TEKNILLINEN KORKEAKOULU

# Salaustekniikat

Kirja sivut: 580-582 (647-668)

# Johdanto

- Salaus on perinteisesti ollut salakirjoitusta, viestin luottamuksellisuuden suojaamista koodaamalla viesti tavalla, jonka vain vastaanottaja(t) pystyy avaamaan
- Salaustekniikat ovat kehittyneet voimakkaasti 1900-luvulla ja sen jälkeen
- Nykyiset salaustekniikat tuottavat käytännössä murtamattoman suojan sekä luottamuksellisuudelle että eheydelle
  - Lisäksi salaustekniikoilla voidaan toteuttaa kiistämättömyys, sähköisen allekirjoituksen muodossa

TEKNILLINEN KORKEAKOULU

# Salausjärjestelmän osat

- Salausalgoritmi
  - Salaa dataa ja purkaa salauksen
    - Usein määrämittaisia lohkoja, esim. 8 tai 16 tavun mittaisia
  - Yleensä oletetaan, että algoritmi on julkinen tai ainakaan salauksen tehokkuus ei perustu algoritmin salaukseen
- Salausavain tai -avaimet
  - Ohjaa algoritmia tuottamaan ja avaamaan tietyn salauksen
  - Oltava riittävän pitkä, jotta vaihtoehtoisia avaimia olisi niin paljon, että arvaamishyökkäys ei ole mahdollinen
  - Usein avain tai osa avaimista on pidettävä salassa
- Salattava data
- Salattu data

# Salauksen murtuminen

- Heikko salausalgoritmi
  - Esim. tuottaa eri avaimilla saman salaustuloksen
  - Saattaa olla myös tahallisesti heikennetty
- Heikko avain
  - Liian lyhyt
  - Eräät algoritmit ovat herkkiä tietyille avaimille (kaikki bitit nollia tms.)
- Hyökkäykset
  - Koko avainavaruuden läpi käyminen
    - Tehoaa esim. Windowsin ja Unixin salasanoihin
  - Salattavan sisällön valitseminen
  - Algoritmin analysointi ja heikkouksien etsiminen
  - Hyökkäyksen kohdistaminen salaamatonta tietoa vastaan

# Miten salaus toimii?

- Salaisen avaimen salauksessa molemmat osapuolet käyttävät samaa avainta
- Julkisen avaimen salauksessa salaajalla on kaksi avainta, yksityinen ja julkinen
  - Kuka tahansa, jolla on julkinen avain tiedossaan, voi salata tiedon sen avulla
  - Vain vastaanottaja, joka tietää yksityisen avaimen, voi avata salatun viestin
- Avaimet ovat bittijonoja
- Salausta voidaan käyttää tietoliikenteen, kuten WWW-yhteyksien tai sähköpostin, salaamiseen

TEKNILLINEN KORKEAKOULU

# Salaisen avaimen salaus eli symmetrinen salaus

- Osapuolilla on jaettu salaisuus
  - Salaisuutta käytetään salausavaimena
- Lisäksi on sovittu käytettävä algoritmi
- Lähettäjän algoritmi käyttää avainta tuottaakseen selväkielisestä viestistä salatun ja vastaanottajan algoritmi avaa viestin samalla avaimella
- Symmetriset algoritmit ovat yleensä laskennallisesti tehokkaita ja riittävällä avaimenpituudella käytännössä murtamattomia
- Suurin ongelma on avaintenvaihto, miten saada sama salaisuus molemmille osapuolille

TEKNILLINEN KORKEAKOULU

# Esimerkki salaisen avaimen salauksesta

- Liki kaikki salaisen avaimen algoritmit perustuvat sekoittamiselle ja hajauttamiselle
  - Bittikuvioita korvataan toisilla ja bittien paikkoja vaihdetaan
- Tässä on osa IDEA-algoritmia
  - Syötedatastaa operoidaan salausavaimen osien kanssa ja tuloksien paikkoja vaihdetaan
  - Sama toistetaan useita kertoaj

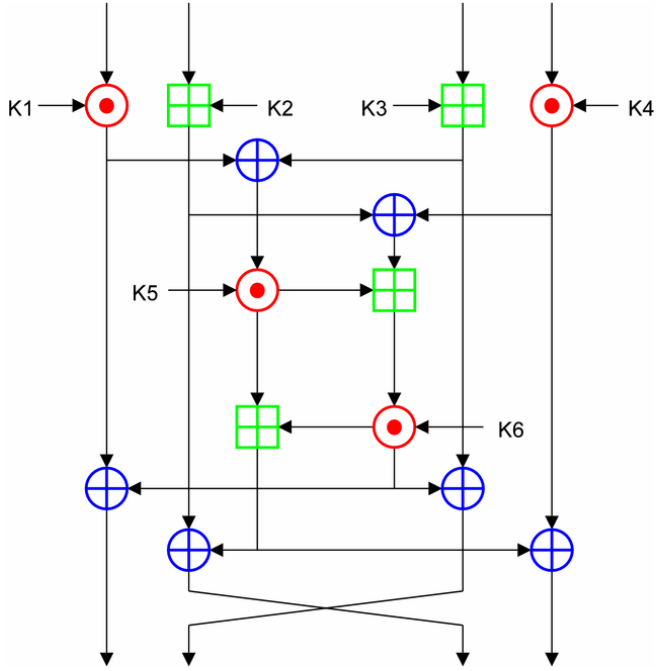



Image © Matt Crypto/Wikipedia

multiplication modulo $2^{16} + 1$

addition modulo $2^{16}$

bitwise XOR

TEKNILLINEN KORKEAKOULU

# Julkisen avaimen salaus

- Julkisen avaimen (asymmetrinen) salaus perustuu algoritmeihin, jotka käyttävät eri avainta salaamiseen ja avaamiseen
  - Avaimet ovat keskenään suhteessa
- Toista avainta kutsutaan julkiseksi ja se voidaan julkaista
  - Sillä salattu viesti aukeaa vain yksityisellä avaimella
- Yksityinen avain on pidettävä salassa
- Julkisen avaimen salaus ei ole yleensä laskennallisesti tehokasta
  - Usein luodaan istuntoavain symmetristä salausta varten ja käytetään julkisen avaimen salausta istuntoavaimen välittämiseksi turvallisesti toiselle osapuolelle

TEKNILLINEN KORKEAKOULU

# Esimerkki julkisen avaimen algoritmista

- Rivest, Shamir ja Adleman kehittivät RSA-algoritmin 1978
- Avainten luonti
  - Valitaan kaksi suurta alkulukua p ja q
  - Talletetaan n=pq
  - Valitaan julkinen avain e, jolla ei ole yhteisiä tekijöitä (p-1)(q-1):n kanssa
  - Yksityinen avain d toteuttaa lauseen ed = 1 mod ((p-1)(q-1))
  - p ja q tuhotaan
- Salaus
  - Kohdellaan viestiä m lukuna ja lasketaan salaviesti $c = m^e \bmod n$
- Purku
  - $c^d \bmod n$ purkaa viestin ja tuottaa
- Toimii koska ed = 1 mod ((p-1)(q-1))
  - Josta seuraa $m^{ed} \bmod n = m \bmod n$

TEKNILLINEN KORKEAKOULU

# Allekirjoitus

- Useat julkisen avaimen algoritmit toimivat myös toisinpäin
  - Viestin, joka aukeaa julkisella avaimella, on oltava salattu yksityisellä avaimella
- Näin voidaan allekirjoittaa dokumentti (tiedosto, tekstinpätkä, dataa)
- Allekirjoitusohjelma laskee datasta tiivisteen (hash) ja salaa sen yksityisellä avaimella
- Allekirjoitus voidaan tarkistaa julkisen avaimen avulla

TEKNILLINEN KORKEAKOULU

# Yksisuuntaiset kryptografiset tiivistefunktiot

- Kryptografiset tiivistefunktiot tuottavat syötedatastaan määrämittaisen bittijonon
  - Funktio on yksisuuntainen, tiivisteestä ei voi päätellä syötedataa
  - Funktio on törmäyksetön, ei ole laskennallisesti käytännöllistä tuottaa dataa, joka tuottaisi saman tiivisteen
    - Tyypillisesti yhden bitin muuttuminen syötteessä muuttaa puolet tuloksen biteistä
- Tunnettuja tiivistefunktioita ovat esim. SHA-1 (160-bit tuloste) ja MD5 (128-bit tuloste)
  - Os tiivistefunktioista ottaa suoraan allekirjoitusavaimen argumentikseen
- Kun tiivistefunktiolla allekirjoitetaan tietoliikenneviestejä eheyden suojaamiseksi, puhutaan MAC-koodeista (Message Authentication Code)

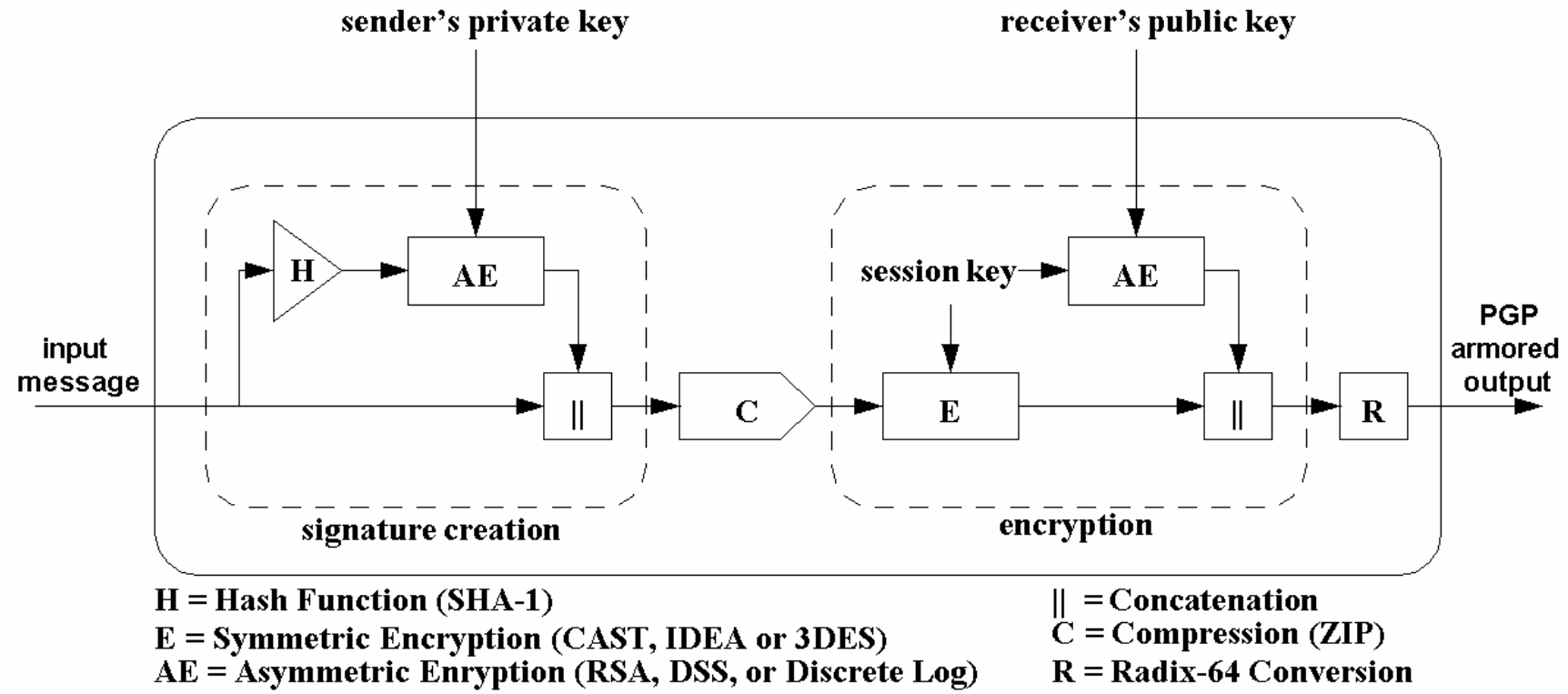
TEKNILLINEN KORKEAKOULU

# Esimerkki kokonaisuudesta: PGP

- Pretty Good Privacy, eräs ensimmäisiä yleisiä julkisen avaimen salauksen toteuttavia sovelluksia
- Toteuttaa sähköpostin ja tiedostojen salauksen
- Kullakin käyttäjällä on *avainrengas*, johon kerätään viestintäkumppanien julkisia avaimia
  - Esimerkiksi hakemalla WWW-sivulta
- Avaimen oikeellisuudesta voi varmistua esim. vertailemalla avaimien sormenjälkiä
  - Lasketaan tiiviste-funktiolla avaimesta
  - Lyhyt lukusarjan, jonka voi painaa käyntikorttiin, lähettää SMS-viestinä tai lukea puhelimessa

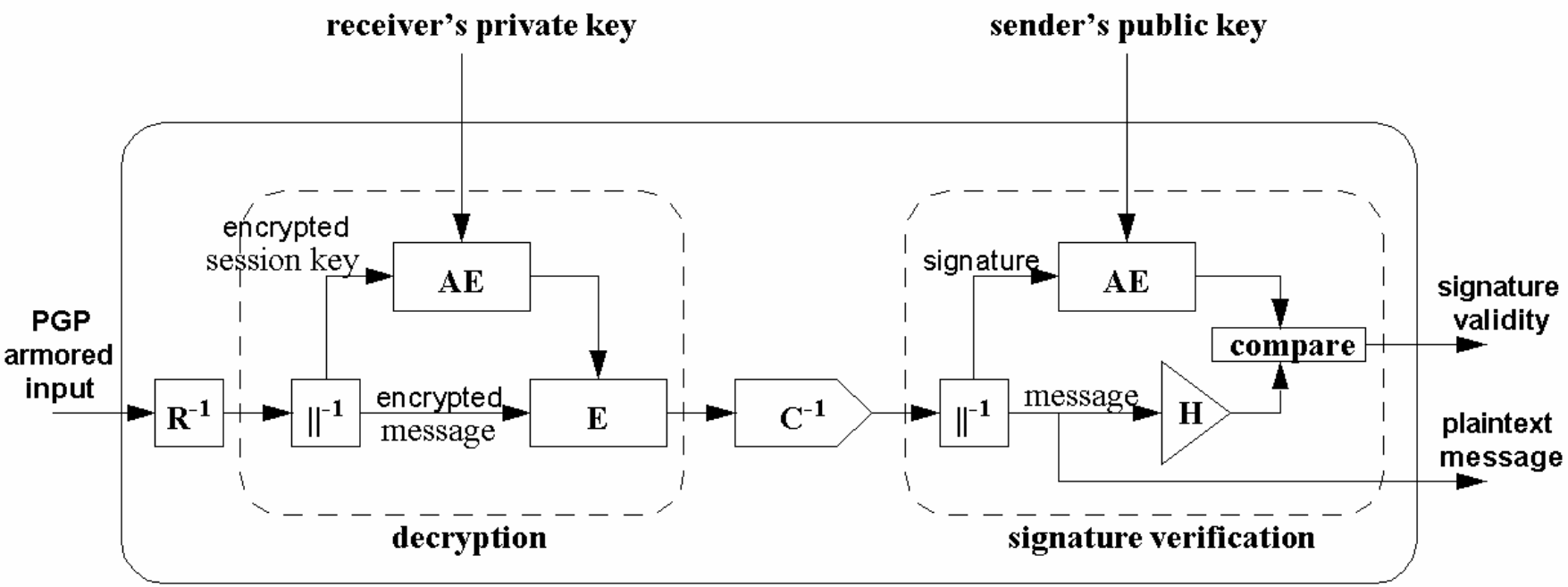
TEKNILLINEN KORKEAKOULU

# PGP-viestin lähettäminen



TEKNILLINEN KORKEAKOULU

# PGP-viestin vastaanottaminen



# Varmenteet

- PGP ei ratkaise julkisen avaimen oikeellisuudesta varmistumisen ongelmaa kunnolla
- Eräs keino on saada luotettu osapuoli allekirjoittamaan julkisia avaimia
  - Allekirjoitettu dokumentti, jossa julkinen avain liitetään esim. henkilöllisyyteen on nimeltään *varmenne*
  - Jos varmenteen vastaanottajalla on allekirjoittajan julkinen avain, hän voi varmistua allekirjoituksen oikeellisuudesta
  - PGP:kin tukee julkisten avainten allekirjoittamista, mutta ei käytä varmennerakennetta
- Varmenteiden heikko kohta on tuo luotettu kolmas osapuoli
- Varmenteita käytetään mm. WWW-palvelimien *autentikoimiseen*

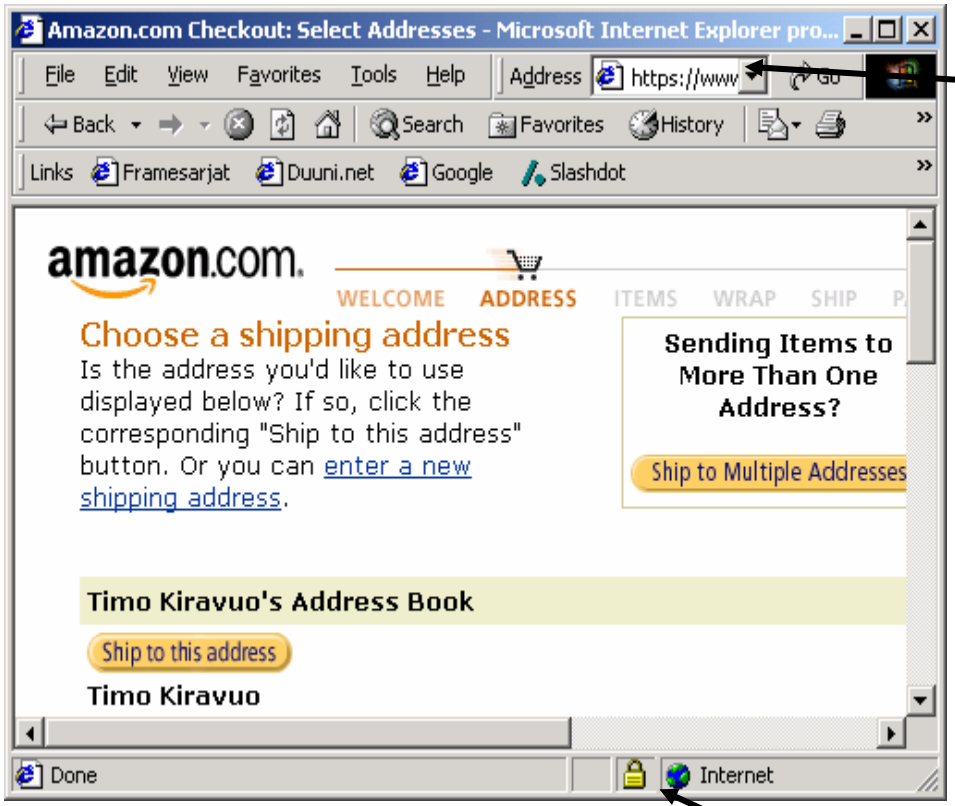
TEKNILLINEN KORKEAKOULU

# SSL ja WWW:n salaus

- WWW:n HTTP-liikenne voidaan salata SSL-protokollalla
  - Secure Socket Layer
  - Salaa liikenteen selaimen ja palvelimen välillä
  - SSL:ää voidaan käyttää minkä tahansa TCP-pohjaisen protokollan salaamiseen
- WWW-palvelin voidaan tunnistaa SSL-varmenteen avulla
  - Käyttäjät on koulutettava tarkistamaan, että salaus on voimassa
- WWW:n salauksesta varmistuminen
  - Salaus on päällä, kun selaimen pieni lukon kuva on kiinni
  - Lisäksi kannattaa katsoa tiedot varmenteista
  - On olemassa hyökkäyksiä, joilla WWW-yhteys saadaan näyttämään salatulta vaikka se ei ole

TEKNILLINEN KORKEAKOULU

# Salattu WWW-yhteys

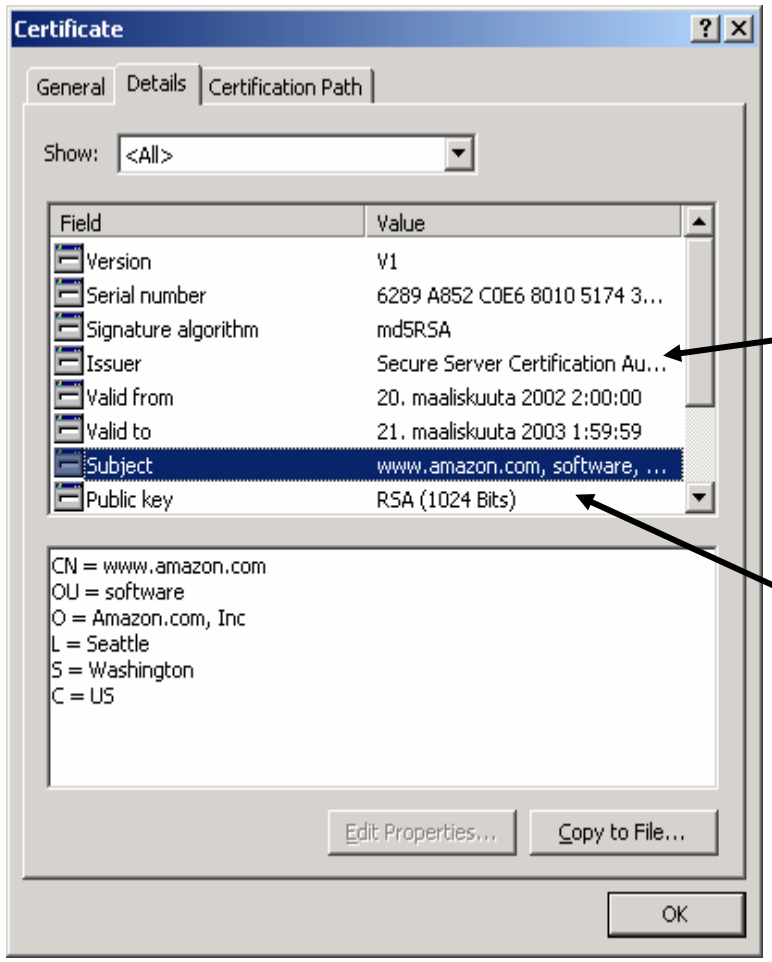



Osoite alkaa HTTPS-liitteellä

SSL-salaus on päällä

TEKNILLINEN KORKEAKOULU

# Selaimen varmenteen tiedot




Lukkoa näpäyttämällä saa varmenteen luettavaksi

Varmentaja

Varmenteen kohde

TEKNILLINEN KORKEAKOULU

# Tunnistaminen ja todentaminen

- Todentaminen on tunnistamisen varmistamista
  - Esim. varmenteen hallussapito ei itsessään todista henkilöllisyyttä
- Verkossa vastapuolen identiteetti voidaan selvittä esim. seuraavasti
  - Todennettava osapuoli esittää varmenteen
  - Todentajalla on varmenteen allekirjoittajan julkinen avain, jolla varmenteen allekirjoitus voidaan tarkistaa
  - Todentaja lähettää todennettavalle haasteen, ison satunnaisluvun
  - Todennettava osapuoli luo myös ison satunnaisluvun, kertoo haasteen sillä, salaa sen yksityisellä avaimellaan ja lähettää satunnaisluvun ja salatun haasteen todentajalle
    - Huomaa että todennettava ei allekirjoita lähettämäämme dataa sellaisenaan
  - Todentaja avaa haasteen salauksen todennettavan julkisella avaimella ja vertailee tulosta omaan satunnaislukunsa kerrottuna olion satunnaisluvulla

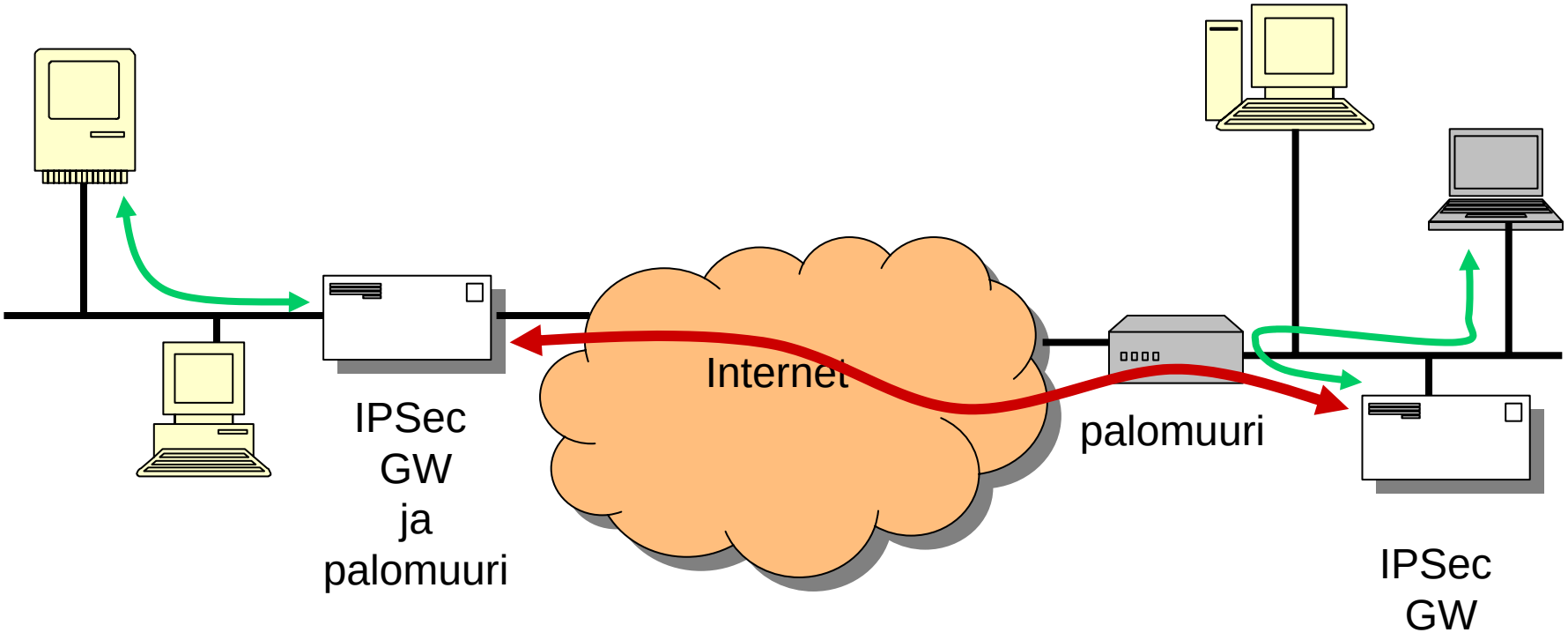
# Kaiken tietoliikenteen salaus

- PGP salaa sähköpostia ja SSL TCP-yhteyksiä
- Kaikki IP-pohjainen liikenne voidaan salata luomalla VPN-tunneli (Virtual Private Network)
  - IPsec on yleisin teknologia
    - Salaa jokaisen IP-paketin
- VPN-tekniikoita käytetään toimipisteiden yhdistämiseen ja etätyöhön

TEKNILLINEN KORKEAKOULU

# Virtual Private Networks (VPN)

- VPN-tekniikat kuten IPsec mahdollistavat lähiverkkojen yhdistämisen



TEKNILLINEN KORKEAKOULU

# Mitä salaustekniikat tarjoavat meille?

- Luottamuksellisuus
  - Salaus (data ei ole ulkopuolisten luettavissa)
  - Vastapuolen tunnistus (tiedetään kenelle tietoa annetaan)
- Eheys
  - Tiivisteet (datan muuttuminen havaitaan)
  - Pääsynhallinta ja tietolähteen tunnistaminen (tiedetään keneltä tietoa otetaan vastaan)
- Saatavuus
  - Salaustekniikat eivät tarjoa saatavuutta
- Kiistämättömyys
  - Allekirjoitukset

# Salauksen toteuttaminen

- Salaus on vaativa alue
  - Algoritmien suunnittelu ja niiden luotettavuudesta varmistuminen on vaativaa
  - Algoritmien ohjelmallinen toteuttaminen on helpompaa, mutta edelleen vaativaa
- Turvallisten ohjelmien toteuttaminen on jo itsessään vaativaa
  - Useimmat ohjelmat kestävät satunnaisia häiriöitä, turvaohjelmoinnissa oletetaan pätevä, motivoitunut hyökkääjä, jolla on täysi lähdekoodi käytettävissä

# Yhteenveto

- Salauksella voidaan ratkaista osa tietoturvan haasteista
  - Salauksella ei pystytä hallitsemaan ihmisten toimintaa
- Salauksen hyödyntäminen on kohtuullisen helppoa
  - On ymmärrettävä mitä salauksesta saadaan
- Salausalgoritmien suunnittelu ja ohjelmointi vaatii osaamista