RSA - Asimetricna kriptografija i primena

Aleksej Jocic

Uvod

- Simetricna kriptografija
  - Isti kljuc za sifrovanje i desifrovanje

Uvod

- Simetricna kriptografija
  - Isti kljuc za sifrovanje i desifrovanje
    $10101 \oplus 11001 = 01100$

Uvod

- Simetricna kriptografija
  - Isti kljuc za sifrovanje i desifrovanje
    $10101 \oplus 11001 = 01100$
    $(m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0 = m$

Uvod

- Simetricna kriptografija
  - Isti kljuc za sifrovanje i desifrovanje
    $10101 \oplus 11001 = 01100$
    $(m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0 = m$
  - Problem bezbedne razmene kljuceva

Uvod

- Simetricna kriptografija
  - Isti kljuc za sifrovanje i desifrovanje
    $10101 \oplus 11001 = 01100$
    $(m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0 = m$
  - Problem bezbedne razmene kljuceva
  - Problem autenticnosti

Uvod

- Asiemtricna kriptografija
  - Razliciti kljucevi za sifrovanje i desifrovanje

Uvod

- Asiemtricna kriptografija
  - Razliciti kljucevi za sifrovanje i desifrovanje
    $f(m, k1) = c$

Uvod

- Asiemtricna kriptografija
  - Razliciti kljucevi za sifrovanje i desifrovanje
    $f(m, k1) = c$
    $f(c, k2) = m$

Uvod

- Asiemtricna kriptografija
  - Razliciti kljucevi za sifrovanje i desifrovanje
    $f(m, k1) = c$
    $f(c, k2) = m$
  - Kljuc za sifrovanje je javno dostupan, (svi znaju $k1$)

Uvod

- Asiemtricna kriptografija
  - Razliciti kljucevi za sifrovanje i desifrovanje
    $f(m, k1) = c$
    $f(c, k2) = m$
  - Kljuc za sifrovanje je javno dostupan, (svi znaju $k1$)
  - Sifrovanje privatnim kljucem korisceno kao digitalni potpis

Uvod

- Asiemtricna kriptografija
  - Razliciti kljucevi za sifrovanje i desifrovanje
    $f(m, k1) = c$
    $f(c, k2) = m$
  - Kljuc za sifrovanje je javno dostupan, (svi znaju $k1$)
  - Sifrovanje privatnim kljucem korisceno kao digitalni potpis
    $f(m, k2) = c$

Uvod

- Asiemtricna kriptografija
  - Razliciti kljucevi za sifrovanje i desifrovanje
    $f(m, k1) = c$
    $f(c, k2) = m$
  - Kljuc za sifrovanje je javno dostupan, (svi znaju $k1$)
  - Sifrovanje privatnim kljucem korisceno kao digitalni potpis
    $f(m, k2) = c$
    $f(c, k1) = m$

- RSA
  - 1977. Ron Rivest, Adi Shamir, Leonard Adleman

- RSA
  - 1977. Ron Rivest, Adi Shamir, Leonard Adleman
  - 1976. Diffie–Hellman razmena kljuceva

RSA

- RSA
  - 1977. Ron Rivest, Adi Shamir, Leonard Adleman
  - 1976. Diffie–Hellman razmena kljuceva

$$g^a \equiv A \mod p$$

- RSA
  - 1977. Ron Rivest, Adi Shamir, Leonard Adleman
  - 1976. Diffie–Hellman razmena kljuceva

$g^a \equiv A \mod p$
$g^b \equiv B \mod p$

RSA

- RSA
  - 1977. Ron Rivest, Adi Shamir, Leonard Adleman
  - 1976. Diffie–Hellman razmena kljuceva

$$g^a \equiv A \mod p$$
$$g^b \equiv B \mod p$$
$$A^b \equiv (g^a)^b$$

- RSA
  - 1977. Ron Rivest, Adi Shamir, Leonard Adleman
  - 1976. Diffie–Hellman razmena kljuceva

$$g^a \equiv A \mod p$$
$$g^b \equiv B \mod p$$
$$A^b \equiv (g^a)^b \equiv (g^b)^a$$

- RSA
  - 1977. Ron Rivest, Adi Shamir, Leonard Adleman
  - 1976. Diffie–Hellman razmena kljuceva

$$g^a \equiv A \mod p$$
$$g^b \equiv B \mod p$$
$$A^b \equiv (g^a)^b \equiv (g^b)^a \equiv B^a$$

RSA

- RSA
  - 1977. Ron Rivest, Adi Shamir, Leonard Adleman
  - 1976. Diffie–Hellman razmena kljuceva

$$g^a \equiv A \mod p$$
$$g^b \equiv B \mod p$$
$$A^b \equiv (g^a)^b \equiv (g^b)^a \equiv B^a \mod p$$

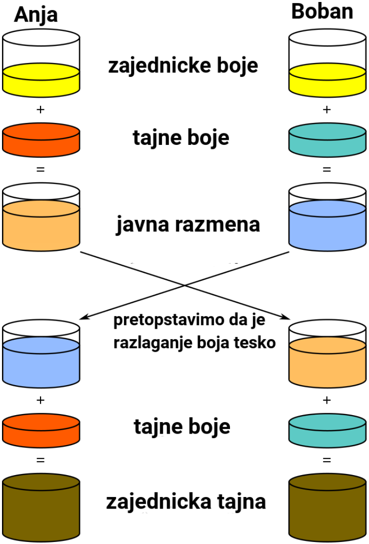

Figure 1: Diffie–Hellman

Mala Fermaova teorema

Ako je p prost broj, za svako a vazi:
$a^{p-1} \equiv 1 \mod p$

RSA

Mala Fermaova teorema

Ako je p prost broj, za svako a vazi:
$a^{p-1} \equiv 1 \mod p$

Posledica

Ako su p i q prosti brojevi, za svako a vazi:
$a^{(p-1)(q-1)}$

Mala Fermaova teorema

Ako je p prost broj, za svako a vazi:
$a^{p-1} \equiv 1 \mod p$

Posledica

Ako su p i q prosti brojevi, za svako a vazi:
$a^{(p-1)(q-1)} \equiv (a^{p-1})^{q-1}$

Mala Fermaova teorema

Ako je p prost broj, za svako a vazi:
$a^{p-1} \equiv 1 \mod p$

Posledica

Ako su p i q prosti brojevi, za svako a vazi:
$a^{(p-1)(q-1)} \equiv (a^{p-1})^{q-1} \equiv 1 \mod q$

Mala Fermaova teorema

Ako je p prost broj, za svako a vazi:
$a^{p-1} \equiv 1 \mod p$

Posledica

Ako su p i q prosti brojevi, za svako a vazi:
$a^{(p-1)(q-1)} \equiv (a^{p-1})^{q-1} \equiv 1 \mod q$
$a^{(p-1)(q-1)}$

RSA

Mala Fermaova teorema

Ako je p prost broj, za svako a vazi:
$a^{p-1} \equiv 1 \mod p$

Posledica

Ako su p i q prosti brojevi, za svako a vazi:
$a^{(p-1)(q-1)} \equiv (a^{p-1})^{q-1} \equiv 1 \mod q$
$a^{(p-1)(q-1)} \equiv (a^{q-1})^{p-1}$

RSA

Mala Fermaova teorema

Ako je p prost broj, za svako a vazi:
$a^{p-1} \equiv 1 \mod p$

Posledica

Ako su p i q prosti brojevi, za svako a vazi:
$a^{(p-1)(q-1)} \equiv (a^{p-1})^{q-1} \equiv 1 \mod q$
$a^{(p-1)(q-1)} \equiv (a^{q-1})^{p-1} \equiv 1 \mod p$

Mala Fermaova teorema

Ako je p prost broj, za svako a vazi:
$a^{p-1} \equiv 1 \mod p$

Posledica

Ako su p i q prosti brojevi, za svako a vazi:
$a^{(p-1)(q-1)} \equiv (a^{p-1})^{q-1} \equiv 1 \mod q$
$a^{(p-1)(q-1)} \equiv (a^{q-1})^{p-1} \equiv 1 \mod p$
$(a^{(p-1)(q-1)} - 1)$ je deljivo i sa p i q.

Mala Fermaova teorema

Ako je p prost broj, za svako a vazi:
$a^{p-1} \equiv 1 \mod p$

Posledica

Ako su p i q prosti brojevi, za svako a vazi:
$a^{(p-1)(q-1)} \equiv (a^{p-1})^{q-1} \equiv 1 \mod q$
$a^{(p-1)(q-1)} \equiv (a^{q-1})^{p-1} \equiv 1 \mod p$
$(a^{(p-1)(q-1)} - 1)$ je deljivo i sa p i q.
p i q su prosti, pa mora da je deljivo i sa $p \cdot q$.

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$

RSA

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$
Takodje: $a^{x(p-1)(q-1)}$

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$
Takodje: $a^{x(p-1)(q-1)} \equiv (a^x)^{(p-1)(q-1)}$

RSA

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$

Takodje: $a^{x(p-1)(q-1)} \equiv (a^x)^{(p-1)(q-1)} \equiv 1 \mod pq$

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$

Takodje: $a^{x(p-1)(q-1)} \equiv (a^x)^{(p-1)(q-1)} \equiv 1 \mod pq$

$a^{x(p-1)(q-1)+1} \equiv a \mod pq$

RSA

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$
Takodje: $a^{x(p-1)(q-1)} \equiv (a^x)^{(p-1)(q-1)} \equiv 1 \mod pq$
$a^{x(p-1)(q-1)+1} \equiv a \mod pq$

Trazimo

e i d tako da:
$(a^e)^d \equiv a^{ed} \equiv a^{x(p-1)(q-1)+1} \mod pq$

RSA

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$
Takodje: $a^{x(p-1)(q-1)} \equiv (a^x)^{(p-1)(q-1)} \equiv 1 \mod pq$
$a^{x(p-1)(q-1)+1} \equiv a \mod pq$

Trazimo

e i d tako da:
$(a^e)^d \equiv a^{ed} \equiv a^{x(p-1)(q-1)+1} \mod pq$
Odnosno: $ed \equiv 1 \mod (p-1)(q-1)$

RSA

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$
Takodje: $a^{x(p-1)(q-1)} \equiv (a^x)^{(p-1)(q-1)} \equiv 1 \mod pq$
$a^{x(p-1)(q-1)+1} \equiv a \mod pq$

Trazimo

e i d tako da:
$(a^e)^d \equiv a^{ed} \equiv a^{x(p-1)(q-1)+1} \mod pq$
Odnosno: $ed \equiv 1 \mod (p-1)(q-1)$
d je modularni inverz od e pod modulom $(p-1)(q-1)$

RSA

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$
Takodje: $a^{x(p-1)(q-1)} \equiv (a^x)^{(p-1)(q-1)} \equiv 1 \mod pq$
$a^{x(p-1)(q-1)+1} \equiv a \mod pq$

Trazimo

e i d tako da:
$(a^e)^d \equiv a^{ed} \equiv a^{x(p-1)(q-1)+1} \mod pq$
Odnosno: $ed \equiv 1 \mod (p-1)(q-1)$
d je modularni inverz od e pod modulom $(p-1)(q-1)$
Mozemo koristiti `Produzeni Euklidov algoritam`.

RSA

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$

Takodje: $a^{x(p-1)(q-1)} \equiv (a^x)^{(p-1)(q-1)} \equiv 1 \mod pq$

$a^{x(p-1)(q-1)+1} \equiv a \mod pq$

Trazimo

e i d tako da:

$(a^e)^d \equiv a^{ed} \equiv a^{x(p-1)(q-1)+1} \mod pq$

Odnosno: $ed \equiv 1 \mod (p-1)(q-1)$

d je modularni inverz od e pod modulom $(p-1)(q-1)$

Mozemo koristiti `Produzeni Euklidov algoritam`.

U buduce cemo oznacavati $n = pq$, a $\varphi(n) = (p-1)(q-1)$

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$

Takodje: $a^{x(p-1)(q-1)} \equiv (a^x)^{(p-1)(q-1)} \equiv 1 \mod pq$

$a^{x(p-1)(q-1)+1} \equiv a \mod pq$

Trazimo

e i d tako da:

$(a^e)^d \equiv a^{ed} \equiv a^{x(p-1)(q-1)+1} \mod pq$

Odnosno: $ed \equiv 1 \mod (p-1)(q-1)$

d je modularni inverz od e pod modulom $(p-1)(q-1)$

Mozemo koristiti `Produzeni Euklidov algoritam`.

U buduce cemo oznacavati $n = pq$, a $\varphi(n) = (p-1)(q-1)$

$a^{\varphi(n)} \equiv 1 \mod n$

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$
Takodje: $a^{x(p-1)(q-1)} \equiv (a^x)^{(p-1)(q-1)} \equiv 1 \mod pq$
$a^{x(p-1)(q-1)+1} \equiv a \mod pq$

Trazimo

e i d tako da:
$(a^e)^d \equiv a^{ed} \equiv a^{x(p-1)(q-1)+1} \mod pq$
Odnosno: $ed \equiv 1 \mod (p-1)(q-1)$
d je modularni inverz od e pod modulom $(p-1)(q-1)$
Mozemo koristiti `Produzeni Euklidov algoritam`.
U buduce cemo oznacavati $n = pq$, a $\varphi(n) = (p-1)(q-1)$
$a^{\varphi(n)} \equiv 1 \mod n$
$a^{ed} \equiv a^{x\varphi(n)+1}$

RSA

Primecujemo

$a^{(p-1)(q-1)} \equiv 1 \mod pq$
Takodje: $a^{x(p-1)(q-1)} \equiv (a^x)^{(p-1)(q-1)} \equiv 1 \mod pq$
$a^{x(p-1)(q-1)+1} \equiv a \mod pq$

Trazimo

e i d tako da:
$(a^e)^d \equiv a^{ed} \equiv a^{x(p-1)(q-1)+1} \mod pq$
Odnosno: $ed \equiv 1 \mod (p-1)(q-1)$
d je modularni inverz od e pod modulom $(p-1)(q-1)$
Mozemo koristiti `Produzeni Euklidov algoritam`.
U buduce cemo oznacavati $n = pq$, a $\varphi(n) = (p-1)(q-1)$
$a^{\varphi(n)} \equiv 1 \mod n$
$a^{ed} \equiv a^{x\varphi(n)+1} \equiv a \mod n$

RSA

- Problem faktorisanja $n = pq$

RSA

- Problem faktorisanja $n = pq$
- $\varphi(n) = (p-1)(q-1)$ nije poznato bez p i q

RSA

- Problem faktorisanja $n = pq$
- $\varphi(n) = (p-1)(q-1)$ nije poznato bez p i q
- d kao modularni inverz od e nije poznat bez $\varphi(n)$

RSA

- Problem faktorisanja $n = pq$
- $\varphi(n) = (p-1)(q-1)$ nije poznato bez p i q
- d kao modularni inverz od e nije poznat bez $\varphi(n)$
- d mozemo da cuvamo tajnim cak i ako objavimo e i n javno

RSA

- Problem faktorisanja $n = pq$
- $\varphi(n) = (p-1)(q-1)$ nije poznato bez p i q
- d kao modularni inverz od e nije poznat bez $\varphi(n)$
- d mozemo da cuvamo tajnim cak i ako objavimo e i n javno

RSA

- Generisanje kljuceva
  - Nadjimo velike proste brojeve p i q

RSA

- Generisanje kljuceva
  - Nadjimo velike proste brojeve p i q
    Testovi prostosti brojeva (Fermaov test)

RSA

- Generisanje kljuceva
  - Nadjimo velike proste brojeve p i q
    Testovi prostosti brojeva (Fermaov test)
  - Generisemo $n = pq$

RSA

- Generisanje kljuceva
  - Nadjimo velike proste brojeve p i q
    Testovi prostosti brojeva (Fermaov test)
  - Generisemo $n = pq$
  - Nadjimo e koji je uzajamno prost sa $(p-1)(q-1)$

RSA

- Generisanje kljuceva
    - Nadjimo velike proste brojeve p i q
      Testovi prostosti brojeva (Fermaov test)
    - Generisemo $n = pq$
    - Nadjimo e koji je uzajamno prost sa $(p-1)(q-1)$
    - Nadjimo d koriscenjem Produzenog Euklidovog algoritma

RSA

- Generisanje kljuceva
  - Nadjimo velike proste brojeve p i q
    Testovi prostosti brojeva (Fermaov test)
  - Generisemo $n = pq$
  - Nadjimo e koji je uzajamno prost sa $(p-1)(q-1)$
  - Nadjimo d koriscenjem Produzenog Euklidovog algoritma
  - Zaboravimo p i q, jer nam vise ne trebaju

RSA

- Generisanje kljuceva
  - Nadjimo velike proste brojeve p i q
    Testovi prostosti brojeva (Fermaov test)
  - Generisemo $n = pq$
  - Nadjimo e koji je uzajamno prost sa $(p-1)(q-1)$
  - Nadjimo d koriscenjem Produzenog Euklidovog algoritma
  - Zaboravimo p i q, jer nam vise ne trebaju
- Javni kljuc se sastoji od brojeva e i n
  $m^e \equiv C \mod n$

RSA

- Generisanje kljuceva
  - Nadjimo velike proste brojeve p i q
    Testovi prostosti brojeva (Fermaov test)
  - Generisemo $n = pq$
  - Nadjimo e koji je uzajamno prost sa $(p-1)(q-1)$
  - Nadjimo d koriscenjem Produzenog Euklidovog algoritma
  - Zaboravimo p i q, jer nam vise ne trebaju
- Javni kljuc se sastoji od brojeva e i n
  $m^e \equiv C \mod n$
- Privatni kljuc se sastoji od brojeva d i n
  $C^d \equiv m \mod n$

RSA

- Generisanje kljuceva
  - Nadjimo velike proste brojeve p i q
    Testovi prostosti brojeva (Fermaov test)
  - Generisemo $n = pq$
  - Nadjimo e koji je uzajamno prost sa $(p-1)(q-1)$
  - Nadjimo d koriscenjem Produzenog Euklidovog algoritma
  - Zaboravimo p i q, jer nam vise ne trebaju
- Javni kljuc se sastoji od brojeva e i n
  $m^e \equiv C \mod n$
- Privatni kljuc se sastoji od brojeva d i n
  $C^d \equiv m \mod n$
- Digitalni potpis se postize sifrovanjem sa privatim kljucem
  $m^d \equiv S \mod n$

RSA

- Generisanje kljuceva
  - Nadjimo velike proste brojeve p i q
    Testovi prostosti brojeva (Fermaov test)
  - Generisemo $n = pq$
  - Nadjimo e koji je uzajamno prost sa $(p-1)(q-1)$
  - Nadjimo d koriscenjem Produzenog Euklidovog algoritma
  - Zaboravimo p i q, jer nam vise ne trebaju
- Javni kljuc se sastoji od brojeva e i n
  $m^e \equiv C \mod n$
- Privatni kljuc se sastoji od brojeva d i n
  $C^d \equiv m \mod n$
- Digitalni potpis se postize sifrovanjem sa privatim kljucem
  $m^d \equiv S \mod n$
- Provera digitalnog potpisa: $S^e \equiv m \mod n$

Prodruzeni Euklidov algoritam

```
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    g, y, x = egcd(b%a,a)
    return (g, x - (b//a) * y, y)

def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        raise Exception('No modular inverse')
    return x%m
```

Napadi na RSA

- Napadi na RSA
  - Pogadjanje poruke, potrebno dopunjavanje poruke random podacima (padding)

Napadi na RSA

- Napadi na RSA
  - Pogadjanje poruke, potrebno dopunjavanje poruke random podacima (padding)
  - Premali eksponent e, korenovanje sifrovanog teksta za male poruke (veliko e)

Napadi na RSA

- Napadi na RSA
  - Pogadjanje poruke, potrebno dopunjavanje poruke random podacima (padding)
  - Premali eksponent e, korenovanje sifrovanog teksta za male poruke (veliko e)
  - Koriscenje istog eksponenta za vise kljuceva, napad koriscenjem Kineske teoreme o ostatku (random izabrano e)

- Napadi na RSA
  - Pogadjanje poruke, potrebno dopunjavanje poruke random podacima (padding)
  - Premali eksponent e, korenovanje sifrovanog teksta za male poruke (veliko e)
  - Koriscenje istog eksponenta za vise kljuceva, napad koriscenjem Kineske teoreme o ostatku (random izabrano e)
  - Desifrovanje sumnjivog teksta, $(x^e \cdot C)^d \equiv (x^e)^d \cdot C^d \equiv x \cdot m \mod n$

Primena

GNU Privacy Guard

- 1999. Werner Koch

Primena

GNU Privacy Guard

- 1999. Werner Koch
- Generisanje kljuca: `gpg --gen-key`

Primena

GNU Privacy Guard

- 1999. Werner Koch
- Generisanje kljuca: `gpg --gen-key`
- Lista javnih kljuceva: `gpg --list-keys`

Primena

GNU Privacy Guard

- 1999. Werner Koch
- Generisanje kljuca: `gpg --gen-key`
- Lista javnih kljuceva: `gpg --list-keys`
- Export privatnih kljuceva: `gpg --export-secret-keys --output backup.gpg`

Primena

GNU Privacy Guard

- 1999. Werner Koch
- Generisanje kljuca: `gpg --gen-key`
- Lista javnih kljuceva: `gpg --list-keys`
- Export privatnih kljuceva: `gpg --export-secret-keys --output backup.gpg`
- Upload kljuceva: `gpg --send-key [KEYID]`

Primena

GNU Privacy Guard

- 1999. Werner Koch
- Generisanje kljuca: `gpg --gen-key`
- Lista javnih kljuceva: `gpg --list-keys`
- Export privatnih kljuceva: `gpg --export-secret-keys --output backup.gpg`
- Upload kljuceva: `gpg --send-key [KEYID]`
- Sifrovanje poruke: `gpg -e file.txt`

Primena

GNU Privacy Guard

- 1999. Werner Koch
- Generisanje kljuca: `gpg --gen-key`
- Lista javnih kljuceva: `gpg --list-keys`
- Export privatnih kljuceva: `gpg --export-secret-keys --output backup.gpg`
- Upload kljuceva: `gpg --send-key [KEYID]`
- Sifrovanje poruke: `gpg -e file.txt`
- Desifrovanje: `gpg -d file.txt`

Primena

GNU Privacy Guard

- 1999. Werner Koch
- Generisanje kljuca: `gpg --gen-key`
- Lista javnih kljuceva: `gpg --list-keys`
- Export privatnih kljuceva: `gpg --export-secret-keys --output backup.gpg`
- Upload kljuceva: `gpg --send-key [KEYID]`
- Sifrovanje poruke: `gpg -e file.txt`
- Desifrovanje: `gpg -d file.txt`
- Potpisivanje poruke ili fajla: `gpg -s file.exe`

Primena

GNU Privacy Guard

- 1999. Werner Koch
- Generisanje kljuca: `gpg --gen-key`
- Lista javnih kljuceva: `gpg --list-keys`
- Export privatnih kljuceva: `gpg --export-secret-keys --output backup.gpg`
- Upload kljuceva: `gpg --send-key [KEYID]`
- Sifrovanje poruke: `gpg -e file.txt`
- Desifrovanje: `gpg -d file.txt`
- Potpisivanje poruke ili fajla: `gpg -s file.exe`
- Potpisivanje kljuca: `gpg --sign-key [KEYID]`

Primena

GNU Privacy Guard

- 1999. Werner Koch
- Generisanje kljuca: `gpg --gen-key`
- Lista javnih kljuceva: `gpg --list-keys`
- Export privatnih kljuceva: `gpg --export-secret-keys --output backup.gpg`
- Upload kljuceva: `gpg --send-key [KEYID]`
- Sifrovanje poruke: `gpg -e file.txt`
- Desifrovanje: `gpg -d file.txt`
- Potpisivanje poruke ili fajla: `gpg -s file.exe`
- Potpisivanje kljuca: `gpg --sign-key [KEYID]`
- ASCII output: `gpg --armor -se file.txt`

Primena

GNU Privacy Guard

- 1999. Werner Koch
- Generisanje kljuca: `gpg --gen-key`
- Lista javnih kljuceva: `gpg --list-keys`
- Export privatnih kljuceva: `gpg --export-secret-keys --output backup.gpg`
- Upload kljuceva: `gpg --send-key [KEYID]`
- Sifrovanje poruke: `gpg -e file.txt`
- Desifrovanje: `gpg -d file.txt`
- Potpisivanje poruke ili fajla: `gpg -s file.exe`
- Potpisivanje kljuca: `gpg --sign-key [KEYID]`
- ASCII output: `gpg --armor -se file.txt`
- GPG password manager: `gpg --armor -c passwords.txt`

Primena

Git

- Podesavanje kljuca: `git config --global user.signingkey [KEYID]`

Primena

Git

- Podesavanje kljuca: `git config --global user.signingkey [KEYID]`
- Potpisivanje komita: `git commit -S`

Primena

Git

- Podesavanje kljuca: `git config --global user.signingkey [KEYID]`
- Potpisivanje komita: `git commit -S`

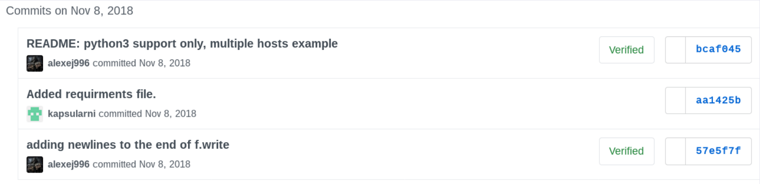

Figure 2: Github signed commits

Primena

SSH

- Generisanje kljuca: `ssh-keygen [-f filename]`

Primena

SSH

- Generisanje kljuca: `ssh-keygen [-f filename]`
- Dodavanje kljuca na remote masinu: `ssh-copy-id [-i filename] user@hostname`

Primena

SSH

- Generisanje kljuca: `ssh-keygen [-f filename]`
- Dodavanje kljuca na remote masinu: `ssh-copy-id [-i filename] user@hostname`
- `~/.ssh/authorized_keys`

Tor

- 1990.-te United States Naval Research Laboratory (Paul Syverson,Michael G. Reed,David Goldschlag)

Tor

- 1990.-te United States Naval Research Laboratory (Paul Syverson,Michael G. Reed,David Goldschlag)
- 20.9.2002. prva verzija Tor-a (javni projekat, anonimnosti u masi)

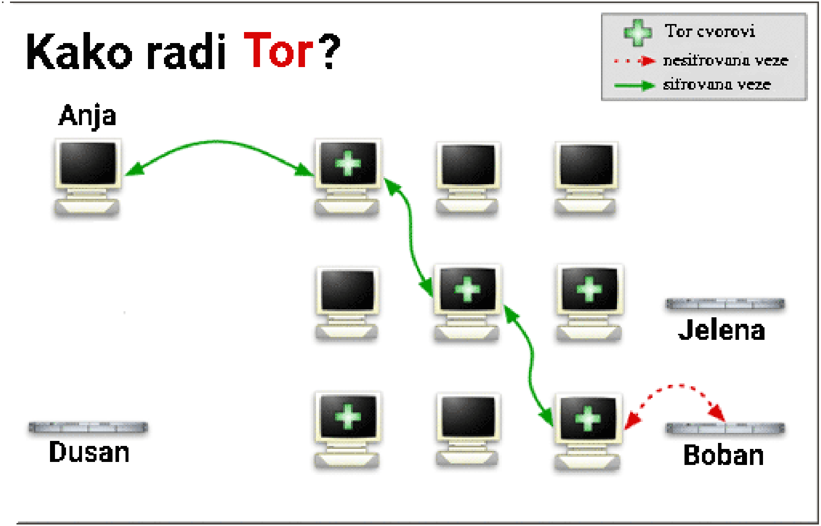

Figure 3: How Tor works

Onion hidden services

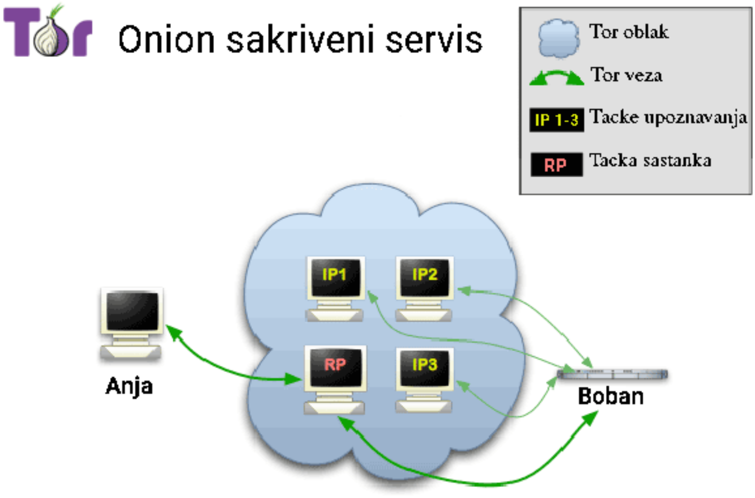

Figure 4: How hidden services works

The Onion Router

- Napadi na Tor
  - Tor ne stiti od vremenske korelacije (pristup sa obe strane veze)

- Napadi na Tor
  - Tor ne stiti od vremenske korelacije (pristup sa obe strane veze)
  - Slabosti u aplikacijama koje koriste Tor

The Onion Router

- Napadi na Tor
  - Tor ne stiti od vremenske korelacije (pristup sa obe strane veze)
  - Slabosti u aplikacijama koje koriste Tor
  - Pogresno konfigurisane aplikacije

The Onion Router

- Napadi na Tor
  - Tor ne stiti od vremenske korelacije (pristup sa obe strane veze)
  - Slabosti u aplikacijama koje koriste Tor
  - Pogresno konfigurisane aplikacije
  - DNS Leak

Hvala

Hvala na paznji!