SSL/TLS

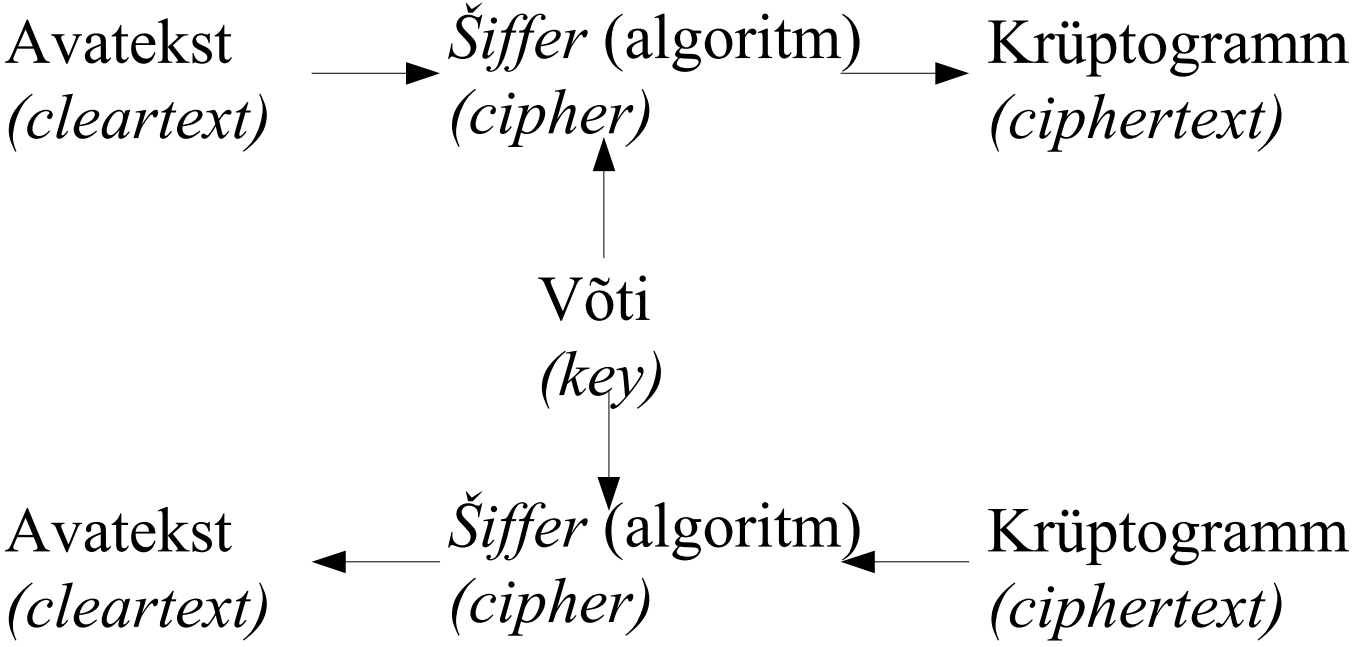
- „kiiks”
  - kuigi tänapäeval tegelikult kasutatakse TLS-i, räägitakse ikka veel SSL-i kasutamisest...

SSL/TLS

- Ühenduse krüpteerimise protokollid (ISO/OSI seansikiht)
  - SSL – Secure Sockets layer
    - SSLv2 – ebaturvaline
    - SSLv3 – ebaturvaline
  - TLS – Transport Layer Security
    - TLS 1.0 – ebaturvaline
    - TLS 1.1 – ebaturvaline
    - TLS 1.2 – OK
    - TLS 1.3 – OK

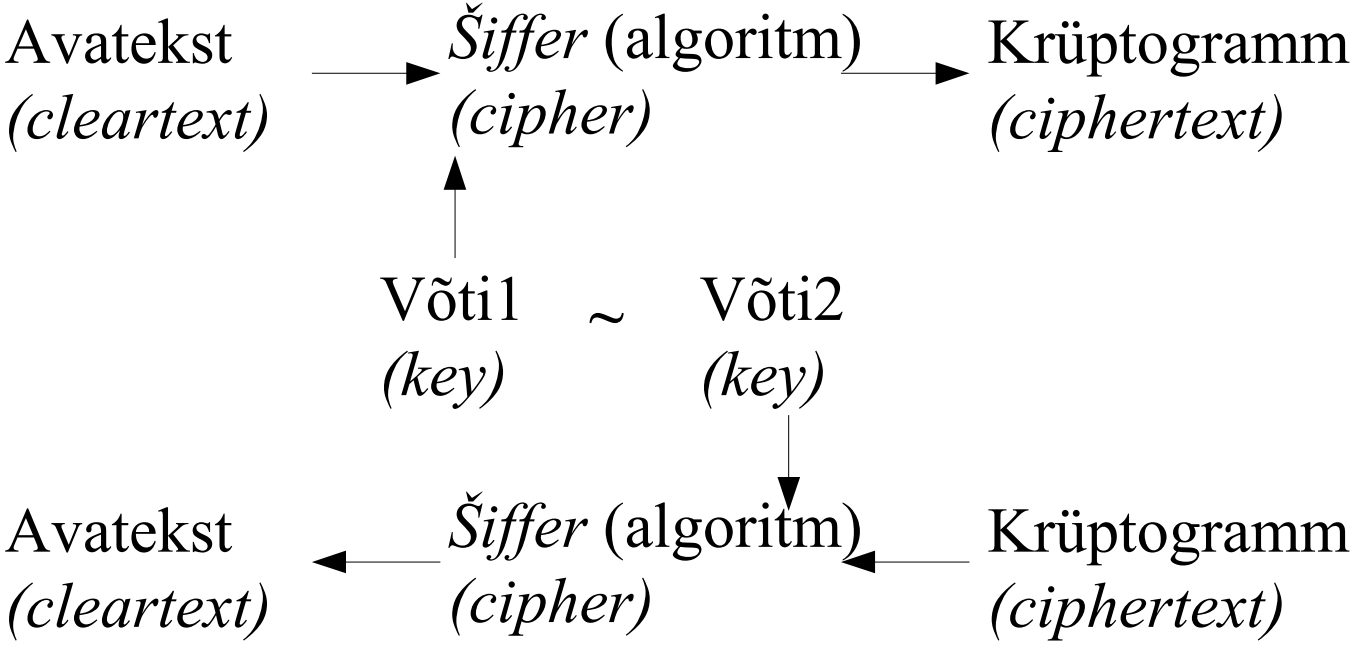
Sümmeetriline krüptoalgoritm

- „Kinni” ja „lahti” krüpteerimine käib sama võtmega



Asümmeetriline krüptoalgoritm

- „Kinni” ja „lahti” erinevate võtmetega



Võtmete pikkused

- Sümmeetriliste krüptoalgoritmide korral
  - 128bit, 256bit
- Asümmeetriliste krüptoalgoritmide korral
  - RSA – 2048bit, 3072bit, 4096bit
  - ECC – 256bit, 384bit

Kasutusalad

- Sümmeetrilised krüptoalgoritmid
  - kuna on kiired, siis kasutatakse reaalsel andmete krüpteerimisel
- Asümmeetrilised krüptoalgoritmid
  - on oluliselt aeglasemad kui sümmeetrilised, kasutatakse
    - võtmevahetuse algoritmides
      - krüpteeritakse võtmeid või võtmevahetuse andmeid (väike maht)
    - digitaalsel signeerimisel (allkirjastamisel)
      - krüpteeritakse räsisid (väike maht)

Avaliku võtme infrastruktuur

- Asümmeetrilise krüptoalgoritmi võtmed genereeritakse võtmepaarina koos ja need on omavahel matemaatiliselt seotud
  - ühest võtmest pole võimalik (st on väga töömahukas) tuletada teist võtit
- Võtmepaarist üks võti kuulutatakse salajaseks ja teine avalikuks
- Salajase võtmega krüpteeritut (krüptogramm) saab lahti krüpteerida vaid avaliku võtmega ja vastupidi – avaliku võtmega krüpteeritut saab lahti ainult salajase võtmega

Avaliku võtme infrastruktuur (*Public Key Infrastructure*, PKI)

- Salajane võti hoitakse salajas
  - (veebi)serveris failis (parooliga kaitstult või ilma)
  - eraldi seadmel, kust seda kätte ei saa – ID-kaardil, mobiil-ID SIM kaardil, USB „token”
  - jagatult erinevates kohtades (SmartID hoiab osa salajasest võtmest telefonis, osa keskserveris...)
- Avalik võti avalikustatakse – on kõigile vabalt saadaval
  - Kuidas seda teha?
  - Kuidas olla kindel, et avalik võti on just õige omaniku oma?

Sertifikaat

- Sertifikaat – tõend, mandaat
  - on avalik võti
  - koos sellele väljaandja poolt lisatud infoga
    - kehtivuse alguse ja lõpu ajad
    - kasutusotstarve
    - omaniku info, ...
  - digitaalselt signeeritud (allkirjastatud) väljaandja poolt
- Peaks tõestama, et see avalik võti kuulub sellele, kelle nimele sertifikaat on väljastatud

Sertifikaadi väljaandja

- Sertifikaadi väljaandjal *(Certificate Authority, CA)* on oma avaliku-salajase võtme paar
- Välja antav sertifikaat allkirjastatakse CA salajase võtmega
  - välja antud sertifikaadi õigsust saab kontrollida CA avaliku võtme abil
    - CA avalik võti on samuti avalik ja CA sertifikaadi osa
- Avaliku PKI sertifikaadi väljaandja **peab** tagama, et sertifikaat antaks välja vaid õigele isikule

Sertifikaatide ahel

- CA sertifikaat võib olla (tavaliselt ongi) samuti välja antud mõne sertifitseerija poolt
  - Nii tekib sertifikaatide ahel, kus sertifikaadid on omavahel krüptograafiliselt seotud (signeeritud). Sertifikaati on võimalik kontrollida, kui on teada, et usaldada võib üht neist ülemsertifikaatidest. **Tavaliselt usaldatakse** kõige kõrgemat/algsemat, mille põhjal on välja antud CA sertifikaadid – **juursertifikaati**

Juursertifikaadid

- Juursertifikaadid (mida usaldatakse) asuvad igas kasutaja seadmes – arvutis/telefonis/brauseris mingis andmabaasis/sertifikaadihoidlas, kuhu neid tavaliselt paneb (ja uuendab) tarkvaratootja
  - Veebibrauseri sisemises sertifikaadihoidlas
  - OS-i keskses sertifikaadihoidlas
  - veebiserveris failides (nt kliendi ID-kaardiga autentimiseks)
- **Tasub olla ettevaatlik** (suvaliste) juursertide lisamisega oma seadme sertifikaadihoidlasse – kui sert on juba hoidlas, siis seda usaldadakse ja loetakse legaalseks ka **kõik** selle serdi põhjal välja antud serdid!

Sertifikaadi kehtivus

- Sertifikaat kehtib, kui on täidetud tingimused
  - praegune ajahetk jääb sertifikaadi kasutamise ajavahemikku (sertifikaadis kirjas)
    - samuti CA serdil ning kõigil ülejäänud vahesertidel kuni juurserdini välja
  - sert on korrektne, signatuur kehtib, CA serti on lubatud kasutada CA-na e sertide väljastamiseks
    - samuti selle serdi väljastanud CA sert ning kõik ülejäänud vaheserdid kuni juurserdini välja
  - serdi ega ühegi vaheserdi kehtivust pole tühistatud või peatatud

Sertifikaadi tühistamine

- CA saab/võib/peab võimaldama vajadusel sertifikaadi kehtivust peatada või tühistada. Näiteks kui selgub, et
  - salajane võti on lekkinud
  - sertifikaati kasutatakse mittesihipäraselt
  - sertifikaat on välja antud valesti (valele isikule)
  - kasutaja enam ei kasuta sertifikaati...
- Kui sertifikaat peatatakse või tühistatakse, paneb CA selle fakti sertifikaadi välja andnud CA serdi juurde käivasse andmebaasi kirja ning levitab seda infot

Sertifikaadi tühistamine

- Sertifikaatide tühistamise/peatamise kohta levitatakse infot peamiselt kahel viisil
  - Tühistusnimekirjade või
  - OCSP (Online Certificate Status Protocol) teenuse abil
- Sertifikaadi kehtivuse kontrollimisel peaks kontrollija (nt veebibrauser) kontrollima serdi ja kõigi CA vahesertide olekut tühistusinfo suhtes

Tühistusnimekirjad

- Igal CA serdil on oma tühistusnimekiri, kus kirjas info selle serdiga välja antud, aga tühistatud või peatatud sertide kohta
  - avalikult faili kujul võrgust tõmmatav, URL serdis kirjas
  - + tavaliselt tasuta (nt ka Eesti ID-kaardi korral)
  - + krüptograafiliselt seotud (signeeritud?) CA serdiga, pole vaja tõmbamiseks kasutada krüpteeritud ühendust
  - – aja jooksul võivad minna (väga) mahukaks
  - – tuleb värskendada mingi aja tagant (kehtib mingi aja), tühistusinfo ei jõua koheselt serdi kontrollijani

Online Certificate Status Protocol

- OCSP teenus – online tühistusinfo teenus
  - teenuse URL serdis kirjas
  - päringute vastused samuti krüptograafiliselt seotud ja kehtivad mingi aja
  - antakse vastus (vaid) küsitud sertifikaadi seisundi kohta selle küsimise hetkel – võib olla kindel, et sert oli küsimise hetkel vastuses olevas seisundis
  - + päringud väikesed ja kiired
  - – teenuse võrguliiklus võib minna (CA juures) väga mahukaks kuigi väiksemaks kui tühistusnimekirjade korral
  - – teatud juhtudel võib teenus olla tasuline (Eesti ID-kaart)
  - – CA saab päringute järgi teada, milliseid saite kasutaja külastab

HTTPS Veebiserver

Sertifikaadipäringu loomine

- Salajase võtme ja sertifikaadipäringu loomine

```
openssl req -new -nodes -newkey
rsa:2048 -keyout salajane.key -out
serdiparing.csr
```

- Vaatamine
  - `openssl req -in serdiparing.csr -text`
  - `openssl x509 -in sert.crt -text`

Veebiserveri käsud

- Start/stop/restart
  - `systemctl start httpd`
  - `systemctl stop httpd`
  - `systemctl restart httpd`
- Konfiguratsiooni kontroll
  - `apachectl configtest`
- Virtuaalserverite nimekiri
  - `httpd -S`

Tulemüüri käsud

- Start/stop analoogiline
  - `systemctl stop firewalld`
- Enable/Disable (käivitamine masina käivitumisel)
  - `systemctl disable firewalld`

Tulemüüri seadistamine

Käsurealt

- Tulemüüril (firewalld) on kaks „keskkonda”
  - runtime – töökeskkond, mis hetkel kehtib
  - permanent – mis hakkab kehtima peale restarti

Tulemüüri seadistamine

- Pordi avamine
  - töökeskkonnas
    - `firewall-cmd --zone=public –add-port=443/tcp`
  - Et ka peale restarti kehtiks
    - firewall-cmd --permanent --zone=public –add-port=443/tcp
    - firewall-cmd -reload
- Teenuse avamine analoogiliselt
    - firewall-cmd --permanent --zone=public --add-service=http

Lingid

- Mozilla soovituslik SSL/TLS konfiguratsiooni generaator

  https://mozilla.github.io/server-side-tls/ssl-config-generator/

- Veebisaidi SSL seadistuse kontroll

  www.ssllabs.com -> Test your server ehk

  https://www.ssllabs.com/ssltest/

  - Kohalikus masinas jooksev SSL tester

    https://github.com/drwetter/testssl.sh

Lingid

- Lisaks serveri HTTPS protokolli seadistusele tuleks turvaliseks seadistada ka veebisaidi poolt kasutatavad
  - küpsised
  - HTTP protokolli päised
- Nende tester

  https://securityheaders.com
- Mozilla web security guidelines
  - https://infosec.mozilla.org/guidelines/web_security