Zaštita podataka

PGP

Pretty Good Privacy

Sadržaj

Zaštita elektronske pošte

- Elektronska pošta predstavlja jednu od najkorišćenijih distribuiranih aplikacija.
- Postoji povećana potreba za pružanjem autentikacije i tajnosti kao servisa u sklopu elektronske pošte.
- U okviru kursa obradićemo dva pristupa koji će najverovatnije dominirati u elektronskoj pošti u bliskoj budućnosti.
- Pretty Good Privacy (PGP) je široko korišćena šema koja ne zavisi niti od jedne organizacije ili institucije, te je zbog toga prikladna kako za ličnu upotrebu, tako i za komercijalnu.
- Secure/Multipurpose Internet Mail Extension (S/MIME) je razvijeno da bude internet standard

PGP istorijat

- Zaslugom Phil Zimmermann-a, PGP pruža tajnost i autentikaciju kao servise koji se mogu koristiti za elektronsku poštu.
- U suštini, Zimmermann je uradio sledeće:
- Izabrao najbolje raspoložive kriptografske algoritme kao sastavne delove
- Integrisao ove algoritme u jednu aplikaciju opšte namene, koja je nezavisna u odnosu na operativni sistem i procesor i koja se zasniva na malom skupu komandi koje su lake za korišćenje
- Obezbedio je da paketi i njihova dokumentacija, uključujući i izvorni kod, budu besplatno dostupni putem interneta
- Napravio sporazum sa kompanijom (Viacrypt, danas Network Associates) da obezbedi potpuno kompatibilnu, nisko budžetnu komercijalnu verziju PGP-a

PGP istorijat

- PGP je doživeo eksplozivni rast i danas je u širokoj upotrebi.
- Može se navesti nekoliko razloga za takav rast:
- Dostupan je besplatno u verzijama koje rade na različitim platformama, uključujući Windows, UNIX, Macintosh, i mnoge druge. Pored toga, komercijalna verzija zadovoljava korisnike koji žele proizvod sa podrškom proizvođača.
- Baziran je na algoritmima koji su preživeli iscrpljujuće javne rasprave i smatraju se izuzetno sigurnima. Konkretno, paket uključuje RSA, DSS, i Diffie-Hellman za šifrovanje pomoću javnog ključa; CAST-128, IDEA, i 3DES za simetrično šifrovanje; i SHA-1 za heš šifrovanje.
- Ima širok spektar upotrebljivosti, od korporacija koje žele da izaberu i sprovedu standardizovanu šemu za šifrovanje fajlova i poruka, do pojedinačnih korisnika koji žele da komuniciraju bezbedno sa drugima širom sveta, putem interneta i ostalih mreža.
- Nije razvijen, niti kontrolisan, od strane bilo koje organizacije.
- PGP je na putu da postane internet standard (RFC 4880, RFC 3156).

PGP notacija

- Većina notacije koja će se koristiti u nastavku, već je ranije korišćena, ali ima i novina.
- Najbolje je zato na početku da sumiramo sve što će biti korišćeno:
  - Ks=ključ sesije korišćen u simetričnim algoritmima
  - PRa=privatni ključ korisnika A, korišćen za šif. javnim ključem
  - PUa=javni ključ korisnika A, korišćen za šif. javnim ključem
  - EP= šifrovanje javnim ključem
  - DP= dešifrovanje javnim ključem
  - EC= šifrovanje simetričnim algoritmom
  - DC= dešifrovanje simetričnim algoritmom
  - H= heš funkcija
  - ||= konkatenacija
  - Z= kompresija ZIP algoritmom
  - R64= konverzija u radix 64 ASCII format
- U PGP dokumentaciji često se koristi izraz tajni ključ koji se odnosi na ključ koji se uparuje sa javnim ključem kod algoritama za šifrovanje pomoću javnog ključa. Bitno je da ne dođe do zabune sa tajnim ključem koji se koristi u simetričnim algoritmima šifrovanja. Zbog toga se može koristiti termin privatni ključ.

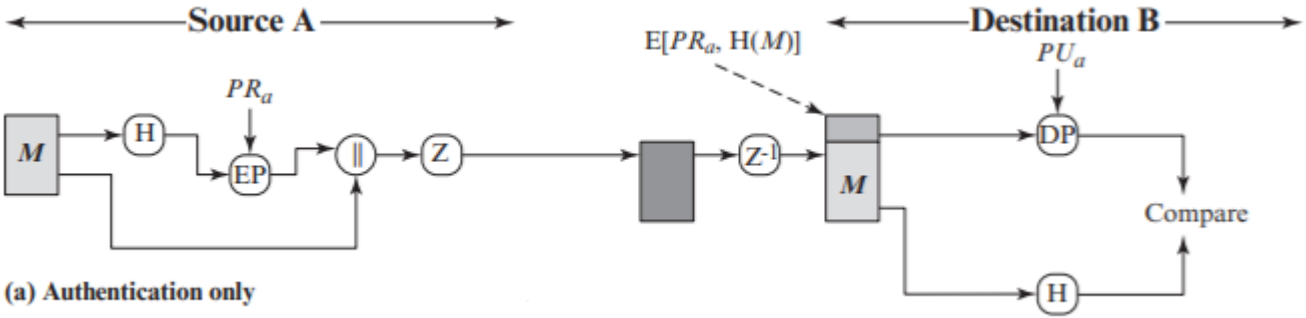
PGP opis servisa

- PGP se sastoji od pet servisa:
  - autentikacije,
  - tajnosti,
  - kompresije,
  - e-mail kompatibilnosti i
  - segmentacije.

PGP opis servisa - autentikacija

- Sekvenca je sledeća:

1. Pošiljalac kreira poruku.
2. SHA-1 se koristi da se generiše160-bitni heš kod poruke.
3. Heš kod se šifruje pomoću RSA korišćenjem privatnog ključa pošiljaoca i rezultat se dodaje na poruku.
4. Primalac koristi RSA sa javnim ključem pošiljaoca da dešifruje heš kod.
5. Primalac generiše novi heš kod za poruku i upoređuje ga sa dešifrovanim heš kodom. Ukoliko se slažu, poruka se prihvata kao autentična.



PGP opis servisa - autentikacija

- Kombinacija SHA-1 i RSA obezbeđuje efikasnu šemu digitalnog potpisa.
    - Zbog jačine RSA, primalac je siguran da je jedino onaj ko poseduje upareni privatni ključ mogao da generiše potpis.
    - Zbog jačine SHA-1, primalac je siguran da niko drugi nije mogao da generiše novu poruku koja ima isti heš kod, a samim tim, i potpis originalne poruke.
- Kao alternativa, potpisi mogu biti generisani korišćenjem DSS/SHA-1.
- Zanimljivost: iako su potpisi normalno povezani sa porukom ili fajlom koji potpisuju, ovo ne mora uvek biti slučaj. Podržani su i nepovezani potpisi. Nepovezani potpis može se čuvati i prenositi nezavisno od poruke koju potpisuje. Ovo se koristi u nekoliko slučajeva:
    - Korisnik može hteti da ima poseban log potpisa svih poslatih ili primljenih poruka.
    - Nepovezani potpis izvršnog programa može da detektuje virus.
    - Koristi se kada više strana treba da potpiše dokument, npr. pravni ugovor. U suprotnom, potpisi bi bili ugneždeni, tj. potpis drugog korisnika bi bio primenjen i na dokument i na potpis prvog zajedno, itd.

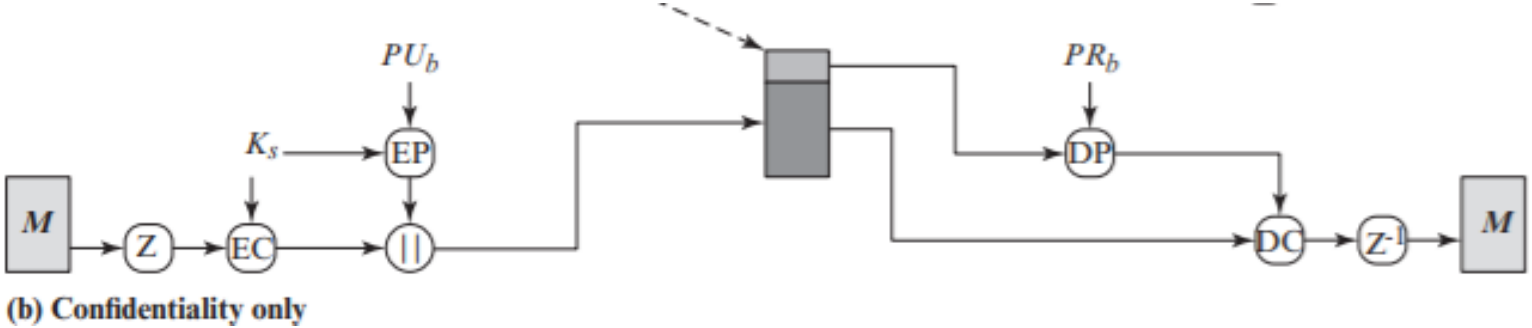
PGP opis servisa - tajnost

- PGP obezbeđuje tajnost šifrovanjem poruka za slanje ili skladištenje.
- U oba slučaja se koristi jedan od simetričnih algoritama zaštite CAST-128, IDEA ili 3DES. Koristi se 64-bitni cipher feedback (CFB) mod funkcionisanja.
- Kao i obično, mora se razmotriti pitanje distribucije ključeva.
- U PGP, svaki ključ simetričnih algoritama se koristi samo jednom. Odnosno, novi ključ se generiše kao slučajni 128-bitni broj za svaku poruku.
- U dokumentaciji se ovaj ključ naziva ključ sesije, iako zapravo predstavlja one-time ključ.
- S obzirom da se upotrebljava samo jedanput, ključ sesije se vezuje za poruku i prenosi zajedno sa njom. Da bi se zaštitio, ključ sesije se šifruje pomoću javnog ključa primaoca.

PGP opis servisa - tajnost

- Sekvenca je sledeća:

1. Pošiljalac generiše poruku i slučajni 128-bitni broj, koji će se koristiti kao ključ sesije, samo za ovu poruku.
2. Poruka se šifruje korišćenjem CAST-128 (ili IDEA ili 3DES) sa ključem sesije.
3. Ključ sesije se šifruje pomoću RSA sa javnim ključem primaoca i zatim se dodaje poruci.
4. Primalac koristi RSA sa svojim privatnim ključem da dešifruje i dobije ključ sesije.
5. Ključ sesije se koristi za dešifrovanje poruke.



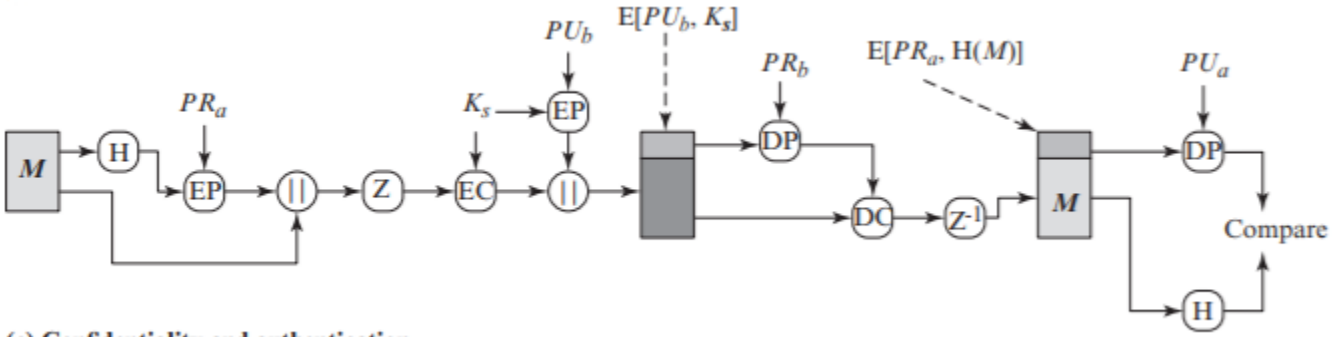
(b) Confidentiality only

PGP opis servisa - tajnost

- Kao alternativu korišćenju RSA za šifrovanje ključa, PGP pruža mogućnost izbora opcije korišćenja Diffie-Hellman algoritma za razmenu ključeva.
- Nekoliko zapažanja vezanih za PGP tajnost:
  - da bi se smanjilo vreme šifrovanja koristi se kombinacija simetričnih algoritama i algoritama za šifrovanje pomoću javnog ključa, umesto da se samo koristi RSA ili ElGamal (verzija Diffie-Hellman-a koja omogućava šifrovanje) za direktno šifrovanje poruke. Simetrični algoritmi su znatno brži od algoritama sa javnim ključem.
  - korišćenje algoritama sa javnim ključem rešava problem distribucije ključa, jer samo primalac može doći do ključa sesije, koji dešifruje poruku.
  - upotreba one-time ključa pojačava već jake simetrične algoritme zaštite. To znači da ako je šifrovanje pomoću javnog ključa bezbedno, čitava šema je bezbedna. U ovu svrhu, PGP pruža korisnicima opseg veličina ključa od 768 do 3072 bita (DSS ključ za potpise je ograničen na 1024 bita).

PGP opis servisa – tajnost i autentikacija

- Na istu poruku mogu se primeniti oba servisa.
  - prvo se generiše potpis za poruku i doda na poruku,
  - zatim se poruka i potpis šifruju korišćenjem CAST-128 (ili IDEA ili 3DES), a ključ sesije se šifrira korišćenjem RSA (ili ElGamal).
- Ovakva sekvenca je bolja od obrnute (šifrovanje, pa onda potpis). Praktično je zgodnije čuvati potpis zajedno sa originalnom porukom. U slučaju verifikacije pomoću treće strane, ako je prvo primenjen potpis, treća strana ne mora da se zamara sa ključem za simetrični algoritam da bi obavila verifikaciju.
- U suštini, kada se koriste oba servisa, pošiljalac najpre potpiše poruku pomoću svog privatnog ključa, zatim šifrira poruku pomoću ključa sesije i na kraju šifrira ključ sesije pomoću javnog ključa primaoca.



(c) Confidentiality and authentication

PGP opis servisa - kompresija

- Podrazumevano, PGP kompresuje poruke nakon što se primeni potpis, ali pre šifrovanja. Na ovaj način se vrši ušteda prostora i za elektronsku poštu i za čuvanje podataka u fajlu.
- Pozicija algoritma kompresije, označavanog sa Z za kompresiju i Z^{-1} za dekompresiju, je kritična:
- Potpis se generiše pre kompresije iz dva razloga:

1. Poželjno je da se potpiše nekompresovana poruka, kako bi se mogla čuvati samo nekompresovana poruka i potpis za buduću verifikaciju. Ako se potpiše kompresovana poruka, onda mora da se čuva kompresovana poruka za verifikaciju ili da se poruka rekompresuje kada se zahteva verifikacija.
    - Čak iako bismo bili voljni da dinamički generišemo rekompresovanu verziju poruke u trenutku verifikacije, PGP-ov algoritam kompresije predstavlja poteškoću. Algoritam nije deterministički. Različite implementacije algoritma postižu različite odnose brzine komprimovanja i procenta kompresije, što kao rezultat daje različite komprimovane forme. Međutim, ti različiti algoritmi kompresije su kompatibilni, tj. svaka verzija algoritma može korektno da dekompresuje izlaz bilo koje od ostalih verzija algoritma. Primena heš algoritma i potpisa nakon kompresije bi ograničila sve PGP implementacije na istu verziju algoritma kompresije.
2. Šifrovanje poruke se primenjuje nakon kompresije da se pojača kriptografska sigurnost. Kompresovana poruka ima manje redudantnosti neko originalna, pa je kriptoanaliza teža.

- Algoritam kompresije koji se koristi je ZIP.

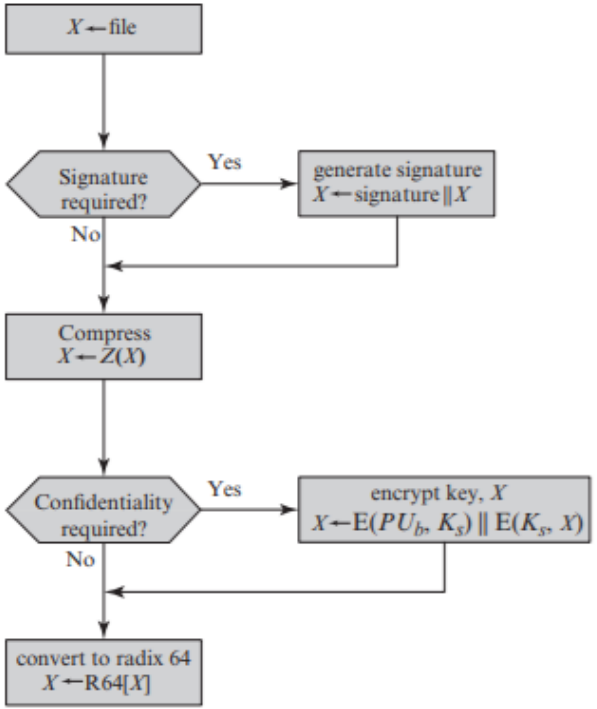
PGP opis servisa – email kompatibilnost

- Kada se koristi PGP barem deo bloka za prenos je šifrovan. Zato se deo ili svi rezultujući blokovi sastoje od toka od 8-bitnih okteta. Međutim, mnogi sistemi elektronske pošte dozvoljavaju korišćenje samo blokova koji se sastoje od ASCII teksta. Da bi se zadovoljila ova restriktivnost, PGP obezbeđuje servis koji konvertuje sirovi 8-bitni binarni tok u tok ASCII karaktera.
- Šema koja se koristi za ovu konverziju je radix-64 konverzija. Svaka grupa od tri okteta binarnih podataka se mapira u četiri ASCII karaktera. Ovaj format takođe dodaje i CRC za detekciju grešaka u prenosu.
- Upotreba radix 64 proširuje poruku za 33%.
- Na sreću, ključ sesije i potpis su relativno kompaktni, a sama poruka je kompresovana.
- Ako ignorišemo ključ sesije i potpis koji zauzimaju relativno mali deo poruke, tipičan opšti efekat kompresije i ekspanzije fajla veličine X bio bi

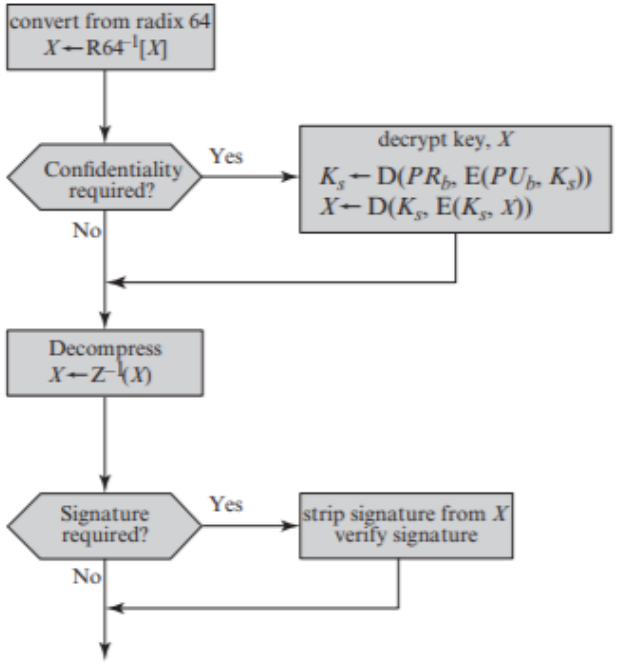
$$1.33 \times 0.5 \times X = 0.665 \times X.$$

- Dakle, i dalje postoji ukupna kompresija od otprilike jedne trećine.
- Karakteristika radix-64 algoritma je i to da sve što dobije na ulazu prevodi u radix-64 format, bez obzira na sadržaj ulaza, čak i ako je to ASCII tekst.
- Tako da, ako je poruka potpisana, a nije šifrovana i zatim je primenjena konverzija na ceo blok, izlaz neće biti čitljiv običnom posmatraču, što pruža dodatni nivo tajnosti.
- PGP ima mogućnost da se konfiguriše tako da se konverzija primenjuje samo na potpis poruke. Ovo omogućava korisnike da čitaju poruku normalno, ali je i dalje potreban PGP za verifikaciju.

PGP opis servisa – dijagrami toka za slanje i prijem



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

PGP opis servisa - segmentacija

- Kod elektronske pošte često postoji ograničenje maksimalne dužine poruke. Često je dužina poruke ograničena od strane aplikacija za elektronsku poštu na 50000 okteta. Svaka duža poruka od te mora se razbiti na segmente koji se šalju nezavisno.
- Da bi zadovoljio ovo ograničenje, PGP automatski deli poruku koja je previše velika u segmente koji su dovoljno mali za slanje putem elektronske pošte. Ova segmentacija se izvršava nakon što se završe svi ostali procesi sa porukom, uključujući i radix-64 konverziju. Samim tim, ključ sesije i potpis se pojavljuju samo jedanput na početku prvog segmenta. Na primajućoj strani, PGP mora da skine sva zaglavlja elektronske pošte i sastavi ceo originalni blok pre nego što počne sa standardnim koracima dijagrama toka za prijem.

PGP ključevi

- PGP koristi četiri tipa ključeva:
  - one-time ključevi sesije za simetrične algoritme,
  - javni ključevi,
  - privatni ključevi,
  - i passphrase-based ključevi za simetrične algoritme.
- Tri posebna zahteva mogu se formulisati uzimajući u obzir ove ključeve:

1. Potreban je način generisanja nepredvidivih ključeva sesije.
2. Želeli bismo da omogućimo korisniku da ima nekoliko parova javnih i privatnih ključeva. Jedan razlog je da bi mogao da menja par povremeno. Kada se to dogodi sve poruke koje su čekale na slanje su poslate korišćenjem starog ključa. Takođe, korisnici koji primaju poruku, koriste stari ključ, sve dok ne dobiju novi. Drugi razlog bi bio taj da korisnik želi da komunicira sa više grupa drugih korisnika i za svaku da koristi poseban par ključeva. Dakle, ne postoji korespodencija jedan na jedan između korisnika i njihovih javnih ključeva. Ovo znači da je potreban neki način za identifikovanje ključeva.
3. Svaki PGP entitet mora održavati fajl sa svojim parovima javnih i privatnih ključeva, kao i fajl sa javnim ključevima njegovih korespondenata.

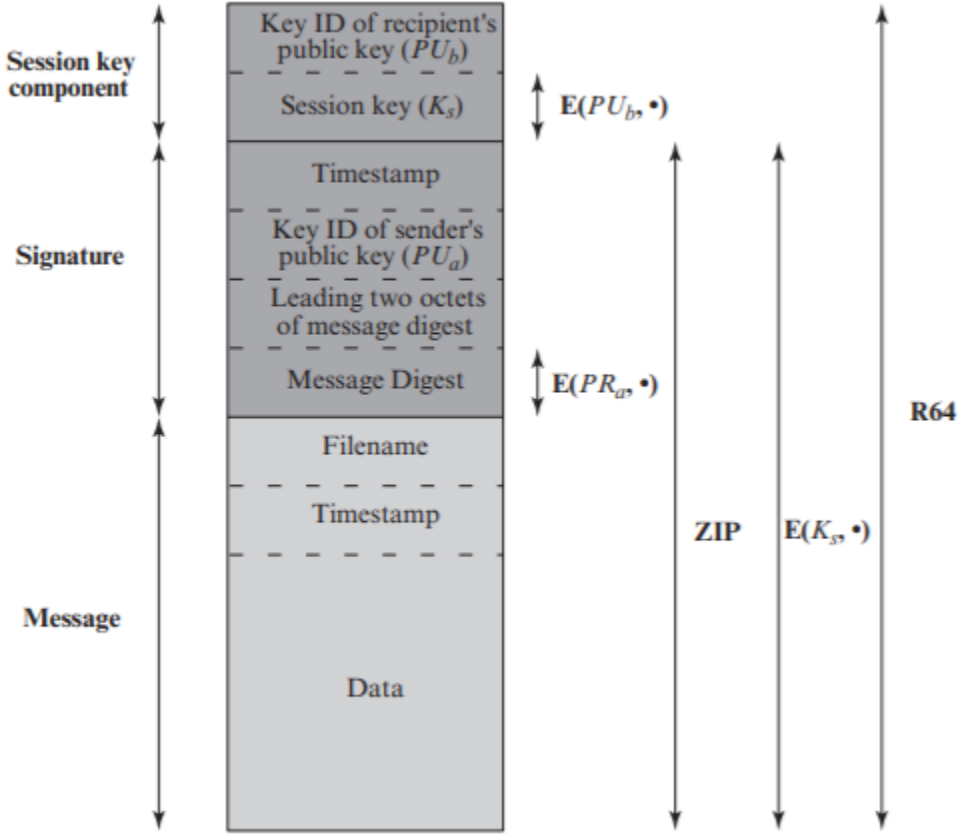
PGP ključevi – generisanje ključeva sesije

- Svaki ključ sesije se povezuje sa samo jednom porukom i koristi se za šifrovanje i dešifrovanje samo te poruke.
- Pretpostavimo da koristimo CAST-128 algoritam (ANSI X12.17).
- Slučajne 128-bitne brojeve generiše sam CAST-128. Ulaz generatora slučajnih brojeva sastoji se od 128-bitnog ključa i dva 64-bitna bloka koja predstavljaju poruku za šifrovanje. Korišćenjem cipher feedback moda, CAST-128 šifrovanjem proizvodi dva 64-bitna šifrovana bloka, koji se kontateniraju i formiraju 128-bitni ključ sesije.
- Ulaz obične poruke generatora slučajnih brojeva, koji se sastoji od dva 64-bitna bloka, se izvodi od toka 128-bitnih slučajnih brojeva. Ovi brojevi zasnovani su na pritisku dirki na tastaturi od strane korisnika. Ovaj slučajni ulaz se kombinuje sa prethodnim ključem sesije koji je bio izlaz CAST-128 i formira ulazni ključ generatora.
- Rezultat je da se proizvodi sekvenca ključeva sesije koja je efektivno nepredvidiva.

PGP ključevi – identifikacija ključa

- Ako postoji jedan par privatni/javni ključ - nema problema.
- Ako postoji više parova privatni/javni ključ - problem, koji ključ upotrebiti za dešifrovanje - potrebna identifikacija ključeva.
- Jedno rešenje - poslati javni ključ korišćen za šifrovanje zajedno sa porukom - nepotrebno gubljenje prostora - RSA javni ključ može biti jako velik.
- Drugo rešenje bi bilo da se dodeli identifikator svakom javnom ključu i da bude jedinstven, barem na nivou jednog korisnika. Tako bi kombinacija korisničkog ID-a i ID-a ključa bila dovoljna da upotpunosti identifikuje ključ. Tada bi bilo potrebno prenositi samo ID ključa koji je mnogo kraći od samog ključa. Problem: menadžment - ID ključa mora biti takav da i pošiljalac i primalac mogu da ga mapiraju u javni ključ (tabele mapiranja).
- Rešenje koje se koristi u PGP-u je da se dodeli ID ključa svakom javnom ključu koji je, sa velikom verovatnoćom, jedinstven u okviru korisnikovog ID-a. ID ključa povezanog sa svakim javnim ključem se sastoji od njegovih najmanje značajnih 64 bita. Odnosno, ID ključa javnog ključa PUa je ($PUa \bmod 2^{64}$).
- ID ključa je takođe neophodan za PGP digitalni potpis. Pošiljalac može da koristi jedan od mnogo privatnih ključeva za šifrovanje, a primalac mora da zna sa kojim javnim ključem da dešifruje. Tako da i digitalni potpis ima 64-bitni ID ključa.

PGP ključevi – struktura poruke



Poruka se sastoji od tri komponente:

- komponenta poruke, koja obuhvata:
  - podatke,
  - ime fajla i
  - vreme kreiranja,
- potpis (opcioni), koji obuhvata:
  - vreme nastajanja potpisa,
  - 160-bitnu SHA-1 vrednost, izračunatu na osnovu podataka i vremena nastajanja potpisa (zbog replay napada), šifrovanu pomoću privatnog ključa pošiljaoca,
  - vodeća dva okteta prethodne vrednosti, da bi se omogućilo primaocu da proveri da li je iskoristio pravi javni ključ za dešifrovanje, upoređujući ovu vrednost sa prva dva okteta dešifrovane, ali i za proveru ispravnosti prenosa,
  - ID ključa javnog ključa pošiljaoca,
- Komponenta poruke i opcioni potpis mogu biti kompresovani i šifrovani ključem sesije.
- Ceo blok se obično konvertuje pomoću radix-64 konverzije.

PGP ključevi – prstenovi ključeva

- ID ključeva je kritično za operacije PGP-a.
- Dva ID-a ključa su uključena u svaku PGP poruku koja obezbeđuje tajnost i autentikaciju.
- Ovi ključevi moraju biti smešteni i organizovani na sistematičan način koji je efikasan za korišćenje od svih strana.
- Šema koja se koristi u PGP-u je da se obezbedi par struktura podataka za svakog korisnika, u jednoj bi se čuvali parovi javnih/privatnih ključeva koji su u vlasništvu tog korisnika, a u drugoj bi se čuvali javni ključevi svih ostalih korisnika za koje taj korisnik zna. Ove strukture podataka se nazivaju prsten privatnih ključeva i prsten javnih ključeva, respektivno.

PGP ključevi – prsten privatnih ključeva

- Timestamp: datum/vreme kada je par ključeva generisan.
- Key ID: najmanje značajnih 64 bita javnog ključa za taj ulaz.
- Public key: javni ključ iz para.
- Private key: privatni ključ iz para; ovo polje je šifrovano.
- User ID: Tipično, e-mail adresa korisnika

Private Key Ring				
Timestamp	**Key ID***	**Public Key**	**Encrypted Private Key**	**User ID***
• • •	• • •	• • •	• • •	• • •
T_i	$PU_i \bmod 2^{64}$	PU_i	$E(H(P_i), PR_i)$	User i
• • •	• • •	• • •	• • •	• • •

PGP ključevi – prsten privatnih ključeva

- Prsten privatnih ključeva može biti indeksiran pomoću ID-a korisnika ili ID-a ključa.
- Iako bi ovaj prsten trebalo da se nalazi samo na mašini korisnika, ima smisla dodatno zaštititi privatni ključ, pa se na njega primenjuje CAST-128 (ili IDEA ili 3DES). Procedura je sledeća:
    1. Korisnik izabere lozinku kojom će se šifrovati privatni ključevi.
    2. Kada sistem generiše novi par ključeva, pita korisnika za lozinku. Koristeći SHA-1, izračunava se 160-bitni heš kod od lozinke.
    3. Sistem šifrira privatni ključ koristeći CAST-128 sa 128 bitnim heš kodom kao ključem.
- Kada korisnik pristupa prstenu privatnih ključeva da dohvati privatni ključ, mora da dostavi lozinku. PGP dohvata šifrovani privatni ključ, generiše heš kod za lozinku, i dešifruje šifrovani privatni ključ koristeći CAST-128 sa heš kodom.
- Ovo je jako kompaktna i efikasna šema. Bezbedna je onoliko koliko je bezbedna lozinka. Korisnik bi trebao da ima lozinku koja se teško pogađa, ali lako pamti.

PGP ključevi – prsten javnih ključeva

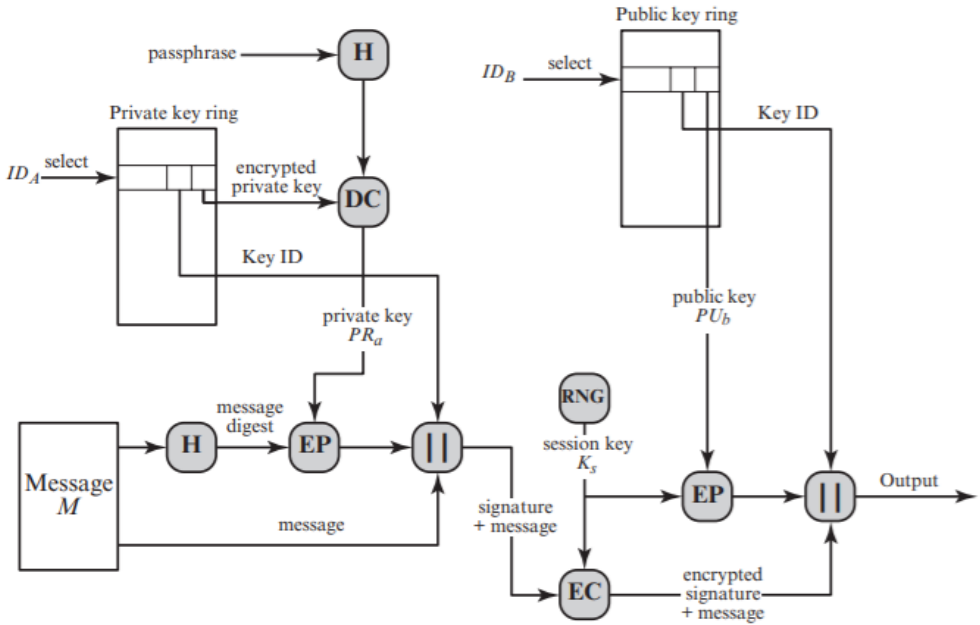
- Timestamp: datum/vreme kada je ovaj ulaz generisan.
- Key ID: najmanje značajnih 64 bita javnog ključa za ovaj ulaz.
- Public Key: javni ključ za ovaj ulaz.
- User ID: identifikuje vlasnika ovog ključa.

Public Key Ring							
Time-stamp	**Key ID***	**Public Key**	**Owner Trust**	**User ID***	**Key Legitimacy**	**Signature(s)**	**Signature Trust(s)**
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
T_i	$PU_i \bmod 2^{64}$	PU_i	trust_flag_i	User i	trust_flag_i		
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
* = field used to index table							

PGP generisanje i prijem poruke – generisanje poruke

PGP entitet koji šalje poruku radi sledeće:

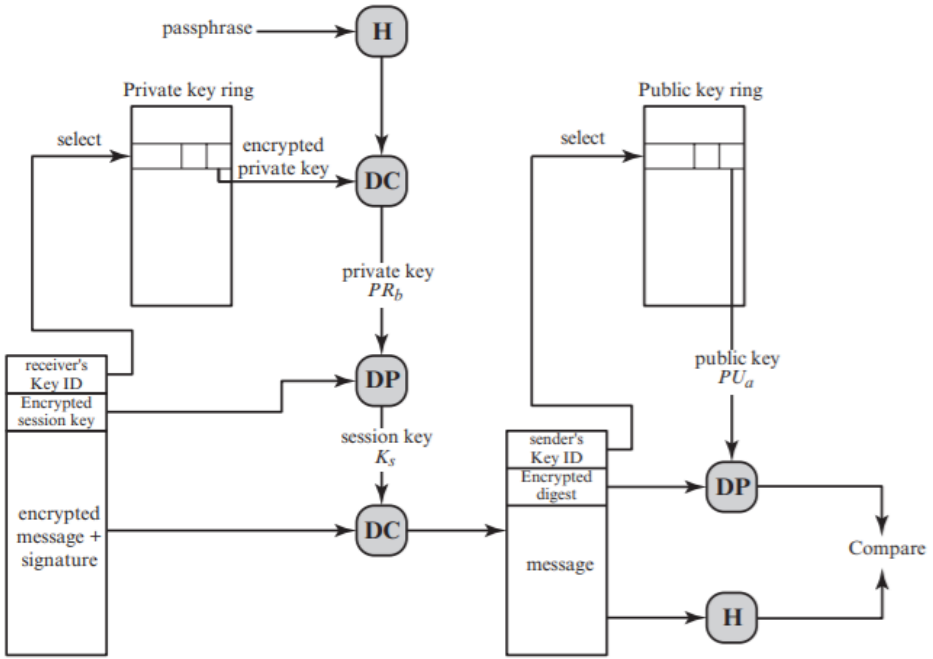
- Potpisivanje poruke
  - PGP dohvata privatni ključ pošiljaoca iz prstena privatnih ključeva koristeći korisnički ID kao indeks. Ako korisnički ID nije dat u komandi, dohvata se prvi privatni ključ iz prstena.
  - PGP traži od korisnika lozinku da izračuna dešifrovani privatni ključ.
  - Komponenta potpisa poruke je konstruisana.
- Šifrovanje poruke
  - PGP generiše ključ sesije i šifruje poruku.
  - PGP dohvata javni ključ primaoca iz prstena javnih ključeva koristeći korisnički ID kao indeks.
  - Komponenta ključa sesije je konstruisana.



PGP generisanje i prijem poruke – prijem poruke

PGP entitet koji prima poruku radi sledeće:

- Dešifrovanje poruke
  - PGP dohvata privatni ključ primaoca iz prstena privatnih ključeva, koristeći ID ključa kao indeks.
  - PGP traži od korisnika lozinku da bi dobio dešifrovani privatni ključ.
  - PGP zatim dohvata ključ sesije i dešifruje poruku.
- Autentikacija poruke
  - PGP dohvata javni ključ pošiljaoca iz prstena javnih ključeva, koristeći ID ključa kao indeks.
  - PGP otkriva heš kod vrednost primljene poruke.
  - PGP izračunava heš kod za primljenu poruku i upoređuje ga sa primljenim heš kodom radi autentikacije.



PGP upravljanje ključem

- Kao što smo videli, PGP pruža efektivnu tajnost i autentikaciju.
- Da bi sistem bio potpun, potrebno je razmotriti i upravljanje javnim ključevima.
- PGP pruža strukturu za rešavanje ovog problema, sa nekoliko predloženih opcija koje se mogu koristiti. Pošto je PGP namenjen za korišćenje u različitim formalnim i neformalnim okruženjima nije definisana stroga šema upravljanja ključevima.
- Problem: A mora da ima prsten javnih ključeva svih PGP-ova koji razmenjuju poruke sa njim.
- man in the middle napad
- Neki pristupi za sigurnu razmenu ključeva
    - Fizički preuzeti ključ od B.
    - Verifikovati ključ putem telefona
    - Dohvati B-ov javni ključ od uzajamno poverljivog D.
    - Dohvati B-ov javni ključ od sertifikujućeg autoriteta od poverenja
- Za slučajeve 3 i 4, A bi morao da ima kopiju javnog ključa treće osobe i morao bi da bude siguran da je taj ključ validan.

PGP upravljanje ključem – korišćenje poverenja

- Osnovna struktura je sledeća.
- Svaki ulaz u prstenu javnih ključeva je sertifikat.
- Povezano sa svakim takvim ulazom je polje legitimiteta ključa, koje indikuje koliko PGP veruje da je ovo validan javni ključ za tog korisnika.
- Što je veći nivo poverenja, to je jača veza između korisničkog ID-a za taj ključ.
- Svaki potpis je povezan sa poljem poverenja potpisa koje indikuje koliko PGP korisnik veruje potpisivaču da sertifikuje javne ključeve.
- Konačno, svaki ulaz definiše javni ključ povezan sa vlasnikom, i polje poverenja vlasnika je uključeno i indikuje stepen do koga se ovom javnom ključu veruje da potpisuje druge javne sertifikate.
- Ovaj nivo poverenja određuje korisnik.

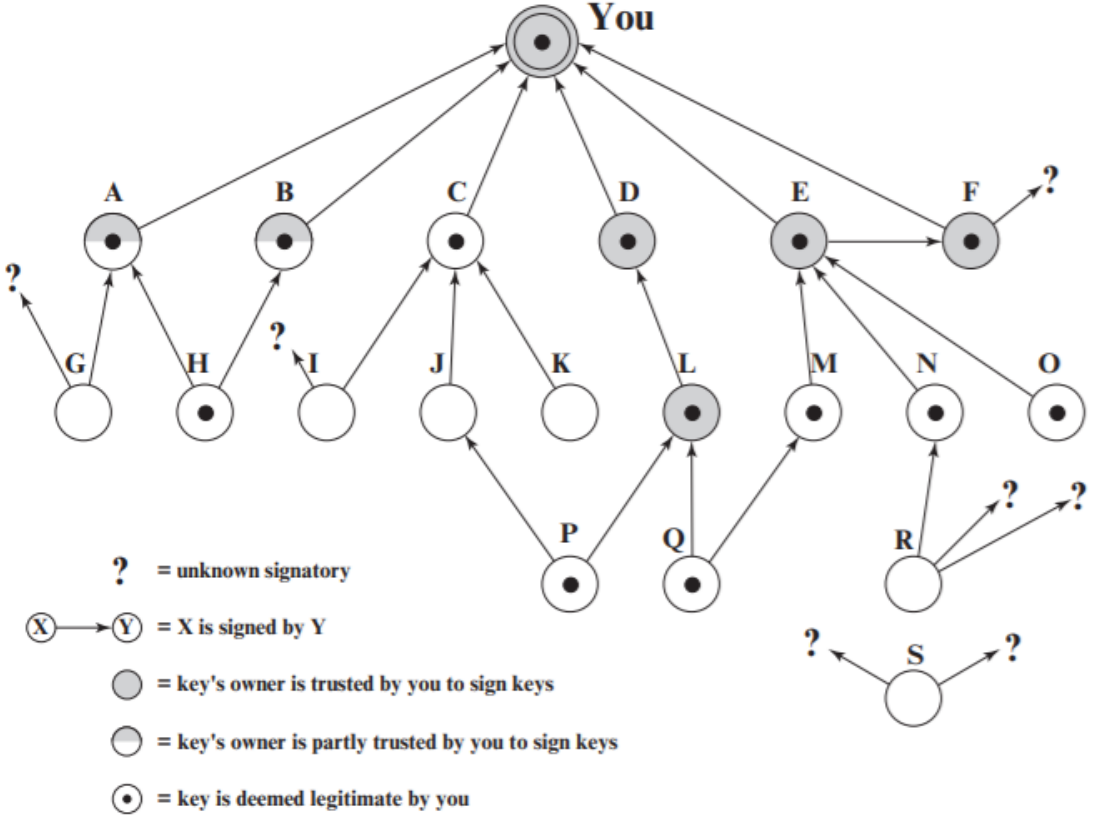
Public Key Ring							
Time-stamp	**Key ID***	**Public Key**	**Owner Trust**	**User ID***	**Key Legitimacy**	**Signature(s)**	**Signature Trust(s)**
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
T_i	$PU_i \bmod 2^{64}$	PU_i	trust_flag_i	User i	trust_flag_i		
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
* = field used to index table							

PGP upravljanje ključem – korišćenje poverenja

- Kada A ubaci novi javni ključ u prsten javnih ključeva, PGP mora da dodeli vrednost flegu poverenja koji je povezan sa vlasnikom ovog javnog ključa. Ako je vlasnik A, tada se vrednost potpunog poverenja dodeljuje ovom polju automatski. U suprotnom, PGP pita A za njegovu procenu poverenja koje se treba dodeliti vlasniku ovog ključa, i A mora da unese željeni nivo. Korisnik može da specificira da je taj vlasnik nepoznat, nepoverljiv, delimično poverljiv i potpuno poverljiv.
- Kada se novi javni ključ unese, jedan ili više potpisa mogu biti zakačeni za njega. Kasnije se može dodati još potpisa. Kada se potpis ubaci u ulaz, PGP pretražuje prsten javnih ključeva da vidi da li je autor potpisa među poznatim vlasnicima javnih ključeva. Ako jeste, tada OWNERTRUST vrednost za ovog vlasnika se postavlja u SIGTRUST polje za taj potpis.U suprotnom se postavlja vrednost nepoznatog korisnika.
- Vrednost polja legitimiteta ključa se računa na osnovu polja poverenja potpisa prisutnih u ovom ulazu. Ukoliko barem jedan potpis ima poverenje potpisa na vrednosti potpuno, tada se polje legitimiteta ključa postavlja na kompletno. U suprotnom, PGP sračunava ovu vrednost na osnovu težinskih suma. Težina 1/X se daje potpisima koji su uvek poverljivi, a 1/Y potpisima koji su uglavnom poverljivi, gde su X i Y konfigurabilni parametri. Kada ukkupna težina dostigne 1, povezanost se smatra verodostojnom, i vrednost polja legitimiteta ključa se postavlja na kompletnu. Tako da u odsustvu potpunog poverenja imamo barem X potpisa kojima uvek verujemo ili Y potpisa kojima uglavnom verujemo ili neka kombinacija ta dva.

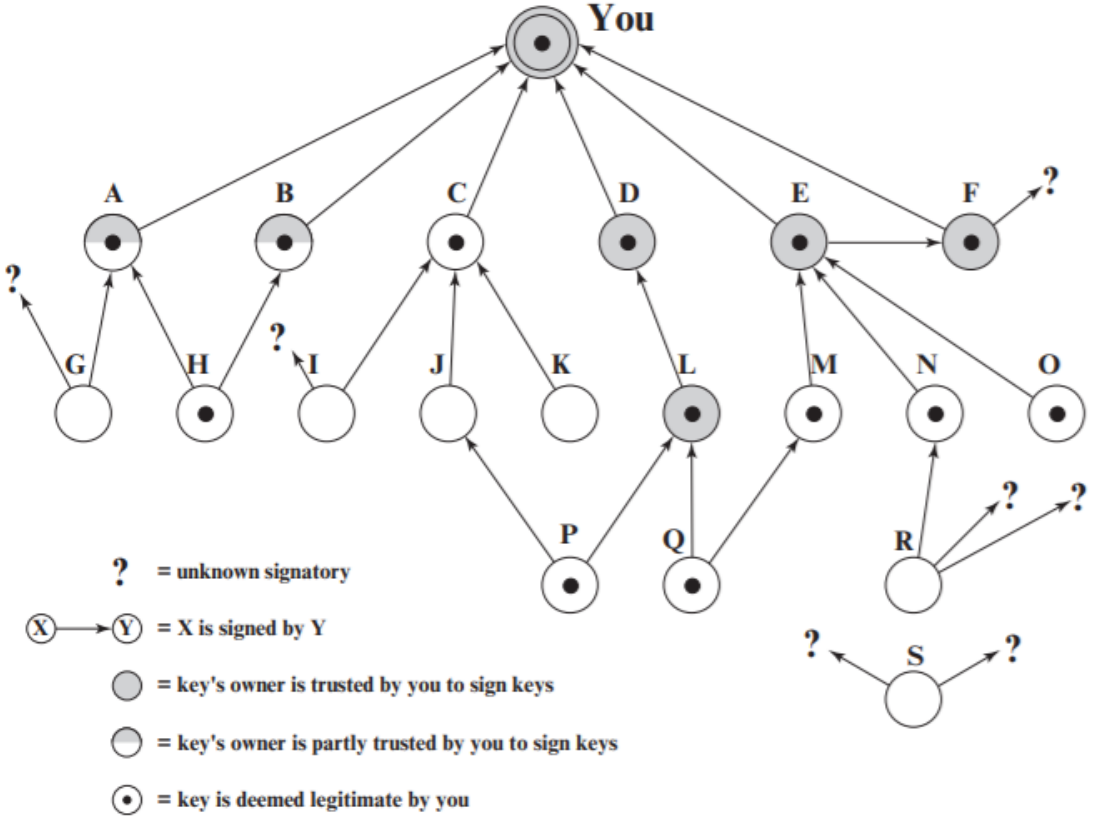
PGP upravljanje ključem – korišćenje poverenja

- "You" ulaz u prstenu javnih ključeva korespodentan sa ovim korisnikom. Ključ - legitiman, OWNERTRUST vrednost je ultimativno (potpuno) poverenje.
- Svaki drugi čvor ima OWNERTRUST nedefinisano, osim ako nije nešto definisano od strane korisnika. U primeru uvek veruje sledećim korisnicima da potpisuju druge ključeve: D, E, F, L. Delimično veruje korisnicima A i B da potpisuju druge ključeve.



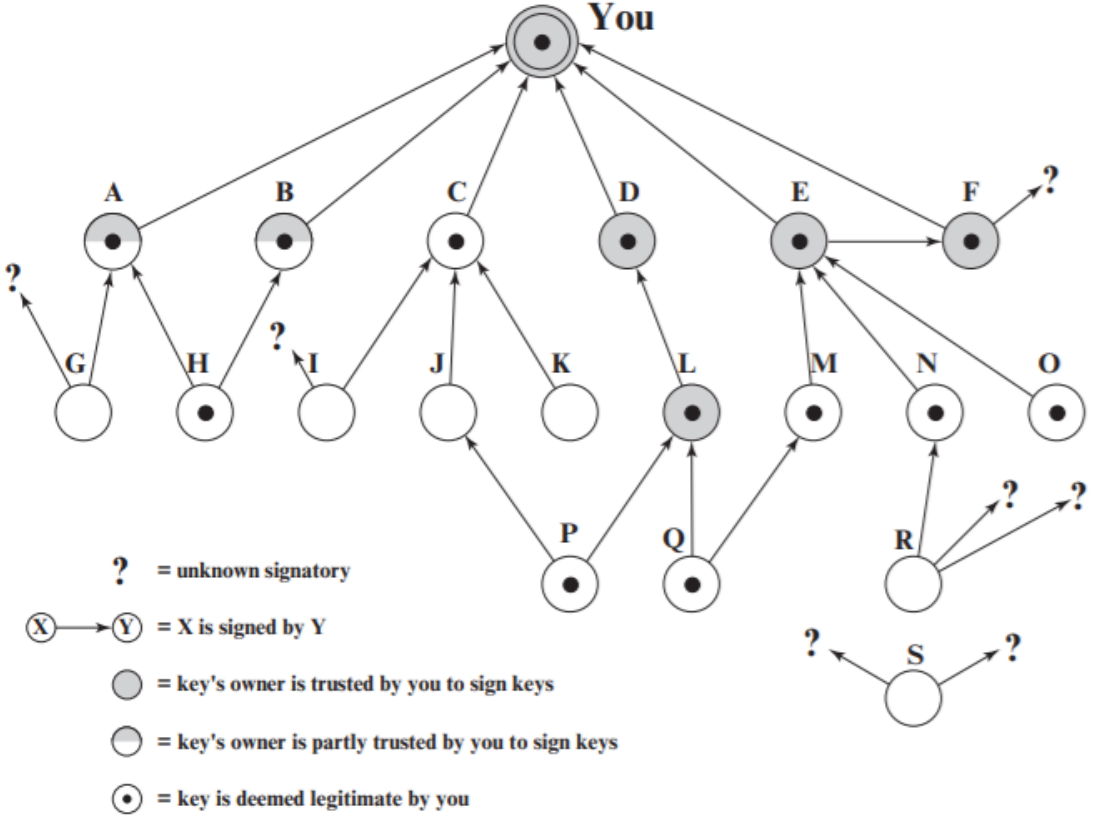
PGP upravljanje ključem – korišćenje poverenja

- Šta je sve ilustrovano u primeru:
- Svi ključevi čiji su vlasnici potpuno ili delimično od poverenja su potpisani od ovog korisnika, osim čvora L. Obično se tako radi. Čak i E koji je potpisan od strane potpuno poverljivog F, je potpisan od strane ovog korisnika.
- Pretpostavljamo da su dva delimično od poverenja korisnika dovoljna da sertifikuju ključ. Otud je ključ H legitiman za PGP jer ga potpisuju A i B, koji su oba delimično od poverenja.



PGP upravljanje ključem – korišćenje poverenja

- Ključ može biti legitiman jer ga potpisuje potpuno poverljiv korisnik ili dva delimično poverljiva korisnika, ali njegov korisnik može da ne bude od poverenja da potpisuje druge ključeve. Na primer, N.
- Prikazan je nepovezan čvor S, sa dva nepoznata potpisa. Takav ključ može biti dobijen od servera ključeva. PGP ne može da pretpostavi da je ovaj ključ legitiman samo zato što je došao sa servera. Korisnik mora da potvrdi legitimitet ključa, tako što će da ga potpiše ili tako što će reći PGP-u da je spreman da u potpunosti veruje jednom od potpisivača ključa.



PGP upravljanje ključem – povlačenje javnih ključeva

- Korisnik može poželeti da povuče svoj javni ključ (kompromitovan je, želi da ga zameni, ...).
- Konvencija za povlačenje javnog ključa je da vlasnik izda sertifikat povlačenja ključa potpisan od strane vlasnika. Sertifikat ima istu formu kao normalni sertifikat potpisa, ali uključuje indikator koji govori da je namena sertifikata da se povuče javni ključ. Vlasnik bi zatim trebalo da pokuša da raširi ovaj sertifikat na što više mesta i što je brže moguće da bi omogućio korespodentima da ažuriraju svoje javne ključeve.

PITANJA?

rti.etf.bg.ac.rs/rti/ir4zp