode isti heš.

Heš funkcije

Alisa šalje poruku X Bobu i želi da se osigura da greška u protokolu komunikacije ne izmeni njenu poruku:

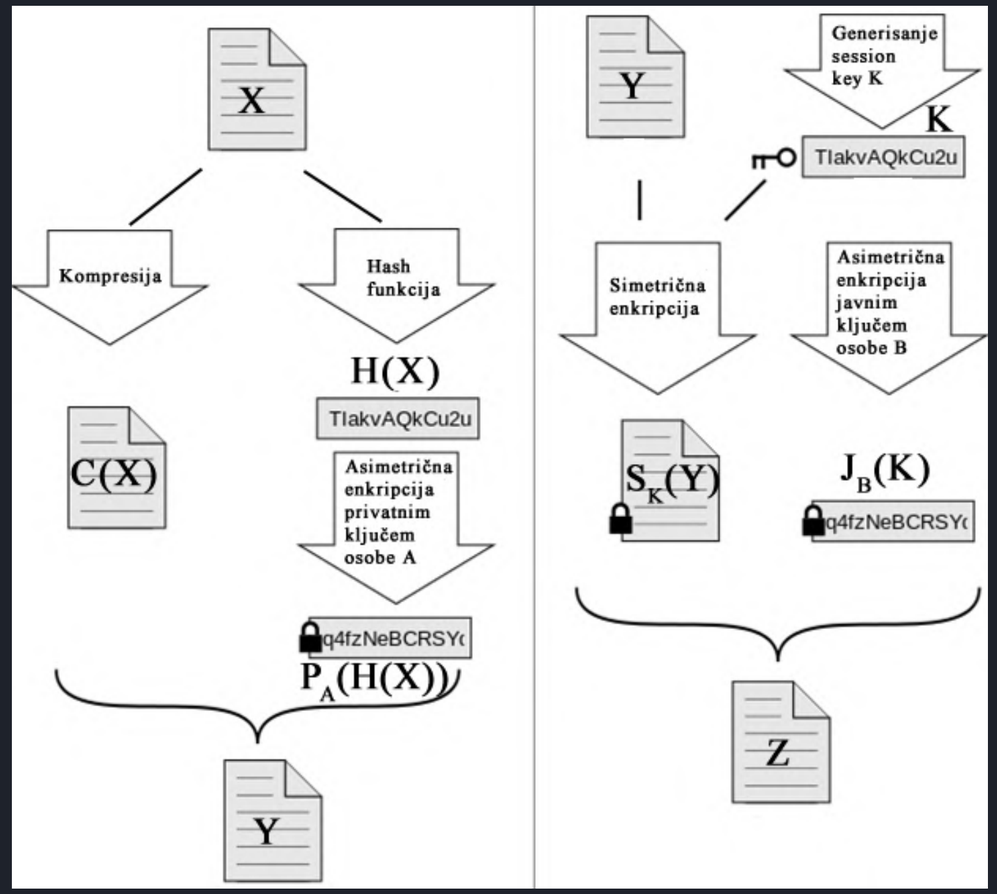
1. Alisa računa heš poruke X, i dobija H(X);
2. Alisa spaja poruku X i heš H(X) i dobija poruku Y, koju prosleđuje Bobu;
3. Bob rastavlja poruku na X i H(X) i izračunava heš od poruke X, čime dobija H’(X);
4. Ukoliko je H(X) = H’(X) znači da poruka X nije bila izmenjena, bar ne od strane greške u komunikaciji.

- Algoritama za heširanje je bilo više tokom istorije, i mnogi, poput MD5, su napušteni zbog svojih ranjivosti.
- Aktuelna bezbedna rešenja predstavljaju algoritmi iz SHA-2 i SHA-3 grupe, što ne znači da će u budućnosti to biti slučaj.
- Kao i uvek kod informacione bezbednosti, kada se pojavi zahtev za upotrebu nekog bezbednosnog mehanizma poput funkcije za heširanje, potrebno je sprovesti istraživanje da se proveri koji algoritam se smatra za zlatni standard.

Bezbedna komunikacija

Upotrebom simetrične šifre, asimetrične šifre i heš funkcije zajedno, moguće je garantovati poverljivost, integritet i neporecivost komunikacije preko interneta ili neke slične mreže

ŠIFROVANJE PORUKE



Bezbedna komunikacija

Upotrebom simetrične šifre, asimetrične šifre i heš funkcije zajedno, moguće je garantovati poverljivost, integritet i neporecivost komunikacije preko interneta ili neke slične mreže

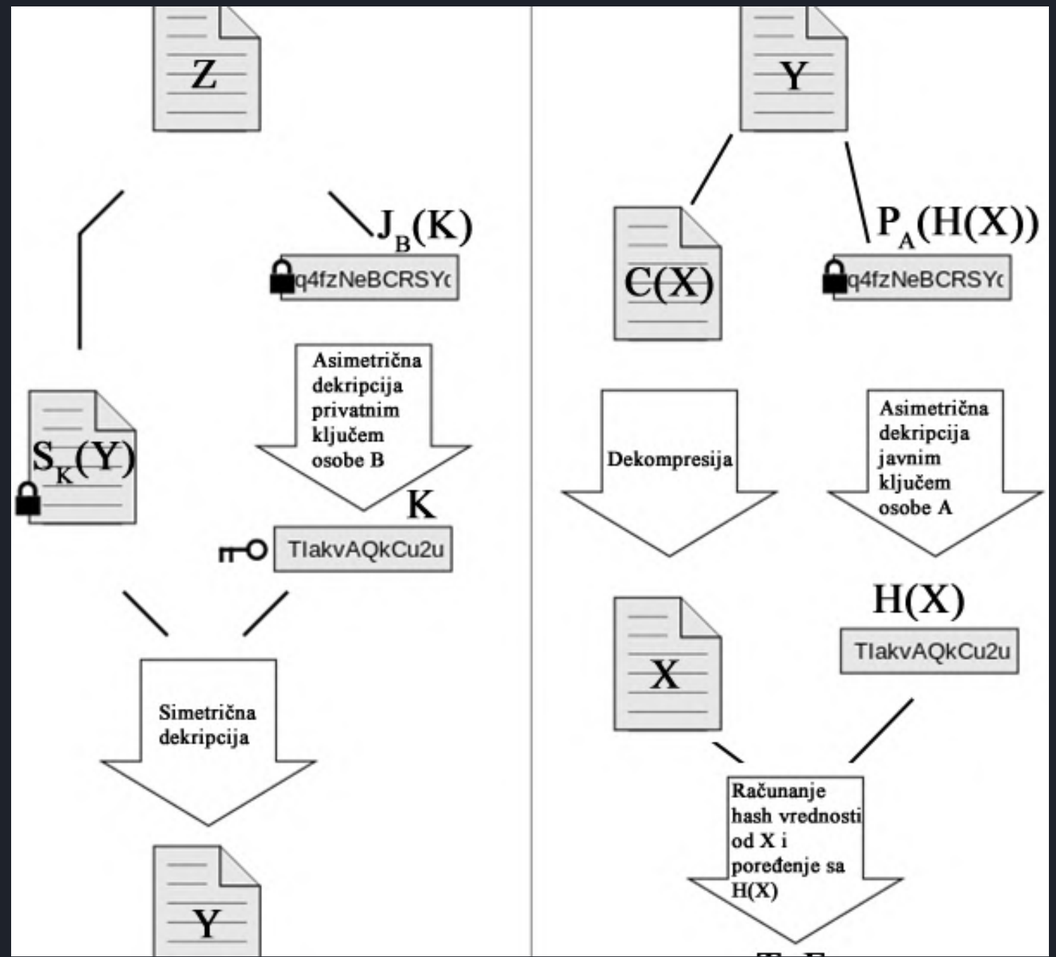
ŠIFROVANJE PORUKE

1. Alisa formira heš poruke X i dobija H(X);
2. Upotrebom asimetrične šifre i svog privatnog ključa, Alisa šifruje heš i dobija šifrat PA(H(X));
3. Nakon što izvrši kompresiju poruke X i dobije C(X), Alisa spaja poruku i PA(H(X)) u Y;
4. Koristeći ranije opisan postupak, Alisa šifruje poruku i šalje šifrat Z Bobu.

Bezbedna komunikacija

DEŠIFROVANJE PORUKE

Preduslov da Bob može da dešifruje poruku, proveri da li je ona došla od Alise i da li se menjala u toku tranzita jeste da poznaje i koristi sve algoritme koje je Alisa koristila, kao i da ima pristup Alisinom javnom ključu.



Bezbedna komunikacija

DEŠIFROVANJE PORUKE

Preduslov da Bob može da dešifruje poruku, proveri da li je ona došla od Alise i da li se menjala u toku tranzita jeste da poznaje i koristi sve algoritme koje je Alisa koristila, kao i da ima pristup Alisinom javnom ključu.

1. Bob dešifruje poruku Z i dobija poruku Y po prethodno opisanom postupku
2. Koristeći javni ključ od Alise, dešifruje PA(H(X)) i dobija heš originalne poruke, odnosno H’(X);
3. Bob vrši dekompresiju originalne poruke i izračunava njen heš, koji poredi sa H(X);
4. Ukoliko je H’(X) = H(X) znači da poruka nije menjana u toku tranzita, kako od strane greške u transportu tako i od strane malicioznog napadača, te je Alisin digitalan potpis validan.

Komunikacija je istinski sigurna samo ako javni ključ JA stvarno pripada Alisi, i samo ako javni ključ JB stvarno pripada Bobu.