Криптографија
- једанаести део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

17. мај 2024.

Интегритет поруке и хеш функције

- Бобан треба да буде сигуран да Алисина порука није успут промењена (случајно или намерно) - интегритет поруке

Интегритет поруке и хеш функције

- Бобан треба да буде сигуран да Алисина порука није успут промењена (случајно или намерно) - интегритет поруке
  - Како је комуникација шифрована, а Цица нема тајни кључ за криптовање: промењена порука може да буде нечитљива.

Интегритет поруке и хеш функције

- Бобан треба да буде сигуран да Алисина порука није успут промењена (случајно или намерно) - интегритет поруке
  - Како је комуникација шифрована, а Цица нема тајни кључ за криптовање: промењена порука може да буде нечитљива.
  - Већи проблем: ако је порука читљива Бобан неће приметити да је промењена

Интегритет поруке и хеш функције

- Бобан треба да буде сигуран да Алисина порука није успут промењена (случајно или намерно) - интегритет поруке
  - Како је комуникација шифрована, а Цица нема тајни кључ за криптовање: промењена порука може да буде нечитљива.
  - Већи проблем: ако је порука читљива Бобан неће приметити да је промењена
- Зато се у криптосистем обично укључује и хеш алгоритам
  - Алиса примењује хеш алгоритам на поруку пре криптовања, Бобан примењује хеш алгоритам на дешифровану поруку и упоређује добијену вредност са Алисиним резултатом

Интегритет поруке и хеш функције

- Бобан треба да буде сигуран да Алисина порука није успут промењена (случајно или намерно) - интегритет поруке
  - Како је комуникација шифрована, а Цица нема тајни кључ за криптовање: промењена порука може да буде нечитљива.
  - Већи проблем: ако је порука читљива Бобан неће приметити да је промењена
- Зато се у криптосистем обично укључује и хеш алгоритам
  - Алиса примењује хеш алгоритам на поруку пре криптовања, Бобан примењује хеш алгоритам на дешифровану поруку и упоређује добијену вредност са Алисиним резултатом
  - Цица мења шифрат али не може декриптује тај промењени шифрат. Зато не зна како треба да промени Алисину вредност хеш алгоритма

- Хеш функција h има следеће особине
  - h је једносмерна

- Хеш функција h има следеће особине
  - h је једносмерна
  - h је отпорна на колизију
    - слаба отпорност: за дато x тешко је одредити $y \neq x$ тд. $h(x) = h(y)$
    - јака отпорност: тешко је одредити различите x, y тд. $h(x) = h(y)$

- Хеш функција h има следеће особине
  - h је једносмерна
  - h је отпорна на колизију
    - слаба отпорност: за дато x тешко је одредити $y \neq x$ тд. $h(x) = h(y)$
    - јака отпорност: тешко је одредити различите x, y тд. $h(x) = h(y)$
- хеш алгоритам се састоји од више узастопних примена хеш функције

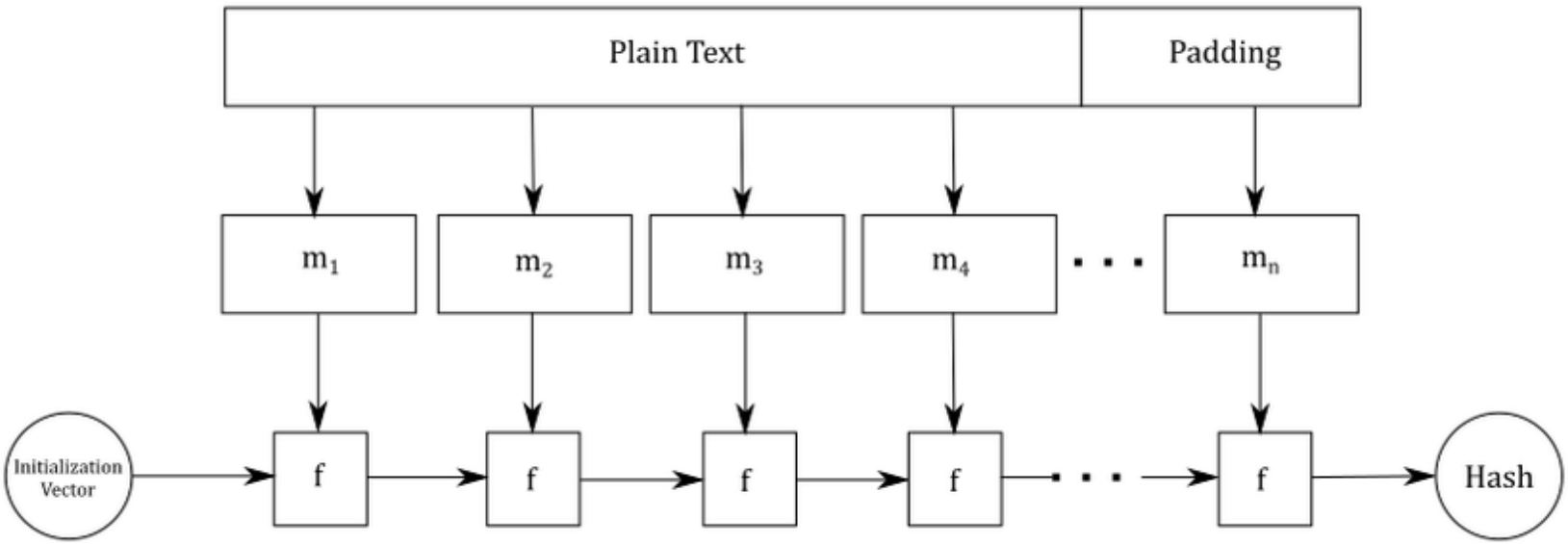
- Хеш функција h има следеће особине
  - h је једносмерна
  - h је отпорна на колизију
    - слаба отпорност: за дато x тешко је одредити $y \neq x$ тд. $h(x) = h(y)$
    - јака отпорност: тешко је одредити различите x, y тд. $h(x) = h(y)$
- хеш алгоритам се састоји од више узастопних примена хеш функције
- хеш функција $h(x, y)$ на улазу има два аргумента фиксиране дужине k и m, при чему је и излаз дужине m

- Хеш алгоритами се најчешће добијају MD конструкцијом (Меркле-Дамгор):
  - порука се дели на блокове $M_1, M_2, \ldots, M_n$ дужине m

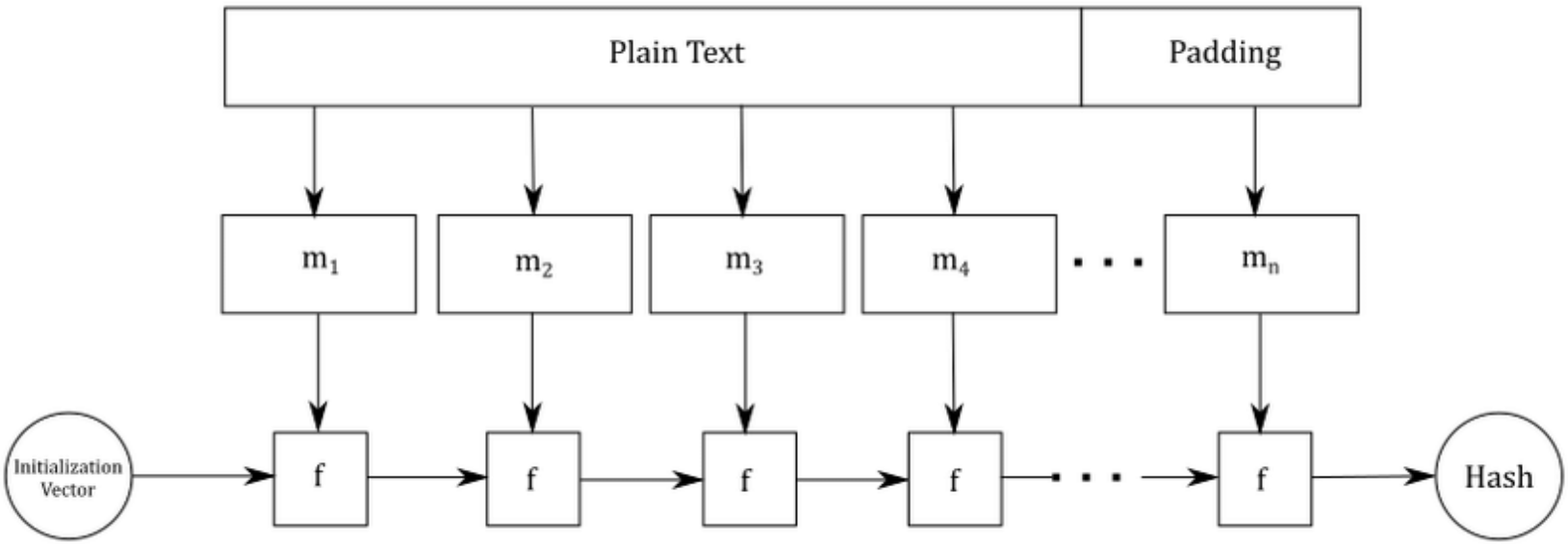
- Хеш алгоритами се најчешће добијају MD конструкцијом (Меркле-Дамгор):
  - порука се дели на блокове $M_1, M_2, \ldots, M_n$ дужине m
  - изабере се нека иницијална вредност K_0 нпр. $00\ldots0$ и рачуна се $K_1 = h\left(K_0, M_1\right)$

- Хеш алгоритами се најчешће добијају MD конструкцијом (Меркле-Дамгор):
  - порука се дели на блокове $M_1, M_2, \ldots, M_n$ дужине m
  - изабере се нека иницијална вредност K_0 нпр. $00\ldots0$ и рачуна се $K_1 = h(K_0, M_1)$
  - затим $K_2 = h(K_1, M_2)$, $K_3 = h(K_2, M_3)$, $\ldots$, $K_n = h(K_{n-1}, M_n)$ и K_n ће бити излаз хеш алгоритма

- Хеш алгоритами се најчешће добијају MD конструкцијом (Меркле-Дамгор):
  - порука се дели на блокове $M_1, M_2, \ldots, M_n$ дужине m
  - изабере се нека иницијална вредност K_0 нпр. $00\ldots0$ и рачуна се $K_1 = h(K_0, M_1)$
  - затим $K_2 = h(K_1, M_2)$, $K_3 = h(K_2, M_3)$, $\ldots$, $K_n = h(K_{n-1}, M_n)$ и K_n ће бити излаз хеш алгоритма



- Хеш алгоритами се најчешће добијају MD конструкцијом (Меркле-Дамгор):
  - порука се дели на блокове $M_1, M_2, \ldots, M_n$ дужине m
  - изабере се нека иницијална вредност K_0 нпр. $00\ldots0$ и рачуна се $K_1 = h(K_0, M_1)$
  - затим $K_2 = h(K_1, M_2)$, $K_3 = h(K_2, M_3)$, $\ldots$, $K_n = h(K_{n-1}, M_n)$ и K_n ће бити излаз хеш алгоритма



- MAC (message authentication code) је хеш алгоритам који уместо подразумеване иницијалне вредности користи тајни кључ

- Пример: Алиса и Бобан размене два кључа k_1 и k_2 Дифи-Хелмановим протоколом, затим Алиса сваки од блокова $M_1, M_2, \ldots, M_n$ шифрује AES-ом са кључем k_1 и шаље Бобану те шифрате и вредност MAC алгоритма примењеног на $M_1, M_2, \ldots, M_n$ са кључем k_2

- Пример: Алиса и Бобан размене два кључа k_1 и k_2 Дифи-Хелмановим протоколом, затим Алиса сваки од блокова $M_1, M_2, \ldots, M_n$ шифрује AES-ом са кључем k_1 и шаље Бобану те шифрате и вредност MAC алгоритма примењеног на $M_1, M_2, \ldots, M_n$ са кључем k_2
- За хеш функцију се може користити $h(x, y) = AES_x(y)$

- Пример: Алиса и Бобан размене два кључа k_1 и k_2 Дифи-Хелмановим протоколом, затим Алиса сваки од блокова $M_1, M_2, \ldots, M_n$ шифрује AES-ом са кључем k_1 и шаље Бобану те шифрате и вредност MAC алгоритма примењеног на $M_1, M_2, \ldots, M_n$ са кључем k_2
- За хеш функцију се може користити $h(x, y) = AES_x(y)$
- Видети: Живковић, Глава 19.1: MD5 алгоритам

- Пример: Алиса и Бобан размене два кључа k_1 и k_2 Дифи-Хелмановим протоколом, затим Алиса сваки од блокова $M_1, M_2, \ldots, M_n$ шифрује AES-ом са кључем k_1 и шаље Бобану те шифрате и вредност MAC алгоритма примењеног на $M_1, M_2, \ldots, M_n$ са кључем k_2
- За хеш функцију се може користити $h(x, y) = AES_x(y)$
- Видети: Живковић, Глава 19.1: MD5 алгоритам
- Генерално, сви хеш алгоритми користе понављање и комбиновање пуно једноставних корака (као AES)

- Пример: Алиса и Бобан размене два кључа k_1 и k_2 Дифи-Хелмановим протоколом, затим Алиса сваки од блокова $M_1, M_2, \ldots, M_n$ шифрује AES-ом са кључем k_1 и шаље Бобану те шифрате и вредност MAC алгоритма примењеног на $M_1, M_2, \ldots, M_n$ са кључем k_2
- За хеш функцију се може користити $h(x, y) = AES_x(y)$
- Видети: Живковић, Глава 19.1: MD5 алгоритам
- Генерално, сви хеш алгоритми користе понављање и комбиновање пуно једноставних корака (као AES)
- Улаз хеш алгоритма је порука променљиве дужине, излаз има фиксирану дужину која је обично много мања од улаза

Аутентикација

- Бобан мора да буде сигуран да порука коју је добио долази од Алисе (нпр. порука може да буде склапање уговора)

Аутентикација

- Бобан мора да буде сигуран да порука коју је добио долази од Алисе (нпр. порука може да буде склапање уговора)
- Аутентикација = процес којим се доказује да порука долази од правог пошиљаоца,

Аутентикација

- Бобан мора да буде сигуран да порука коју је добио долази од Алисе (нпр. порука може да буде склапање уговора)
- Аутентикација = процес којим се доказује да порука долази од правог пошиљаоца, обухвата:
  - дигитални потпис - повезује поруку са јавним кључем

Аутентикација

- Бобан мора да буде сигуран да порука коју је добио долази од Алисе (нпр. порука може да буде склапање уговора)
- Аутентикација = процес којим се доказује да порука долази од правог пошиљаоца, обухвата:
  - дигитални потпис - повезује поруку са јавним кључем
  - сертификат - повезује јавни кључ са конкретном особом, то је документ (издат од овлашћеног лица) у коме пише ,,Алиса користи кључ 12345“

Аутентикација

- Бобан мора да буде сигуран да порука коју је добио долази од Алисе (нпр. порука може да буде склапање уговора)
- Аутентикација = процес којим се доказује да порука долази од правог пошиљаоца, обухвата:
  - дигитални потпис - повезује поруку са јавним кључем
  - сертификат - повезује јавни кључ са конкретном особом, то је документ (издат од овлашћеног лица) у коме пише „Алиса користи кључ 12345“
- Имали смо пример дигиталног потписа (код RSA):
  - f_A = Алисина функција криптовања
  - x = вредност коју она треба да потпише (x је изабрао Бобан или је добијено на основу поруке)
  - Алиса рачуна и објављује $f_A^{-1}(x)$. Свако може да провери Алисин потпис јер је f_A јавно, али нико не може да направи њен потпис јер је f_A^{-1} тајно

- Проблем: Обично се кључ и дигитални потпис размењују асиметричним криптосистемом, а порука симетричним

- Проблем: Обично се кључ и дигитални потпис размењују асиметричним криптосистемом, а порука симетричним
- Ако потпис не зависи од поруке: Цица може да одвоји Алисин потпис и да га подметне на неку другу поруку

- Проблем: Обично се кључ и дигитални потпис размењују асиметричним криптосистемом, а порука симетричним
- Ако потпис не зависи од поруке: Цица може да одвоји Алисин потпис и да га подметне на неку другу поруку
- Нпр. Цица се Бобану представи као Алиса, Бобан шаље Цици x и пита је колико је $f_A^{-1}(x)$. Цица може да започне комуникацију са Алисом и постави јој исто питање са истим x. Цица само проследи Бобану Алисин одговор

- Проблем: Обично се кључ и дигитални потпис размењују асиметричним криптосистемом, а порука симетричним
- Ако потпис не зависи од поруке: Цица може да одвоји Алисин потпис и да га подметне на неку другу поруку
- Нпр. Цица се Бобану представи као Алиса, Бобан шаље Цици x и пита је колико је $f_A^{-1}(x)$. Цица може да започне комуникацију са Алисом и постави јој исто питање са истим x. Цица само проследи Бобану Алисин одговор
- Зато потпис треба везати за поруку M.

- Проблем: Обично се кључ и дигитални потпис размењују асиметричним криптосистемом, а порука симетричним
- Ако потпис не зависи од поруке: Цица може да одвоји Алисин потпис и да га подметне на неку другу поруку
- Нпр. Цица се Бобану представи као Алиса, Бобан шаље Цици x и пита је колико је $f_A^{-1}(x)$. Цица може да започне комуникацију са Алисом и постави јој исто питање са истим x. Цица само проследи Бобану Алисин одговор
- Зато потпис треба везати за поруку M.
  - Избор $x = M$ је добро, али споро решење (порука би се слала асиметричним криптосистемом)

- Проблем: Обично се кључ и дигитални потпис размењују асиметричним криптосистемом, а порука симетричним
- Ако потпис не зависи од поруке: Цица може да одвоји Алисин потпис и да га подметне на неку другу поруку
- Нпр. Цица се Бобану представи као Алиса, Бобан шаље Цици x и пита је колико је $f_A^{-1}(x)$. Цица може да започне комуникацију са Алисом и постави јој исто питање са истим x. Цица само проследи Бобану Алисин одговор
- Зато потпис треба везати за поруку M.
  - Избор $x = M$ је добро, али споро решење (порука би се слала асиметричним криптосистемом)
  - Зато се користи $x = H(M)$, где је H хеш алгоритам

Све заједно:

Бобан може да направи кључ K за AES , Алиси пошаље

1. шифрат $X = K^{e_A} \mod n_A$,
2. Шифрат $C = AES_K(M)$ поруке M, и
3. потпис $H^{d_B} \mod n_B$, где је $H = hash(M)$.

Алиса дешифрује својим тајним кључем X и тако добија кључ K за AES . Затим кључем K дешифрује C, добија поруку M, па израчунава хеш вредност $H = hash(M)$. На крају проверава потпис S, тако што га шифрује Бобановим јавним кључем и провери да ли се резултат слаже са H. У случају да се слаже, закључује да је поруку потписао Бобан, пошто само он зна свој тајни кључ.

Решење 2. Исто као у претходној варијанти, сем што се уместо S шаље $AES_K(S)$. Тиме се спречава да Цица издвоји из поруке $H = hash(M)$, после чега може да исту поруку са новим потписом пошаље са потписом Дејана.

ЕлГамалов потпис

- Не може аналогно претходном

ЕлГамалов потпис

- Не може аналогно претходном
- Јавно: прост p и g генератор $\mathbb{Z}_p^*$

ЕлГамалов потпис

- Не може аналогно претходном
- Јавно: прост p и g генератор $\mathbb{Z}_p^*$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност H поруке ($H < p$)

ЕлГамалов потпис

- Не може аналогно претходном
- Јавно: прост p и g генератор $\mathbb{Z}_p^*$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност H поруке ($H < p$)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $r = g^k$

ЕлГамалов потпис

- Не може аналогно претходном
- Јавно: прост p и g генератор $\mathbb{Z}_p^*$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност H поруке ($H < p$)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $r = g^k$
  - Израчуна $x = k^{-1}\left(H + a_A r\right) \mod p - 1$

ЕлГамалов потпис

- Не може аналогно претходном
- Јавно: прост p и g генератор $\mathbb{Z}_p^*$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност H поруке ($H < p$)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $r = g^k$
  - Израчуна $x = k^{-1}\left(H + a_A r\right) \mod p-1$
  - Алисин потпис је (H, r, x)

ЕлГамалов потпис

- Не може аналогно претходном
- Јавно: прост p и g генератор $\mathbb{Z}_p^*$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност H поруке ($H < p$)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $r = g^k$
  - Израчуна $x = k^{-1}\left(H + a_A r\right) \mod p-1$
  - Алисин потпис је (H, r, x)
- Бобан проверава потпис
  - Након декриптовања хешира поруку и упореди вредност са H

ЕлГамалов потпис

- Не може аналогно претходном
- Јавно: прост p и g генератор $\mathbb{Z}_p^*$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност H поруке ($H < p$)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $r = g^k$
  - Израчуна $x = k^{-1}\left(H + a_A r\right) \mod p-1$
  - Алисин потпис је (H, r, x)
- Бобан проверава потпис
  - Након декриптовања хешира поруку и упореди вредност са H
  - Рачуна $r^x \mod p$ и $g^H \left(g^{a_A}\right)^r \mod p$ и упоређује их
    - Објашњење $r^x = g^{kx} = g^{H + a_A r}$

ЕлГамалов потпис

- Не може аналогно претходном
- Јавно: прост p и g генератор $\mathbb{Z}_p^*$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност H поруке ($H < p$)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $r = g^k$
  - Израчуна $x = k^{-1}\left(H + a_A r\right) \mod p-1$
  - Алисин потпис је (H, r, x)
- Бобан проверава потпис
  - Након декриптовања хешира поруку и упореди вредност са H
  - Рачуна $r^x \mod p$ и $g^H \left(g^{a_A}\right)^r \mod p$ и упоређује их
    - Објашњење $r^x = g^{kx} = g^{H + a_A r}$
- Постоји и верзија у којој се H изоставља из потписа

Пример 20.1. *Нека је хеш вредност поруке* $H = 316$. *Алиса користи* $= 677$, $g = 2$ *и приватни кључ* $a_A = 307$. *Према томе, њен јавни кључ је* $g^{a_A} = 2^{307} \mod 677 = 498$. *Она или шаље Бобану* p, g, $g^a \mod p$, *тј.* 677, 2, 498, *или он то проналази на њеном сајту.*

Она бира кључ поруке $k = 401$ *(што је у реду, јер је* $\mathrm{nzd}(k, p-1) = 1$*). Алиса израчунава* $r = g^k = 2^{401} \equiv 616 \pmod p$, *па је* $r = 616$. *Она решава конгруенцију* $kx = H + a_A r \pmod{p-1}$, *односно* $401x \equiv 316 + 307 \cdot 616 \pmod{676}$. *Дакле,* $x \equiv 401^{-1}(316 + 307 \cdot 616)$. *Пошто је* $401^{-1} \equiv 617 \pmod{676}$, *добија се да је* $x \equiv 617(316 + 307 \cdot 616) \equiv 56 \pmod{676}$. *Алиса шаље* $(r, x, H) = (616, 56, 316)$ *као потпис хеш вредности и шаље* $(616, 56, 316)$. *Бобан прима ту тројку и израчунава*

- $r^x = 616^{56} \equiv 293 \pmod{677}$
- $g^H = 2^{316} \equiv 424 \pmod{677}$.
- $(g^{a_A})^r = 498^{616} \equiv 625 \pmod{677}$.
- $g^H (g^{a_A})^r = 424 \cdot 625 \equiv 293 \pmod{677}$.

Потпис је тиме верификован, јер је $r^x \equiv g^H (g^{a_A})^r \pmod p$.

ЕлГамалов потпис над елиптичким кривама

ЕлГамалов потпис над елиптичким кривама

- Јавно: тачка G са елиптичке криве $E(\mathbb{Z}_p)$

ЕлГамалов потпис над елиптичким кривама

- Јавно: тачка G са елиптичке криве $E(\mathbb{Z}_p)$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност поруке $H < p - 1$ (цео број)

ЕлГамалов потпис над елиптичким кривама

- Јавно: тачка G са елиптичке криве $E(\mathbb{Z}_p)$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност поруке $H < p - 1$ (цео број)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $R = kG = (r_1, r_2)$

ЕлГамалов потпис над елиптичким кривама

- Јавно: тачка G са елиптичке криве $E(\mathbb{Z}_p)$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност поруке $H < p-1$ (цео број)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $R = kG = (r_1, r_2)$
  - Израчуна цео број $x = k^{-1}(H + a_A r_1) \mod p-1$

ЕлГамалов потпис над елиптичким кривама

- Јавно: тачка G са елиптичке криве $E(\mathbb{Z}_p)$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност поруке $H < p-1$ (цео број)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $R = kG = (r_1, r_2)$
  - Израчуна цео број $x = k^{-1}(H + a_A r_1) \mod p-1$
  - Алисин потпис је (H, r_1, x)

ЕлГамалов потпис над елиптичким кривама

- Јавно: тачка G са елиптичке криве $E(\mathbb{Z}_p)$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност поруке $H < p-1$ (цео број)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $R = kG = (r_1, r_2)$
  - Израчуна цео број $x = k^{-1}(H + a_A r_1) \mod p-1$
  - Алисин потпис је (H, r_1, x)
- Бобан проверава потпис
  - Након декриптовања хешира поруку и упореди вредност са H

ЕлГамалов потпис над елиптичким кривама

- Јавно: тачка G са елиптичке криве $E(\mathbb{Z}_p)$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност поруке $H < p-1$ (цео број)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $R = kG = (r_1, r_2)$
  - Израчуна цео број $x = k^{-1}(H + a_A r_1) \mod p-1$
  - Алисин потпис је (H, r_1, x)
- Бобан проверава потпис
  - Након декриптовања хешира поруку и упореди вредност са H
  - Одреди тачку $R = (r_1, \dots) \in E(\mathbb{Z}_p)$

ЕлГамалов потпис над елиптичким кривама

- Јавно: тачка G са елиптичке криве $E(\mathbb{Z}_p)$
- Алиса потписује поруку (помоћу њеног тајног кључа a_A):
  - Израчуна хеш вредност поруке $H < p-1$ (цео број)
  - Бира случајно k тд. НЗД$(k, p-1) = 1$ и рачуна $R = kG = (r_1, r_2)$
  - Израчуна цео број $x = k^{-1}(H + a_A r_1) \mod p-1$
  - Алисин потпис је (H, r_1, x)
- Бобан проверава потпис
  - Након декриптовања хешира поруку и упореди вредност са H
  - Одреди тачку $R = (r_1, \dots) \in E(\mathbb{Z}_p)$
  - Рачуна тачке xR и $HG \oplus r_1(a_A G)$ и упоређује их

Шноров потпис

- p и q прости бројеви тд. $q \ll p$ и $q|p-1$. Стандардно: $p \approx 2^{512}$ и $q \approx 2^{140}$
- број a тд. $a^q \equiv 1 \pmod{p}$. Свима познато p, q, a

Шноров потпис

- p и q прости бројеви тд. $q \ll p$ и $q|p-1$. Стандардно: $p \approx 2^{512}$ и $q \approx 2^{140}$
- број a тд. $a^q \equiv 1 \pmod{p}$. Свима познато p, q, a
- Сваки учесник n има тајни кључ s_n и јавни кључ $v_n = a^{-s_n} \bmod p$

Шноров потпис

- p и q прости бројеви тд. $q \ll p$ и $q|p-1$. Стандардно: $p \approx 2^{512}$ и $q \approx 2^{140}$
- број a тд. $a^q \equiv 1 \pmod{p}$. Свима познато p, q, a
- Сваки учесник n има тајни кључ s_n и јавни кључ $v_n = a^{-s_n} \bmod p$
- Алиса потписује поруку M тако што
  - бира случајно $r < q$ и рачуна $x = a^r \bmod p$

Шноров потпис

- p и q прости бројеви тд. $q \ll p$ и $q|p-1$. Стандардно: $p \approx 2^{512}$ и $q \approx 2^{140}$
- број a тд. $a^q \equiv 1 \pmod{p}$. Свима познато p, q, a
- Сваки учесник n има тајни кључ s_n и јавни кључ $v_n = a^{-s_n} \bmod p$
- Алиса потписује поруку M тако што
  - бира случајно $r < q$ и рачуна $x = a^r \bmod p$
  - надовезује M и x, хешира ту вредност и добија e

Шноров потпис

- p и q прости бројеви тд. $q \ll p$ и $q|p-1$. Стандардно: $p \approx 2^{512}$ и $q \approx 2^{140}$
- број a тд. $a^q \equiv 1 \pmod{p}$. Свима познато p, q, a
- Сваки учесник n има тајни кључ s_n и јавни кључ $v_n = a^{-s_n} \bmod p$
- Алиса потписује поруку M тако што
  - бира случајно $r < q$ и рачуна $x = a^r \bmod p$
  - надовезује M и x, хешира ту вредност и добија e
  - рачуна $y = r + s_A e \bmod q$
  - Алисин потпис је (x, e, y)

Шноров потпис

- p и q прости бројеви тд. $q \ll p$ и $q|p-1$. Стандардно: $p \approx 2^{512}$ и $q \approx 2^{140}$
- број a тд. $a^q \equiv 1 \pmod{p}$. Свима познато p, q, a
- Сваки учесник n има тајни кључ s_n и јавни кључ $v_n = a^{-s_n} \bmod p$
- Алиса потписује поруку M тако што
  - бира случајно $r < q$ и рачуна $x = a^r \bmod p$
  - надовезује M и x, хешира ту вредност и добија e
  - рачуна $y = r + s_A e \bmod q$
  - Алисин потпис је (x, e, y)
- Бобан проверава њен потпис тако што

Шноров потпис

- p и q прости бројеви тд. $q \ll p$ и $q|p-1$. Стандардно: $p \approx 2^{512}$ и $q \approx 2^{140}$
- број a тд. $a^q \equiv 1 \pmod{p}$. Свима познато p, q, a
- Сваки учесник n има тајни кључ s_n и јавни кључ $v_n = a^{-s_n} \bmod p$
- Алиса потписује поруку M тако што
  - бира случајно $r < q$ и рачуна $x = a^r \bmod p$
  - надовезује M и x, хешира ту вредност и добија e
  - рачуна $y = r + s_A e \bmod q$
  - Алисин потпис је (x, e, y)
- Бобан проверава њен потпис тако што
  - рачуна $a^y v_A^e \bmod p$ и упоређује са x

Шноров потпис

- p и q прости бројеви тд. $q \ll p$ и $q|p-1$. Стандардно: $p \approx 2^{512}$ и $q \approx 2^{140}$
- број a тд. $a^q \equiv 1 \pmod{p}$. Свима познато p, q, a
- Сваки учесник n има тајни кључ s_n и јавни кључ $v_n = a^{-s_n} \bmod p$
- Алиса потписује поруку M тако што
  - бира случајно $r < q$ и рачуна $x = a^r \bmod p$
  - надовезује M и x, хешира ту вредност и добија e
  - рачуна $y = r + s_A e \bmod q$
  - Алисин потпис је (x, e, y)
- Бобан проверава њен потпис тако што
  - рачуна $a^y v_A^e \bmod p$ и упоређује са x
  - декриптује M, хешира Mx (надовезивање) и упоређује са e

Шноров потпис

- p и q прости бројеви тд. $q \ll p$ и $q|p-1$. Стандардно: $p \approx 2^{512}$ и $q \approx 2^{140}$
- број a тд. $a^q \equiv 1 \pmod{p}$. Свима познато p, q, a
- Сваки учесник n има тајни кључ s_n и јавни кључ $v_n = a^{-s_n} \bmod p$
- Алиса потписује поруку M тако што
  - бира случајно $r < q$ и рачуна $x = a^r \bmod p$
  - надовезује M и x, хешира ту вредност и добија e
  - рачуна $y = r + s_A e \bmod q$
  - Алисин потпис је (x, e, y)
- Бобан проверава њен потпис тако што
  - рачуна $a^y v_A^e \bmod p$ и упоређује са x
  - декриптује M, хешира Mx (надовезивање) и упоређује са e
- Шноров поступак даје исту сигурност као RSA потпис (проблем дискретног логаритма у $\mathbb{Z}_p$)

Шноров потпис

- p и q прости бројеви тд. $q \ll p$ и $q|p-1$. Стандардно: $p \approx 2^{512}$ и $q \approx 2^{140}$
- број a тд. $a^q \equiv 1 \pmod{p}$. Свима познато p, q, a
- Сваки учесник n има тајни кључ s_n и јавни кључ $v_n = a^{-s_n} \bmod p$
- Алиса потписује поруку M тако што
  - бира случајно $r < q$ и рачуна $x = a^r \bmod p$
  - надовезује M и x, хешира ту вредност и добија e
  - рачуна $y = r + s_A e \bmod q$
  - Алисин потпис је (x, e, y)
- Бобан проверава њен потпис тако што
  - рачуна $a^y v_A^e \bmod p$ и упоређује са x
  - декриптује M, хешира Mx (надовезивање) и упоређује са e
- Шноров поступак даје исту сигурност као RSA потпис (проблем дискретног логаритма у $\mathbb{Z}_p$)
- бржи је од RSA потписа: Алиса може унапред да припреми x, а код провере Бобан рачуна степен $< q$

Сертификати

- Повезују јавни кључ са конкретном особом, то је документ (издат од овлашћеног лица) у коме пише ,,Алиса користи кључ 12345“

Сертификати

- Повезују јавни кључ са конкретном особом, то је документ (издат од овлашћеног лица) у коме пише ,,Алиса користи кључ 12345“
- Постоје разни нивои сертификата:
  - највиши ниво - повезује кључ са неким идентификационим докуметом, оверава се код нотара
  - слабије - нпр. повезује кључ са електронском поштом

Сертификати

- Повезују јавни кључ са конкретном особом, то је документ (издат од овлашћеног лица) у коме пише ,,Алиса користи кључ 12345“
- Постоје разни нивои сертификата:
  - највиши ниво - повезује кључ са неким идентификационим докуметом, оверава се код нотара
  - слабије - нпр. повезује кључ са електронском поштом
- Најпознатији сертификациони центар је фирма Верисајн (Verisign), али постоје и други (неке државе не признају Верисајн)

Сертификати

- Повезују јавни кључ са конкретном особом, то је документ (издат од овлашћеног лица) у коме пише ,,Алиса користи кључ 12345“
- Постоје разни нивои сертификата:
  - највиши ниво - повезује кључ са неким идентификационим докуметом, оверава се код нотара
  - слабије - нпр. повезује кључ са електронском поштом
- Најпознатији сертификациони центар је фирма Верисајн (Verisign), али постоје и други (неке државе не признају Верисајн)
- Сертификат може да се опозове нпр. због губитка тајности кључа

Пример сертификата:

Верзија: V3
Серијски број: низ хексадекадих цифара
Издавач: Verisign
Важи од: 7. априла 2013.
Важи до: 6. априла 2014.
Субјекат: bankofamerica.com
Алгоритам потписа: MD5/RSA
Јавни кључ: n_{BA}, e_{BA} (низ хексадекадних цифара)
Хеш: MD5 хеш вредност претходног дела овог сертификата.
Потпис: $hash^{d_V} \mod n_V$.

Потписао Верисајн

Пример сертификата:

Верзија: V3
Серијски број: низ хексадекадих цифара
Издавач: Verisign
Важи од: 7. априла 2013.
Важи до: 6. априла 2014.
Субјекат: bankofamerica.com
Алгоритам потписа: MD5/RSA
Јавни кључ: n_{BA}, e_{BA} (низ хексадекадних цифара)
Хеш: MD5 хеш вредност претходног дела овог сертификата.
Потпис: $hash^{d_V} \mod n_V$.

Потписао Верисајн

- Пре почетка комуникације Алиса и Бобан размењују сертификате и свако провера сертификат оног другог (проверава хеш вредност и Верисајнов потпис)

Пример:

- Корисник картице америчке банке покушава да подигне новац на банкомату у Србији

Пример:

- Корисник картице америчке банке покушава да подигне новац на банкомату у Србији
- Српска банка треба да искомуницира са америчком, комуникација се шифрује AES-ом

Пример:

- Корисник картице америчке банке покушава да подигне новац на банкомату у Србији
- Српска банка треба да искомуницира са америчком, комуникација се шифрује AES-ом
- Српска банка проверава сертификат америчке

Пример:

- Корисник картице америчке банке покушава да подигне новац на банкомату у Србији
- Српска банка треба да искомуницира са америчком, комуникација се шифрује AES-ом
- Српска банка проверава сертификат америчке
- Српска банка користи RSA са кључем из сертификата америчке да пошаље кључ за AES и њен потпис

Пример:

- Корисник картице америчке банке покушава да подигне новац на банкомату у Србији
- Српска банка треба да искомуницира са америчком, комуникација се шифрује AES-ом
- Српска банка проверава сертификат америчке
- Српска банка користи RSA са кључем из сертификата америчке да пошаље кључ за AES и њен потпис
- Банкомат може да исплати готовину након што банке договоре трансакцију

Сертификационо стабло

Пример:

- Банка има Верисајнов сертификат

Сертификационо стабло

Пример:

- Банка има Верисајнов сертификат
- Свака филијала банке треба да има свој сертификат
  - Непрактично је да Верисајн верификује сертификат сваке филијале
  - Банка има свој сертификациони центар (нижег нивоа) који издаје сертификате филијалама

Сертификационо стабло

Пример:

- Банка има Верисајнов сертификат
- Свака филијала банке треба да има свој сертификат
  - Непрактично је да Верисајн верификује сертификат сваке филијале
  - Банка има свој сертификациони центар (нижег нивоа) који издаје сертификате филијалама
- Слично, свака филијала може да издаје сертификате запосленима

Сертификационо стабло

Пример:

- Банка има Верисајнов сертификат
- Свака филијала банке треба да има свој сертификат
  - Непрактично је да Верисајн верификује сертификат сваке филијале
  - Банка има свој сертификациони центар (нижег нивоа) који издаје сертификате филијалама
- Слично, свака филијала може да издаје сертификате запосленима
- Корисник проверава сертификат и службеника банке и филијале и банке - сертификациони пут

Сертификационо стабло

Пример:

- Банка има Верисајнов сертификат
- Свака филијала банке треба да има свој сертификат
  - Непрактично је да Верисајн верификује сертификат сваке филијале
  - Банка има свој сертификациони центар (нижег нивоа) који издаје сертификате филијалама
- Слично, свака филијала може да издаје сертификате запосленима
- Корисник проверава сертификат и службеника банке и филијале и банке - сертификациони пут
- Тако се долазе до сертификационог стабла, на врху је Верисајн

Сертификационо стабло

Пример:

- Банка има Верисајнов сертификат
- Свака филијала банке треба да има свој сертификат
  - Непрактично је да Верисајн верификује сертификат сваке филијале
  - Банка има свој сертификациони центар (нижег нивоа) који издаје сертификате филијалама
- Слично, свака филијала може да издаје сертификате запосленима
- Корисник проверава сертификат и службеника банке и филијале и банке - сертификациони пут
- Тако се долазе до сертификационог стабла, на врху је Верисајн
- Сертификациона стабла се користе за пословну примену

Мрежа поверења

- мења сертификационо стабло (углавном код приватних корисника)

Мрежа поверења

- мења сертификационо стабло (углавном код приватних корисника)
- Сваки корисник сам одлучује коме верује
  - Корисник X прави сертификат $S_X(K_Y)$ у ком потписује (потврђује) јавни кључ K_Y корисника Y

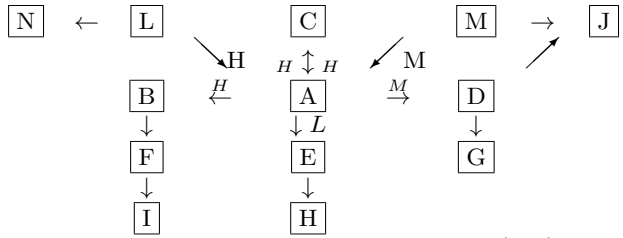
Мрежа поверења

- мења сертификационо стабло (углавном код приватних корисника)
- Сваки корисник сам одлучује коме верује
  - Корисник X прави сертификат $S_X(K_Y)$ у ком потписује (потврђује) јавни кључ K_Y корисника Y
- Корисник (Алиса) прави прстен јавних кључева, он садржи:
  - кориснике (тј. њихове кључеве) којима Алиса верује
  - кориснике у чији потпис Алиса верује
  - кориснке који верују Алиси

Мрежа поверења

- мења сертификационо стабло (углавном код приватних корисника)
- Сваки корисник сам одлучује коме верује
  - Корисник X прави сертификат $S_X(K_Y)$ у ком потписује (потврђује) јавни кључ K_Y корисника Y
- Корисник (Алиса) прави прстен јавних кључева, он садржи:
  - кориснике (тј. њихове кључеве) којима Алиса верује
  - кориснике у чији потпис Алиса верује
  - кориснке који верују Алиси
- Мрежа поверења је саставни део програма PGP за шифровање електронске поште (Pretty good privacy)

име	потписани кључ	ниво поверења у кључ	мера поверења у његове потписе кључева	мера поверења потписивача у серификате других кључева
Бобан	$S_A(K_B)$	Висок	Висок	
Цица	$S_A(K_C)$	Висок	Висок	
Деа	$S_A(K_D)$	Висок	Средњи	
Ед	$S_A(K_E)$	Висок	Низак	
Цица	$S_C(K_A)$			Висок
Лаза	$S_L(K_A)$			Висок
Марко	$S_M(K_A)$			Средњи



У овом дијаграму $X \to Y$ значи да је $S_X(K_Y)$ у прстеновима и X и Y. Даље, $X \overset{H}{\to} Y$ значи да је у оба прстена, а X има потпуно поверење у сертификате других јавних кључева који потичу од Y.

Претпоставимо да Алиса жели да пошаље поруку F. A контактира са F, и F шаље свој прстен A. Прстен учесника F садржи $S_B(K_F)$. Пошто A верује серификатима других кључева који потичу од B, сада A има поверење у јавни кључ учесника F.

Алиса жели да пошаље поруку G. Прстен учесника G садржи $S_D(K_G)$. Међутим, Алиса има осредње поверење у D-ове сертификате других кључева. Због тога Алиса нема поверења у G-ов јавни кључ. Слично, A нема поверење у H-ов јавни кључ.

Алиса жели да пошаље поруку J. Прстен учесника J садржи $S_D K_J$ и $S_M K_J$. Алиса има осредње поверење у D-ове и M-ове сертификате других кључева, а две осредње оцене имају за последицу да Алиса нема поверења у J-ов јавни кључ.

Алиса жели да пошаље поруку I. Прстен учесника I садржи $S_F K_I$. Алиса има поверења у јавни кључ особе F, али нема основа да верује F-овом сертификату I, па A нема поверења у јавни кључ I.

Алиса жели да пошаље поруку N. Прстен учесника N садржи $S_L K_N$. Алиса има поверења у L-ове сертификате, па има поверење у јавни кључ особе N.

Ако Алиса шаље поруку F, PGP ће то дозволити. Ако Алиса шаље поруку I, PGP ће избацити поруку да она нема основа за поверење у јавни кључ особе I.

Рецимо да C жели да пошаље поруку B. B шаље C свој прстен, који садржи $S_A(K_B)$. Сада C има поверење у сертификате које добија од A.