ЗАШТИТА ПОДАТАКА

Заштита електронске поште

Pretty Good Privacy (PGP)

Преглед

- Биће објашњено:
  - Заштита електронске поште
  - PGP
    - историјат
    - нотација
    - операциони опис
      - аутентикација
      - тајност
      - компресија
      - e-mail компатибилност
      - сегментација
    - криптографски кључеви и прстенови кључева
      - генерисање кључа сесије
      - идентификација кључа
      - прстенови кључева
    - управљање јавним кључем
      - приступи управљању јавним кључем
      - коришћење поверења
      - повлачење јавних кључева

Заштита електронске поште

- Електронска пошта представља једну од најкоришћенијих дистрибуираних апликација.
- Постоји повећана потреба за пружањем аутентикације и тајности као сервиса у склопу електронске поште.
- У оквиру курса обрадићемо два приступа који ће највероватније доминирати у електронској пошти у блиској будућности.
  - Pretty Good Privacy (PGP) је широко коришћена шема која не зависи нити од једне организације или институције, те је због тога прикладна како за личну употребу, тако и за комерцијалну.
  - Secure/Multipurpose Internet Mail Extension (S/MIME) је развијено да буде интернет стандард.

PGP историјат

- Заслугом Phila Zimmermanna, PGP пружа тајност и аутентикацију као сервисе који се могу користити за електронску пошту.
- Zimmermann је урадио следеће:

1. Изабрао најбоље расположиве криптографске алгоритме као саставне делове
2. Интегрисао ове алгоритме у једну апликацију опште намене, која је независна у односу на оперативни систем и процесор и која се заснива на малом скупу команди које су лаке за коришћење
3. Обезбедио је да пакети и њихова документација, укључујући и изворни код, буду бесплатно доступни путем интернета
4. Направио споразум са компанијом (Viacrypt, данас Network Associates) да обезбеди потпуно компатибилну, ниско буџетну комерцијалну верзију PGP-а

PGP историјат(2)

- PGP је доживео експлозивни раст и данас је у широкој употреби.
- Може се навести неколико разлога за такав раст:

1. Доступан је бесплатно у верзијама које раде на различитим платформама, укључујући Windows, UNIX, Macintosh, и многе друге. Поред тога, комерцијална верзија задовољава кориснике који желе производ са подршком произвођача.
2. Базиран је на алгоритмима који су преживели исцрпљујуће јавне расправе и сматрају се изузетно сигурнима. Конкретно, пакет укључује RSA, DSS, и Diffie-Hellman за шифровање помоћу јавног кључа; CAST-128, IDEA, и 3DES за симетрично шифровање; и SHA-1 за хеш шифровање.
3. Има широк спектар употребљивости, од корпорација које желе да изаберу и спроведу стандардизовану шему за шифровање фајлова и порука, до појединачних корисника који желе да комуницирају безбедно са другима широм света, путем интернета и осталих мрежа.
4. Није развијен, нити контролисан, од стране било које организације.
5. PGP је на путу да постане интернет стандард (RFC 4880, RFC 3156).

PGP нотација

- Већина нотације која ће се користити у наставку, већ је раније коришћена, али има и новина.
- Најбоље је зато на почетку да сумирамо све што ће бити коришћено:
  - Ks=кључ сесије коришћен у симетричним алгоритмима
  - PRa=приватни кључ корисника A, коришћен за шиф. јавним кључем
  - PUa=јавни кључ корисника A, коришћен за шиф. јавним кључем
  - EP= шифровање јавним кључем
  - DP= дешифровање јавним кључем
  - EC= шифровање симетричним алгоритмом
  - DC= дешифровање симетричним алгоритмом
  - H= хеш функција
  - ||= конкатенација
  - Z= компресија ZIP алгоритмом
  - R64= конверзија у radix 64 ASCII формат
- У PGP документацији често се користи израз тајни кључ који се односи на кључ који се упарује са јавним кључем код алгоритама за шифровање помоћу јавног кључа. Битно је да не дође до забуне са тајним кључем који се користи у симетричним алгоритмима шифровања. Због тога се може користити термин приватни кључ.

PGP операциони опис

- PGP се састоји од пет сервиса:
  - аутентикације,
  - тајности,
  - компресије,
  - e-mail компатибилности и
  - сегментације.

PGP операциони опис(2)

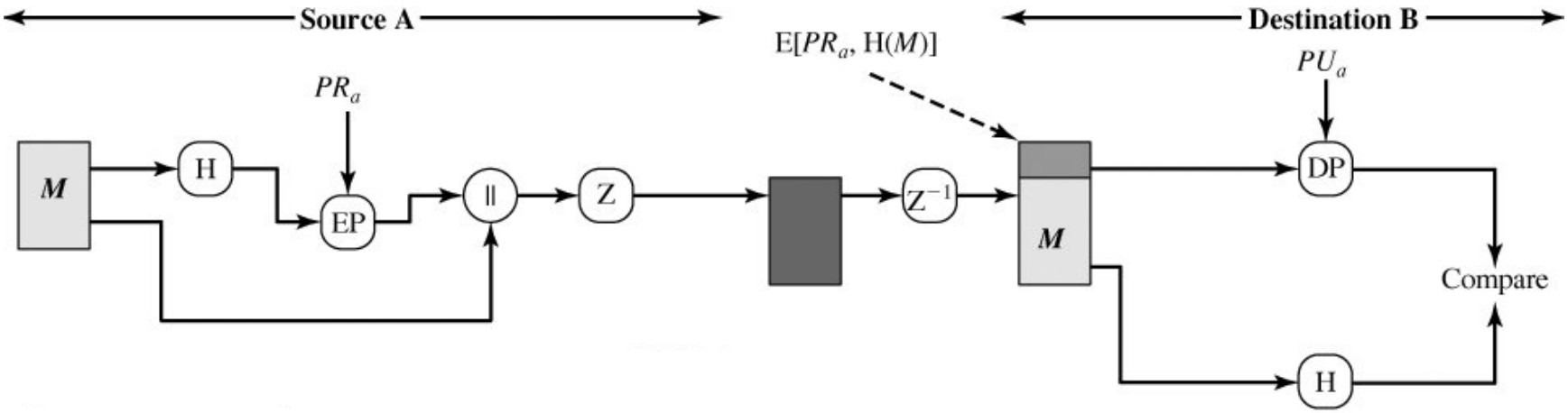
Функција	Алгоритми	Опис коришћења
Дигитални потпис	DSS/SHA или RSA/SHA	Хеш код поруке се креира коришћењем SHA-1. Тако добијена вредност се шифрира помоћу DSS или RSA са приватним кључем пошиљаоца и укључује се у поруку.
Шифровање поруке	CAST или IDEA или 3DES са 3 кључа са Diffie-Hellman или RSA	Порука се шифрује коришћењем CAST-128 или IDEA или 3DES са one-time кључем сесије који је генерисао пошиљалац. Кључ сесије се шифрира коришћењем Diffie-Hellman или RSA са јавним кључем примаоца и укључује се у поруку.
Компресија	ZIP	Порука може бити компресована, за складиштење или пренос, помоћу ZIP-а.
e-mail компатибилност	Radix 64 conversion	Да би се обезбедила транспарентност за email апликације, шифрована порука може се конвертовати у ASCII стринг коришћењем radix 64 конверзије.
Сегментација		Да би избегао ограничења максималне величине поруке, PGP спроводи сегментацију и састављање сегмената.

PGP аутентикација

- Секвенца је следећа:

1. Пошиљалац креира поруку.
2. SHA-1 се користи да се генерише160-битни хеш код поруке.
3. Хеш код се шифрује помоћу RSA коришћењем приватног кључа пошиљаоца и резултат се додаје на поруку.
4. Прималац користи RSA са јавним кључем пошиљаоца да дешифрује хеш код.
5. Прималац генерише нови хеш код за поруку и упоређује га са дешифрованим хеш кодом. Уколико се слажу, порука се прихвата као аутентична.

PGP аутентикација(2)



PGP аутентикација(3)

- Комбинација SHA-1 и RSA обезбеђује ефикасну шему дигиталног потписа.
  - Због јачине RSA, примаоц је сигуран да је једино онај ко поседује упарени приватни кључ могао да генерише потпис.
  - Због јачине SHA-1, примаоц је сигуран да нико други није могао да генерише нову поруку која има исти хеш код, а самим тим, и потпис оригиналне поруке.
- Као алтернатива, потписи могу бити генерисани коришћењем DSS/SHA-1.
- Занимљивост: иако су потписи нормално повезани са поруком или фајлом који потписују, ово не мора увек бити случај. Подржани су и неповезани потписи. Неповезани потпис може се чувати и преносити независно од поруке коју потписује. Ово се користи у неколико случајева:
  - Корисник може хтети да има посебан лог потписа свих послатих или примљених порука.
  - Неповезани потпис извршног програма може да детектује вирус.
  - Користи се када више страна треба да потпише документ, нпр. правни уговор. У супротном, потписи би били угнеждени, тј. потпис другог корисника би био примењен и на документ и на потпис првог заједно, итд.

PGP тајност

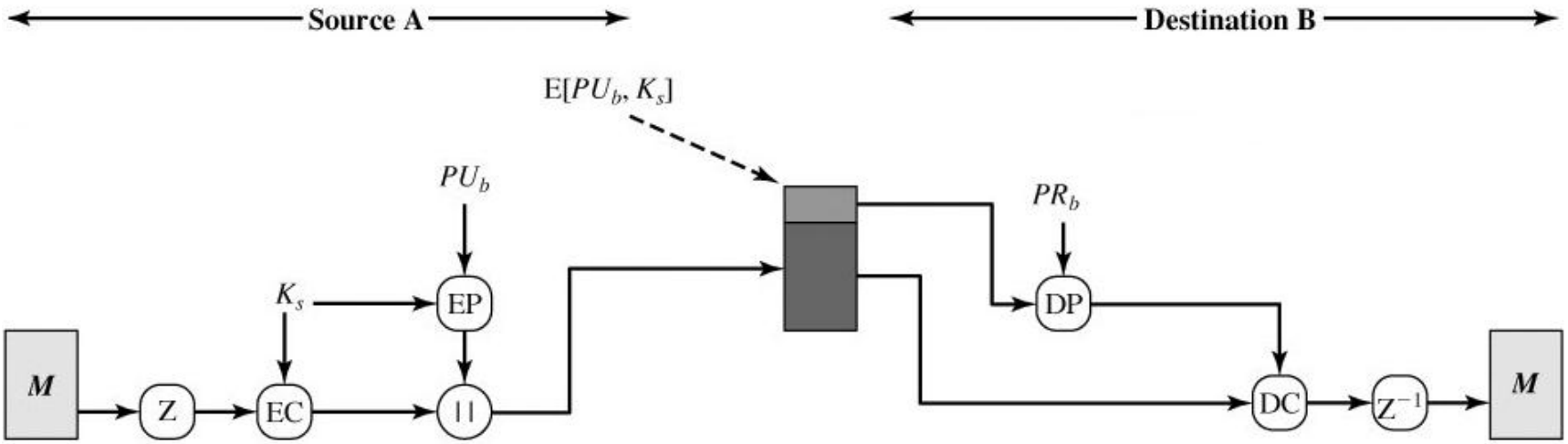
- PGP обезбеђује тајност шифровањем порука за слање или складиштење.
- У оба случаја се користи један од симетричних алгоритама заштите CAST-128, IDEA или 3DES. Користи се 64-битни cipher feedback (CFB) мод функционисања.
- Као и обично, мора се размотрити питање дистрибуције кључева.
- У PGP, сваки кључ симетричних алгоритама се користи само једном. Односно, нови кључ се генерише као случајни128-битни број за сваку поруку.
- У документацији се овај кључ назива кључ сесије, иако заправо представља one-time кључ.
- С обзиром да се употребљава само једанпут, кључ сесије се везује за поруку и преноси заједно са њом. Да би се заштитио, кључ сесије се шифрује помоћу јавног кључа примаоца.

PGP тајност(2)

- Секвенца је следећа:

1. Пошиљалац генерише поруку и случајни 128-битни број, који ће се користити као кључ сесије, само за ову поруку.
2. Порука се шифрује коришћењем CAST-128 (или IDEA или 3DES) са кључем сесије.
3. Кључ сесије се шифрује помоћу RSA са јавним кључем примаоца и затим се додаје поруци.
4. Прималац користи RSA са својим приватним кључем да дешифрује и добије кључ сесије.
5. Кључ сесије се користи за дешифровање поруке.

PGP тајност(3)



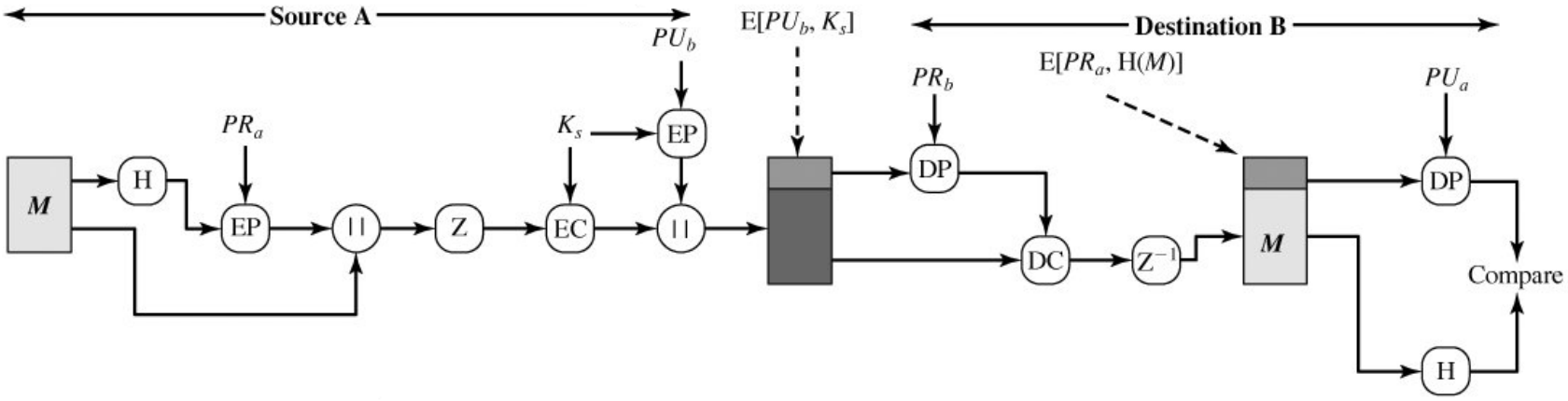
PGP тајност(4)

- Као алтернативу коришћењу RSA за шифровање кључа, PGP пружа могућност избора опције коришћења Diffie-Hellman алгоритма за размену кључева.
- Неколико запажања везаних за PGP тајност:
  - да би се смањило време шифровања користи се комбинација симетричних алгоритама и алгоритама за шифровање помоћу јавног кључа, уместо да се само користи RSA или ElGamal (верзија Diffie-Hellman-а која омогућава шифровање) за директно шифровање поруке. Симетрични алгоритми су знатно бржи од алгоритама са јавним кључем.
  - коришћење алгоритама са јавним кључем решава проблем дистрибуције кључа, јер само прималац може доћи до кључа сесије, који дешифрује поруку.
  - употреба one-time кључа појачава већ јаке симетричне алгоритме заштите. То значи да ако је шифровање помоћу јавног кључа безбедно, читава шема је безбедна. У ову сврху, PGP пружа корисницима опсег величина кључа од 768 до 3072 бита (DSS кључ за потписе је ограничен на 1024 бита).

PGP тајност и аутентикација

- На исту поруку могу се применити оба сервиса.
  - прво се генерише потпис за поруку и дода на поруку,
  - затим се порука и потпис шифрују коришћењем CAST-128 (или IDEA или 3DES), а кључ сесије се шифрира коришћењем RSA (или ElGamal).
- Оваква секвенца је боља од обрнуте (шифровање, па онда потпис). Практично је згоднije чувати потпис заједно са оригиналном поруком. У случају верификације помоћу треће стране, ако је прво примењен потпис, трећа страна не мора да се замара са кључем за симетрични алгоритам да би обавила верификацију.
- У суштини, када се користе оба сервиса, пошиљалац најпре потпише поруку помоћу свог приватног кључа, затим шифрира поруку помоћу кључа сесије и на крају шифрира кључ сесије помоћу јавног кључа примаоца.

PGP тајност и аутентикација(2)



PGP компресија

- Подразумевано, PGP компресује поруке након што се примени потпис, али пре шифровања. На овај начин се врши уштеда простора и за електронску пошту и за чување података у фајлу.
- Позиција алгоритма компресије, означаваног са Z за компресију и Z^{-1} за декомпресију, је критична:

1. Потпис се генерише пре компресије из два разлога:
   a. Пожељно је да се потпише некомпресована порука, како би се могла чувати само некомпресована порука и потпис за будућу верификацију. Ако се потпише компресована порука, онда мора да се чува компресована порука за верификацију или да се порука рекомпресује када се захтева верификација.

PGP компресија(2)

b. Чак иако бисмо били вољни да динамички генеришемо рекомпресовану верзију поруке у тренутку верификације, PGP-ов алгоритам компресије представља потешкоћу. Алгоритам није детерминистички. Различите имплементације алгоритма постижу различите односе брзине компримовања и процента компресије, што као резултат даје различите компримоване форме. Међутим, ти различити алгоритми компресије су компатибилни, тј. свака верзија алгоритма може коректно да декомпресује излаз било које од осталих верзија алгоритма. Примена хеш алгоритма и потписа након компресије би ограничила све PGP имплементације на исту верзију алгоритма компресије.

2. Шифровање поруке се примењује након компресије да се појача криптографска сигурност. Компресована порука има мање редудантности неко оригинална, па је криптоанализа тежа.

- Алгоритам компресије који се користи је ZIP.

PGP e-mail компатибилност

- Када се користи PGP барем део блока за пренос је шифрован. Зато се део или сви резултујући блокови састоје од тока од 8-битних октета. Међутим, многи системи електронске поште дозвољавају коришћење само блокова који се састоје од ASCII текста. Да би се задовољила ова рестриктивност, PGP обезбеђује сервис који конвертује сирови 8-битни бинарни ток у ток ASCII карактера.
- Шема која се користи за ову конверзију је radix-64 конверзија. Свака група од три октета бинарних података се мапира у четири ASCII карактера. Овај формат такође додаје и CRC за детекцију грешака у преносу.

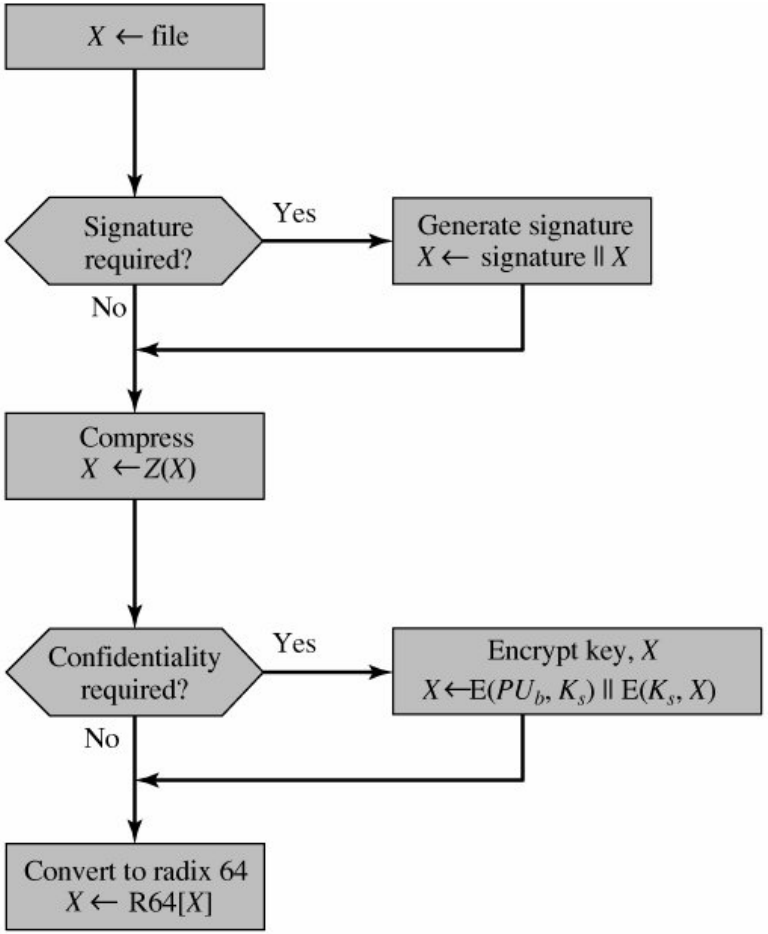
PGP e-mail компатибилност(2)

- Употреба radix 64 проширује поруку за 33%.
- На срећу, кључ сесије и потпис су релативно компактни, а сама порука је компресована.
- Ако игноришемо кључ сесије и потпис који заузимају релативно мали део поруке, типичан општи ефекат компресије и експанзије фајла величине X био би

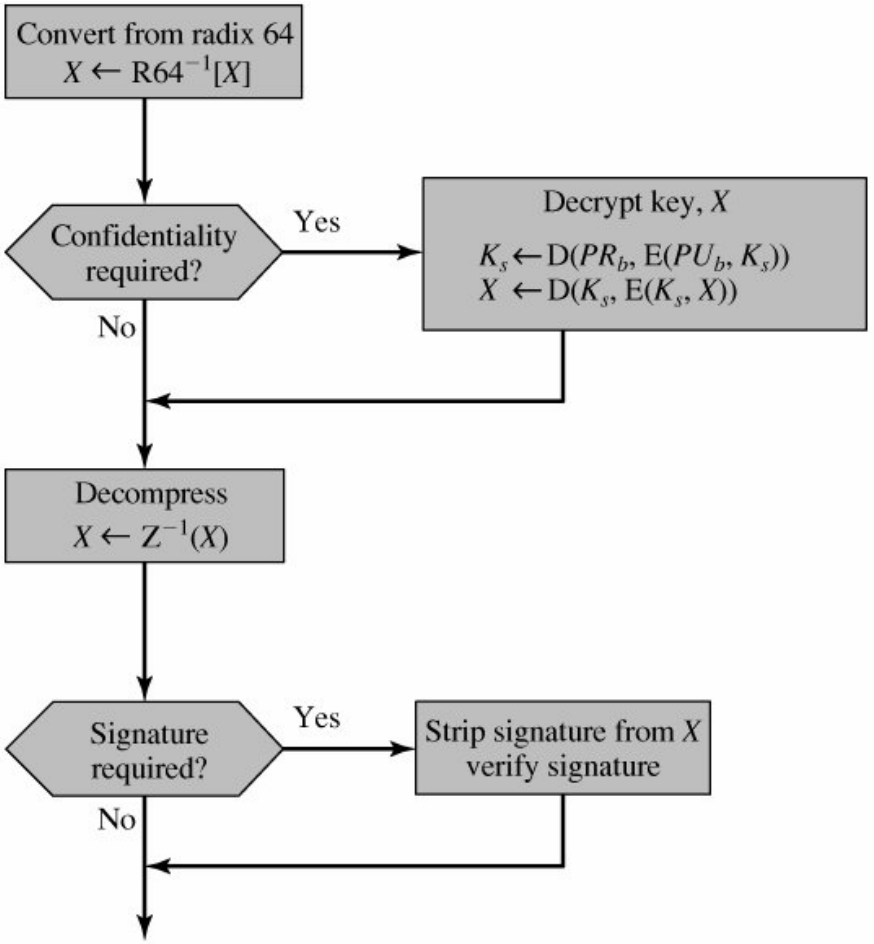
$$1.33 \times 0.5 \times X = 0.665 \times X.$$

- Дакле, и даље постоји укупна компресија од отприлике једне трећине.
- Карактеристика radix-64 алгоритма је и то да све што добије на улазу преводи у radix-64 формат, без обзира на садржај улаза, чак и ако је то ASCII текст.
- Тако да, ако је порука потписана, а није шифрована и затим је примењена конверзија на цео блок, излаз неће бити читљив обичном посматрачу, што пружа додатни ниво тајности.
- PGP има могућност да се конфигурише тако да се конверзија примењује само на потпис поруке. Ово омогућава кориснике да читају поруку нормално, али је и даље потребан PGP за верификацију.

PGP дијаграм тока за слање



PGP дијаграм тока за пријем



PGP сегментација

- Код електронске поште често постоји ограничење максималне дужине поруке. Често је дужина поруке ограничена од стране апликација за електронску пошту на 50000 октета. Свака дужа порука од те мора се разбити на сегменте који се шаљу независно.
- Да би задовољио ово ограничење, PGP аутоматски дели поруку која је превише велика у сегменте који су довољно мали за слање путем електронске поште. Ова сегментација се извршава након што се заврше сви остали процеси са поруком, укључујући и radix-64 конверзију. Самим тим, кључ сесије и потпис се појављују само једанпут на почетку првог сегмента. На примајућој страни, PGP мора да скине сва заглавља електронске поште и састави цео оригинални блок пре него што почне са стандардним корацима дијаграма тока за пријем.

PGP кључеви и прстенови кључева

- PGP користи четири типа кључева:
  - one-time кључеви сесије за симетричне алгоритме,
  - јавни кључеви,
  - приватни кључеви,
  - и passphrase-based кључеви за симетричне алгоритме.
- Три посебна захтева могу се формулисати узимајући у обзир ове кључеве:

1. Потребан је начин генерисања непредвидивих кључева сесије.
2. Желели бисмо да омогућимо кориснику да има неколико парова јавних и приватних кључева. Један разлог је да би могао да мења пар повремено. Када се то догоди све поруке које су чекале на слање су послате коришћењем старог кључа. Такође, корисници који примају поруку, користе стари кључ, све док не добију нови. Други разлог би био тај да корисник желе да комуницира са више група других корисника и за сваку да користи посебан пар кључева. Дакле, не постоји коресподенција један на један између корисника и њихових јавних кључева. Ово значи да је потребан неки начин за идентификовање кључева.
3. Сваки PGP ентитет мора одржавати фајл са својим паровима јавних и приватних кључева, као и фајл са јавним кључевима његових кореспондената.

PGP генерисање кључа сесије

- Сваки кључ сесије се повезује са само једном поруком и користи се за шифровање и дешифровање само те поруке.
- Претпоставимо да користимо CAST-128 алгоритам (ANSI X12.17).
- Случајне 128-битне бројеве генерише сам CAST-128. Улаз генератора случајних бројева састоји се од 128-битног кључа и два 64-битна блока која представљају поруку за шифровање. Коришћењем cipher feedback мода, CAST-128 шифровањем производи два 64-битна шифрована блока, који се контатенирају и формирају 128-битни кључ сесије.
- Улаз обичне поруке генератора случајних бројева, који се састоји од два 64-битна блока, се изводи од тока 128-битних случајних бројева. Ови бројеви засновани су на притиску дирки на тастатури од стране корисника. Овај случајни улаз се комбинује са претходним кључем сесије који је био излаз CAST-128 и формира улазни кључ генератора.
- Резултат је да се производи секвенца кључева сесије која је ефективно непредвидива.

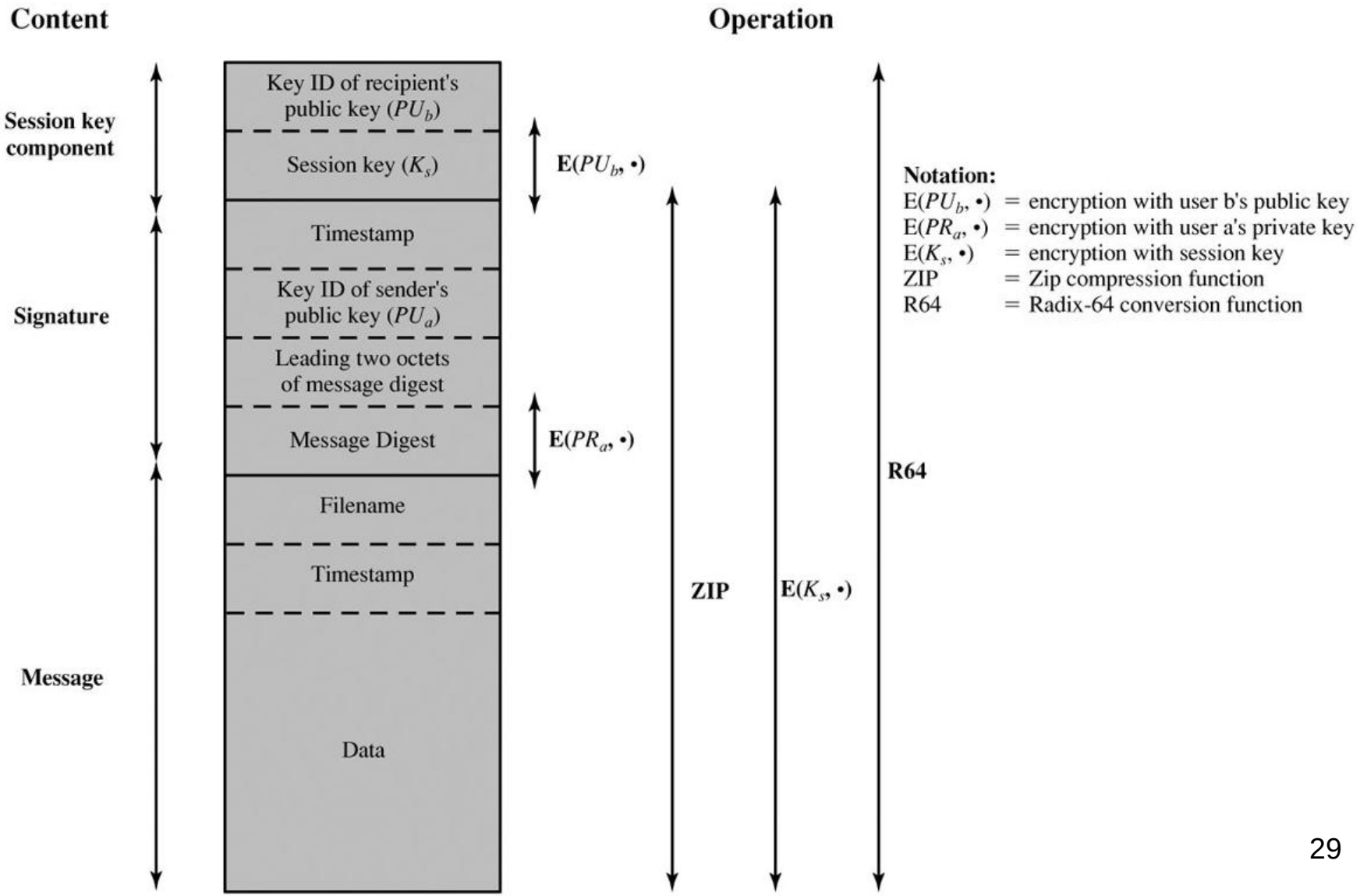
PGP идентификација кључа

- Ако постоји један пар приватни/јавни кључ - нема проблема.
- Ако постоји више парова приватни/јавни кључ - проблем, који кључ употребити за дешифровање - потребна идентификација кључева.
- Једно решење - послати јавни кључ коришћен за шифровање заједно са поруком - непотребно губљење простора - RSA јавни кључ може бити јако велик.
- Друго решење би било да се додели идентификатор сваком јавном кључу и да буде јединствен, барем на нивоу једног корисника. Тако би комбинација корисничког ID-а и ID-а кључа била довољна да употпуности идентификује кључ. Тада би било потребно преносити само ID кључа који је много краћи од самог кључа. Проблем: менаџмент - ID кључа мора бити такав да и пошиљалац и примаоц могу да га мапирају у јавни кључ (табеле мапирања).

PGP идентификација кључа(2)

- Решење које се користи у PGP-у је да се додели ID кључа сваком јавном кључу који је, са великом вероватноћом, јединствен у оквиру корисниковог ID-а. ID кључа повезаног са сваким јавним кључем се састоји од његових најмање значајних 64 бита. Односно, ID кључа јавног кључа PUa је (PUa mod 2^{64}).
- ID кључа је такође неопходан за PGP дигитални потпис. Пошиљалац може да користи један од много приватних кључева за шифровање, а прималац мора да зна са којим јавним кључем да дешифрује. Тако да и дигитални потпис има 64-битни ID кључа.

PGP структура поруке



PGP структура поруке(2)

- Порука се састоји од три компоненте:
  - компонента поруке, која обухвата:
    - податке,
    - име фајла и
    - време креирања,
  - потпис (опциони), који обухвата:
    - време настајања потписа,
    - 160-битну SHA-1 вредност, израчунату на основу података и времена настајања потписа (због replay напада), шифровану помоћу приватног кључа пошиљаоца,
    - водећа два октета претходне вредности, да би се омогућило примаоцу да провери да ли је искористио прави јавни кључ за дешифровање, упоређујући ову вредност са прва два октета дешифроване, али и за проверу исправности преноса,
    - ID кључа јавног кључа пошиљаоца,
  - компонента кључа сесије (опционо), која обухвата:
    - кључ сесије и
    - ID кључа јавног кључа примаоца.
- Компонента поруке и опциони потпис могу бити компресовани и шифровани кључем сесије.
- Цео блок се обично конвертује помоћу radix-64 конверзије.

PGP прстенови кључева

- ID кључева је критично за операције PGP-а.
- Два ID-а кључа су укључена у сваку PGP поруку која обезбеђује тајност и аутентикацију.
- Ови кључеви морају бити смештени и организовани на систематичан начин који је ефикасан за коришћење од свих страна.
- Шема која се користи у PGP-у је да се обезбеди пар структура података за сваког корисника, у једној би се чували парови јавних/приватних кључева који су у власништву тог корисника, а у другој би се чували јавни кључеви свих осталих корисника за које тај корисник зна. Ове структуре података се називају прстен приватних кључева и прстен јавних кључева, респективно.

PGP прстен приватних кључева

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 прстен приватних кључева(2)

- Timestamp: датум/време када је пар кључева генерисан.
- Key ID: најмање значајних 64 бита јавног кључа за тај улаз.
- Public key: јавни кључ из пара.
- Private key: приватни кључ из пара; ово поље је шифровано.
- User ID: Типично, e-mail адреса корисника

PGP прстен приватних кључева(3)

- Прстен приватних кључева може бити индексиран помоћу ID-а корисника или ID-а кључа.
- Иако би овај прстен требало да се налази само на машини корисника, има смисла додатно заштитити приватни кључ, па се на њега примењује CAST-128 (или IDEA или 3DES). Процедура је следећа:
  1. Корисник изабере лозинку којом ће се шифровати приватни кључеви.
  2. Када систем генерише нови пар кључева, пита корисника за лозинку. Користећи SHA-1, израчунава се160-битни хеш код од лозинке.
  3. Систем шифрира приватни кључ користећи CAST-128 са 128 битним хеш кодом као кључем.
- Када корисник приступа прстену приватних кључева да дохвати приватни кључ, мора да достави лозинку. PGP дохвата шифровани приватни кључ, генерише хеш код за лозинку, и дешифрује шифровани приватни кључ користећи CAST-128 са хеш кодом.
- Ово је јако компактна и ефикасна шема. Безбедна је онолико колико је безбедна лозинка. Корисник би требао да има лозинку која се тешко погађа, али лако памти.

PGP прстен јавних кључева

Timestamp	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		
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

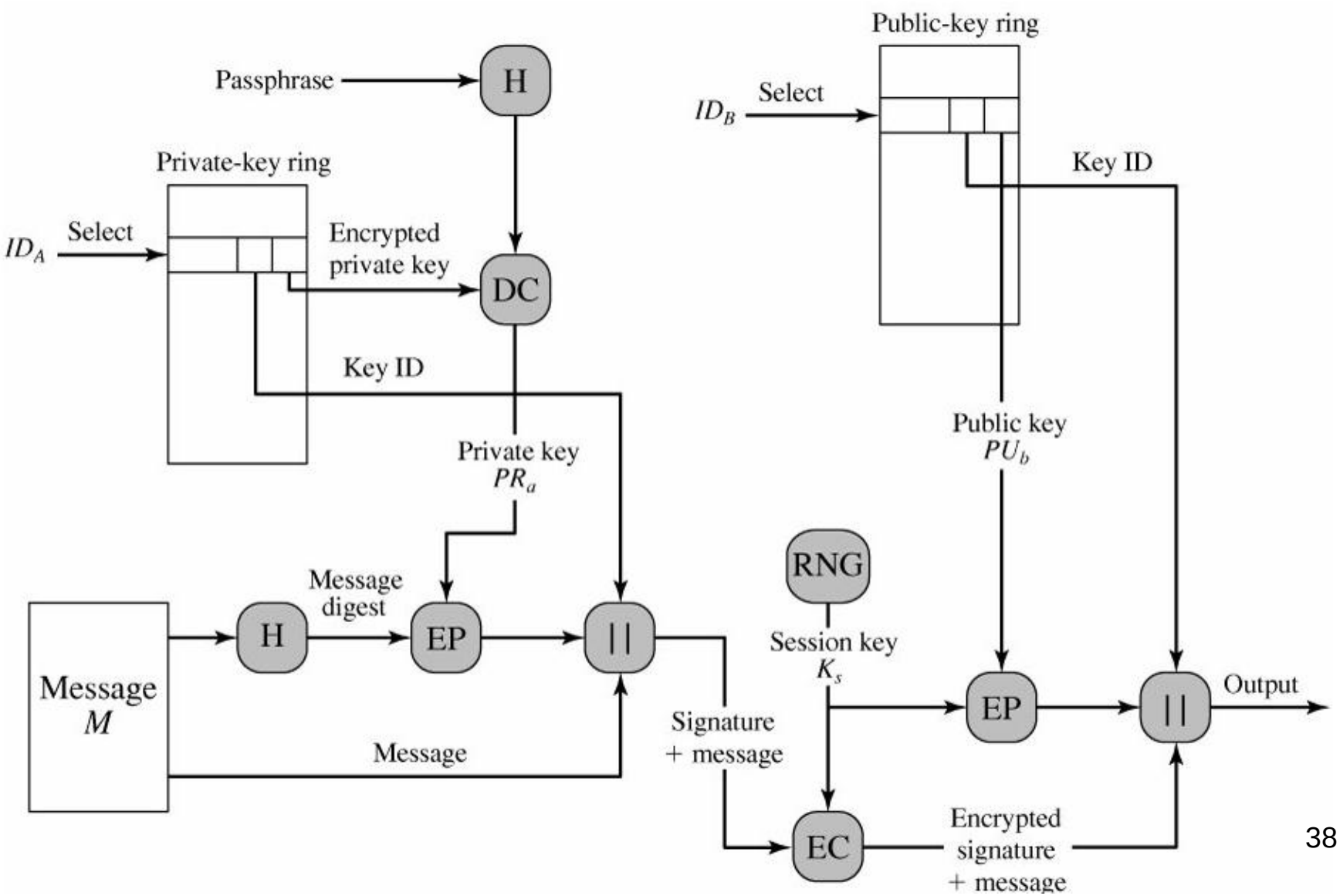
PGP прстен јавних кључева(2)

- Timestamp: датум/време када је овај улаз генерисан.
- Key ID: најмање значајних 64 бита јавног кључа за овај улаз.
- Public Key: јавни кључ за овај улаз.
- User ID: идентификује власника овог кључа.

PGP генерисање поруке (без компресије и конверзије)

- PGP ентитет који шаље поруку ради следеће:
  1. Потписивање поруке
     a. PGP дохвата приватни кључ пошиљаоца из прстена приватних кључева користећи кориснички ID као индекс. Ако кориснички ID није дат у команди, дохвата се први приватни кључ из прстена.
     b. PGP тражи од корисника лозинку да израчуна дешифровани приватни кључ.
     c. Компонента потписа поруке је конструисана.
  2. Шифровање поруке
     a. PGP генерише кључ сесије и шифрује поруку.
     b. PGP дохвата јавни кључ примаоца из прстена јавних кључева користећи кориснички ID као индекс.
     c. Компонента кључа сесије је конструисана.

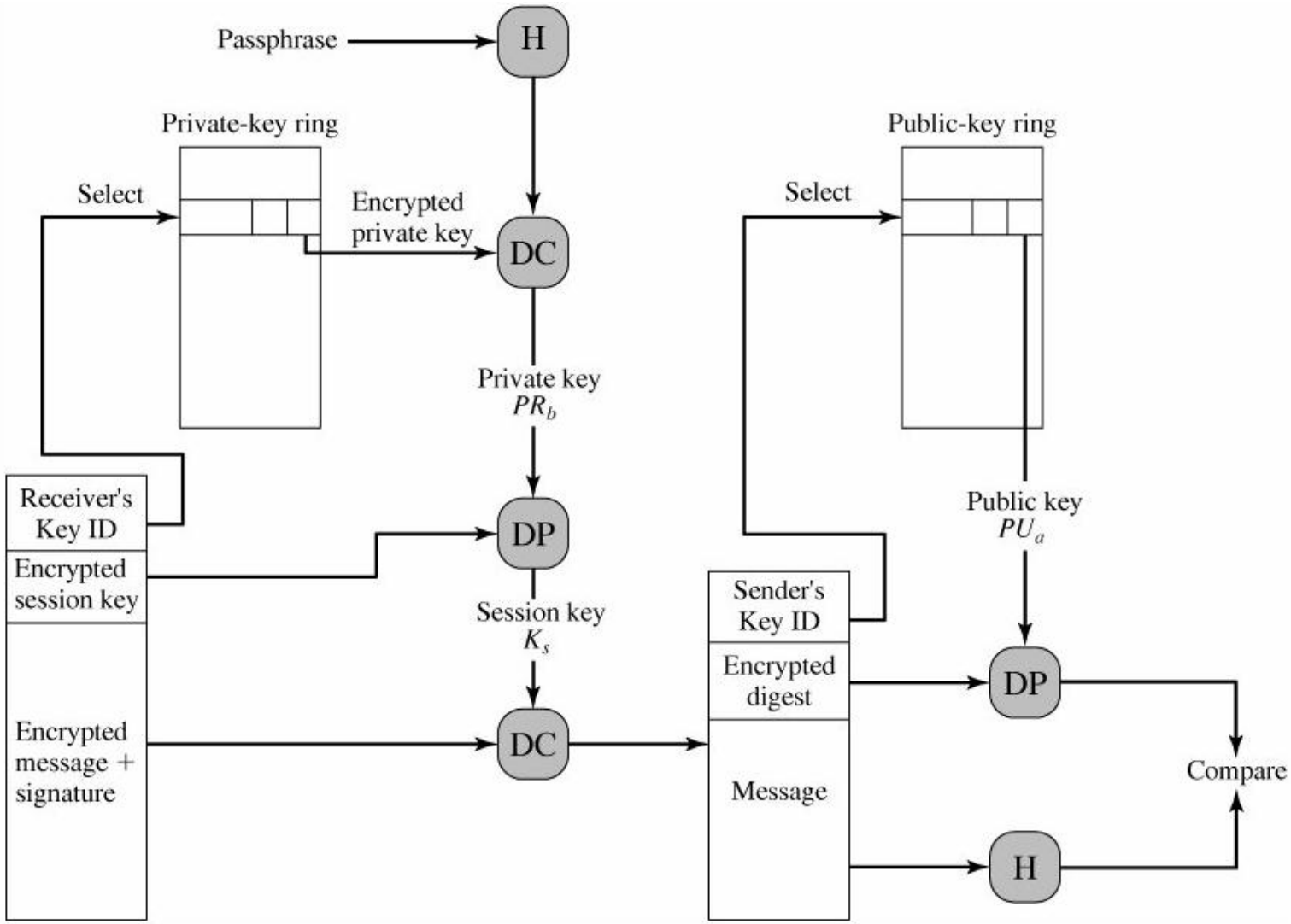
PGP генерисање поруке(2)



PGP пријем поруке (без компресије и конверзије)

- PGP ентитет који прима поруку ради следеће:
  1. Дешифровање поруке
     a. PGP дохвата приватни кључ примаоца из прстена приватних кључева, користећи ID кључа као индекс.
     b. PGP тражи од корисника лозинку да би добио дешифровани приватни кључ.
     c. PGP затим дохвата кључ сесије и дешифрује поруку.
  2. Аутентикација поруке
     a. PGP дохвата јавни кључ пошиљаоца из прстена јавних кључева, користећи ID кључа као индекс.
     b. PGP открива хеш код вредност примљене поруке.
     c. PGP израчунава хеш код за примљену поруку и упоређује га са примљеним хеш кодом ради аутентикације.

PGP prijem poruke(2)



PGP управљање кључем

- Као што смо видели, PGP пружа ефективну тајност и аутентикацију.
- Да би систем био потпун, потребно је размотрити и управљање јавним кључевима.
- PGP пружа структуру за решавање овог проблема, са неколико предложених опција које се могу користити. Пошто је PGP намењен за коришћење у различитим формалним и неформалним окружењима није дефинисана строга шема управљања кључевима.

PGP приступи управљању јавним кључевима

- Проблем: А мора да има прстен јавних кључева свих PGP-ова који размењују поруке са њим.
- man in the middle напад
- Неки приступи за сигурну размену кључева
  - Физички преузети кључ од B.
  - Верификовати кључ путем телефона
  - Дохвати B-ов јавни кључ од узајамно поверљивог D.
  - Дохвати B-ов јавни кључ од сертификујућег ауторитета од поверења
- За случајеве 3 и 4, А би морао да има копију јавног кључа треће особе и морао би да буде сигуран да је тај кључ валидан.

PGP коришћење поверења

- Основна структура је следећа.
- Сваки улаз у прстену јавних кључева је сертификат.
- Повезано са сваким таквим улазом је поље легитимитета кључа, које индикује колико PGP верује да је ово валидан јавни кључ за тог корисника.
- Што је већи ниво поверења, то је јача веза између корисничког ID-а за тај кључ.
- Сваки потпис је повезан са пољем поверења потписа које индикује колико PGP корисник верује потписивачу да сертификује јавне кључеве.
- Коначно, сваки улаз дефинише јавни кључ повезан са власником, и поље поверења власника је укључено и индикује степен до кога се овом јавном кључу верује да потписује друге јавне сертификате.
- Овај ниво поверења одређује корисник.

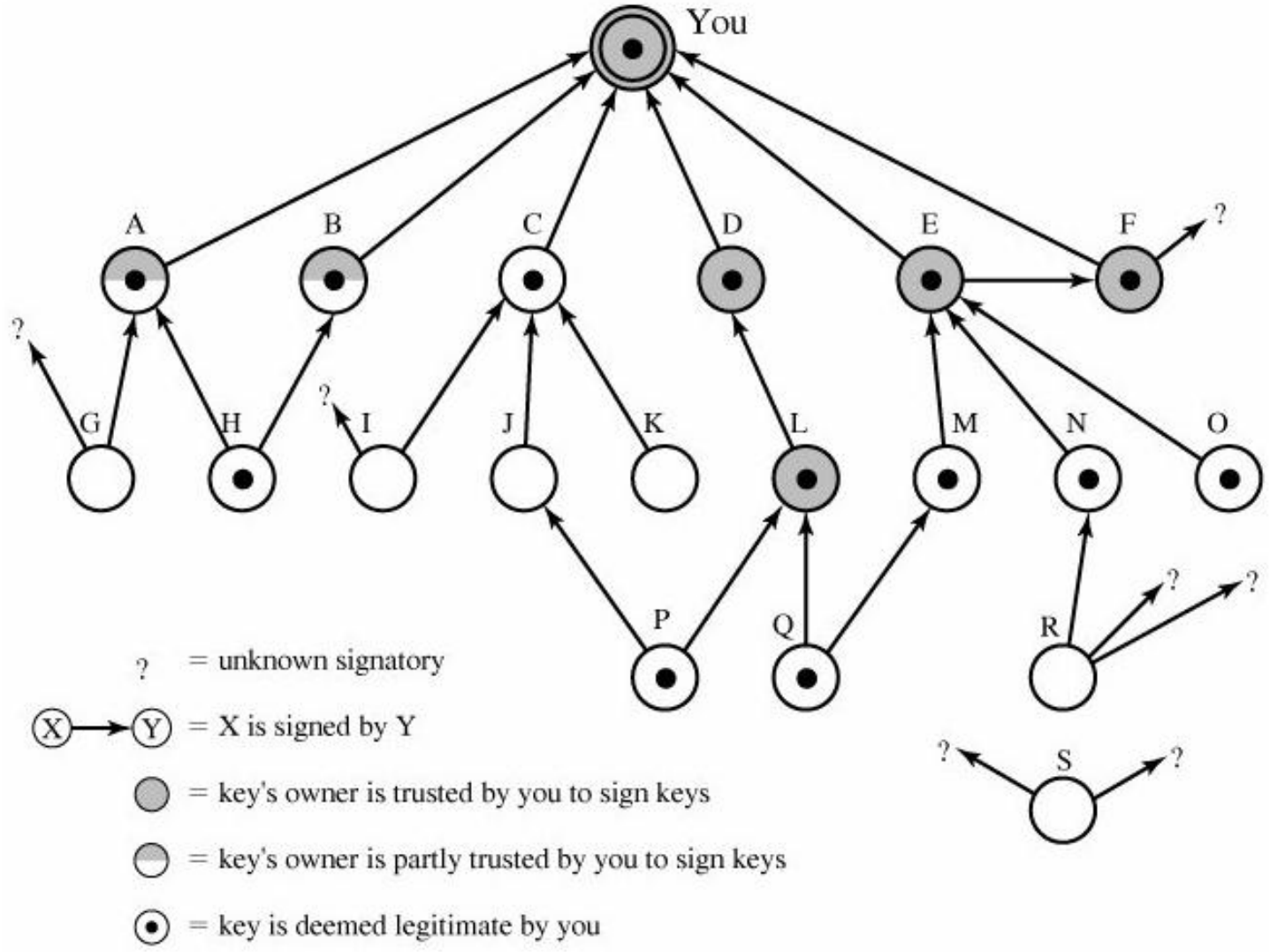
PGP коришћење поверења(2)

- Процесирање поверења:
  1. Када А убаци нови јавни кључ у прстен јавних кључева, PGP мора да додели вредност флегу поверења који је повезан са власником овог јавног кључа. Ако је власник А, тада се вредност потпуног поверења додељује овом пољу аутоматски. У супротном, PGP пита А за његову процену поверења које се треба доделити власнику овог кључа, и А мора да унесе жељени ниво. Корисник може да специфицира да је тај власник непознат, неповерљив, делимично поверљив и потпуно поверљив.
  2. Када се нови јавни кључ унесе, један или више потписа могу бити закачени за њега. Касније се може додати још потписа. Када се потпис убаци у улаз, PGP претражује прстен јавних кључева да види да ли је аутор потписа међу познатим власницима јавних кључева. Ако јесте, тада OWNERTRUST вредност за овог власника се поставља у SIGTRUST поље за тај потпис.У супротном се поставља вредност непознатог корисника.

PGP коришћење поверења(3)

3. Вредност поља легитимитета кључа се рачуна на основу поља поверења потписа присутних у овом улазу. Уколико барем један потпис има поверење потписа на вредности потпуно, тада се поље легитимитета кључа поставља на комплетно. У супротном, PGP срачунава ову вредност на основу тежинских сума. Тежина 1/X се даје потписима који су увек поверљиви, а 1/Y потписима који су углавном поверљиви, где су X и Y конфигурабилни параметри. Када уккупна тежина достигне 1, повезаност се сматра веродостојном, и вредност поља легитимитета кључа се поставља на комплетну. Тако да у одсуству потпуног поверења имамо барем X потписа којима увек верујемо или Y потписа којима углавном верујемо или нека комбинација та два.

PGP коришћење поверења(4)



PGP коришћење поверења(4)

- "You" улаз у прстену јавних кључева кореспондентан са овим корисником. Кључ - легитиман, OWNERTRUST вредност је ултимативно (потпуно) поверење.
- Сваки други чвор има OWNERTRUST недефинисано, осим ако није нешто дефинисано од стране корисника. У примеру увек верује следећим корисницима да потписују друге кључеве: D, E, F, L. Делимично верује корисницима A и B да потписују друге кључеве.
- Шта је све илустровано у примеру:
  1. Сви кључеви чији су власници потпуно или делимично од поверења су потписани од овог корисника, осим чвора L. Обично се тако ради. Чак и E који је потписан од стране потпуно поверљивог F, је потписан од стране овог корисника.
  2. Претпостављамо да су два делимично од поверења корисника довољна да сертификују кључ. Отуд је кључ H легитиман за PGP јер га потписују A и B, који су оба делимично од поверења.
  3. Кључ може бити легитиман јер га потписује потпуно поверљив корисник или два делимично поверљива корисника, али његов корисник може да не буде од поверења да потписује друге кључеве. На пример, N.
  4. Приказан је неповезан чвор S, са два непозната потписа. Такав кључ може бити добијен од сервера кључева. PGP не може да претпостави да је овај кључ легитиман само зато што је дошао са сервера. Корисник мора да потврди легитимитет кључа, тако што ће да га потпише или тако што ће рећи PGP-у да је спреман да у потпуности верује једном од потписивача кључа.

PGP повлачење јавних кључева

- Корисник може пожелети да повуче свој јавни кључ (компромитован је, жели да га замени, ...).
- Конвенција за повлачење јавног кључа је да власник изда сертификат повлачења кључа потписан од стране власника. Сертификат има исту форму као нормални сертификат потписа, али укључује индикатор који говори да је намена сертификата да се повуче јавни кључ. Власник би затим требало да покуша да рашири овај сертификат на што више места и што је брже могуће да би омогућио кореспондентима да ажурирају своје јавне кључеве.