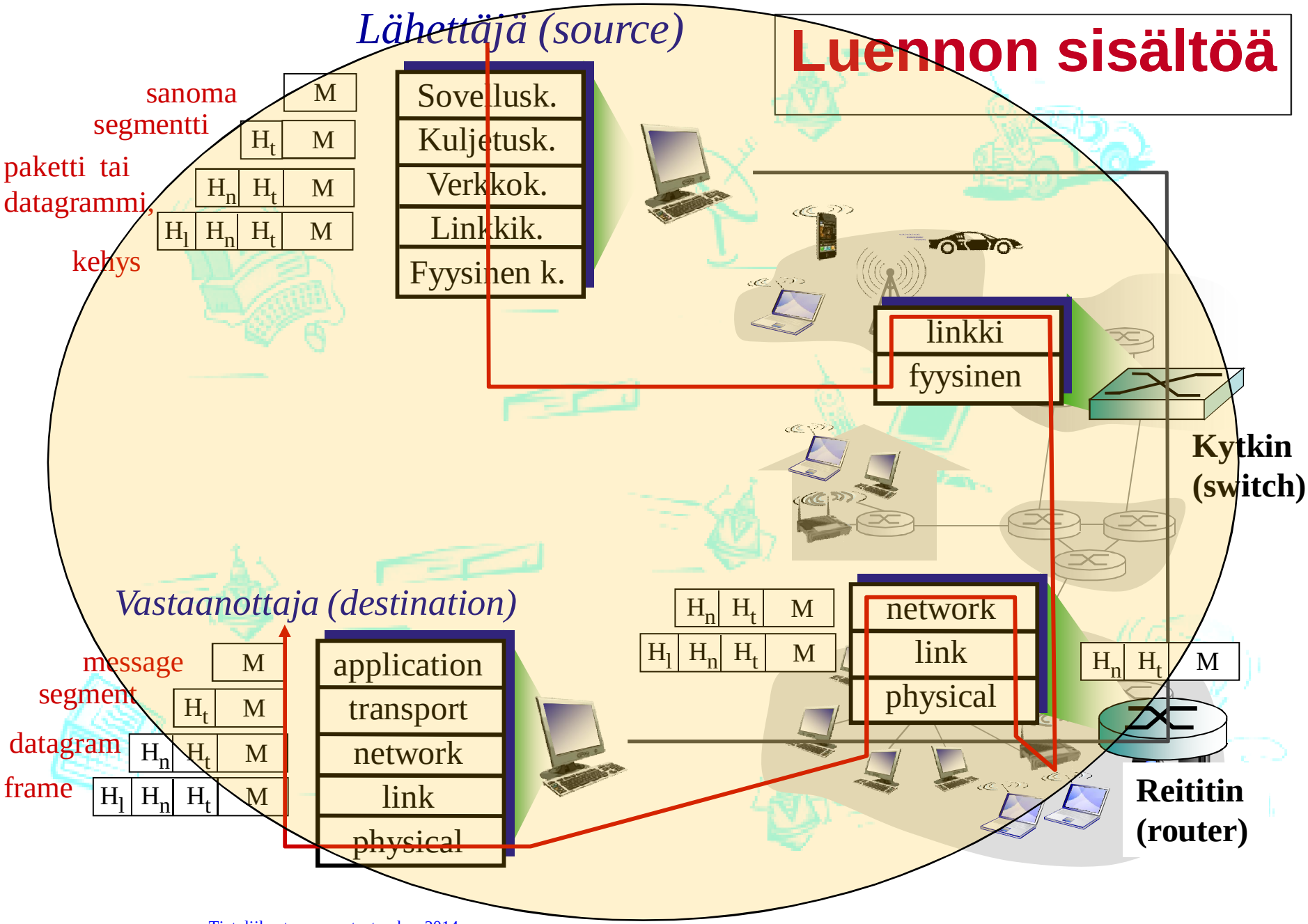
Tietoliikenteen perusteet

Luento 11: Tiedonsiirron turvallisuus: kryptografiaa ja salausavaimia

Syksy 2014, Tiina Niklander

Kurose&Ross: Ch 8

Luennon sisältöä



Sisältö

- **Ymmärtää tietoliikenteen turvallisuuden periaatteet:**
  - **Salaus (ja sen monet käyttötavat)**
  - **Todentaminen (authentication)**
  - **Viestien aitous ja eheys**
- **Tietoturva käytännössä:**
  - **Palomuurit ja tunkeutumisen-havaitsemisjärjestelmät**
  - **Turvallisuus eri kerroksilla**

Oppimistavoitteet:
- Ymmärtää ja osaa selittää käsitteet ja niiden merkitykset
- Osaa kuvata turvallisen protokollan periaatteita

VERKON TIETOTURVA

Verkon tietoturvan käsitteitä

http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf

Luottamuksellisuus (confidentiality): vain lähettäjä ja oikea vastaanottaja “ymmärtävät” viestin sisällön

- Lähettäjä salaa (encrypt) viestin
- Vastaanottaja purkaa (decrypt) viestin

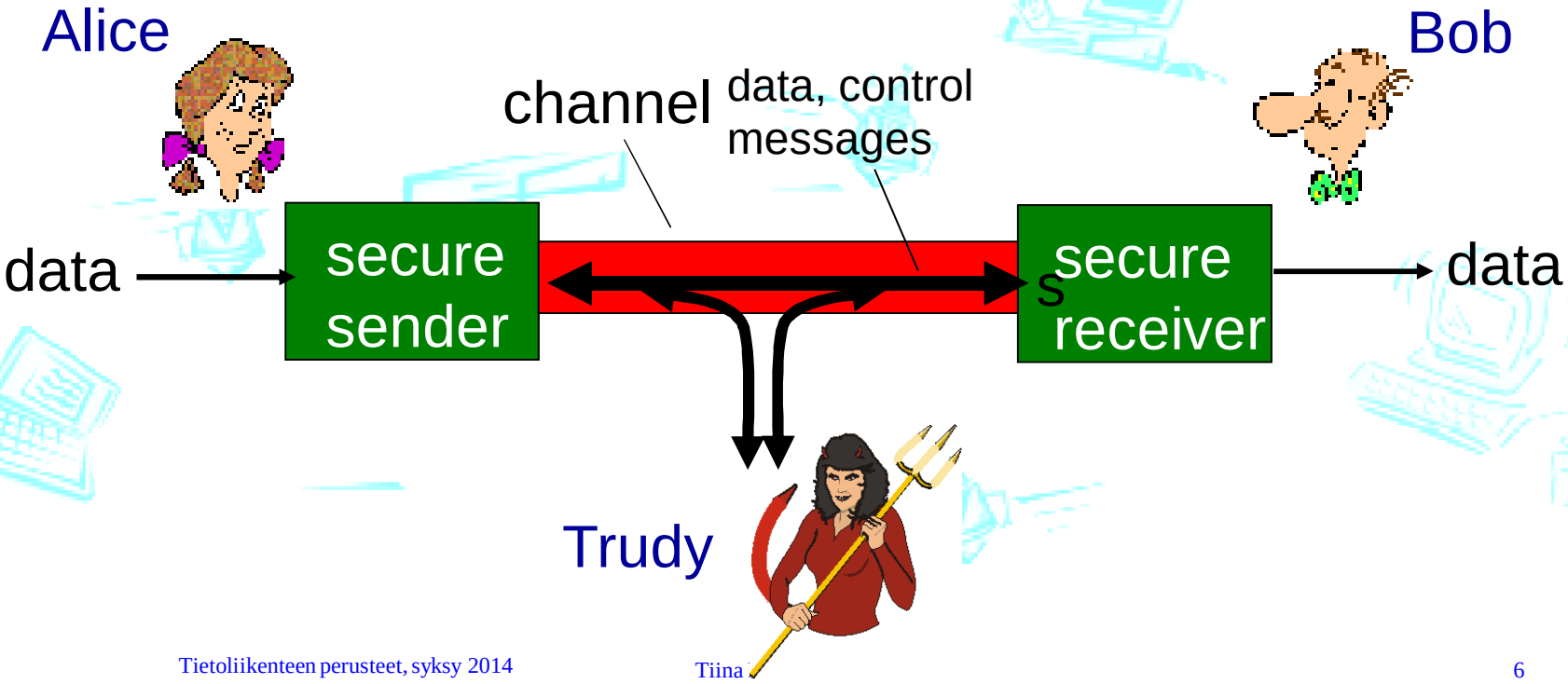
Todentaminen (authentication), tunnistus (identification): lähettäjä ja vastaanottaja haluavat varmistua vastapuol.

Eheys (integrity): lähettäjä ja vastaanottaja haluavat varmistaa, että viestiä ei ole muutettu (siirron aikana, jälkeenpäin) ilman, että se havaitaan.

Pääsy (access) ja käytettävyys (availability): Palvelun pitää olla käytettävissä käyttäjille. Tähän kuuluu sekä käytettävyys (ent. saatavuus) että pääsynvalvonta

Ystäviä ja vihamiehiä: Alice, Bob, Trudy

- Tunnettu esimerkki tietoliikenteen turvallisuudesta!
- Bob ja Alice haluavat keskustella “turvallisesti”
- Trudy (tunkeilija) voi salakuunnella, tulla väliin, poistaa tai lisätä viestejä



Keitä/mitä Bob ja Alice ovat?

- … todellisia ihmisiä!
- www-selaimia ja –palvelimia: esim. verkkokauppa tai vastaavia elektronisia transaktioita.
- Verkkopankin asiakkaita ja palvelimia
- Nimipalvelimia (DNS servers) – luento 4
- Reitittimiä, jotka vaihtavat reititystaulutietojaan – luento 8
- ja vastaavia …

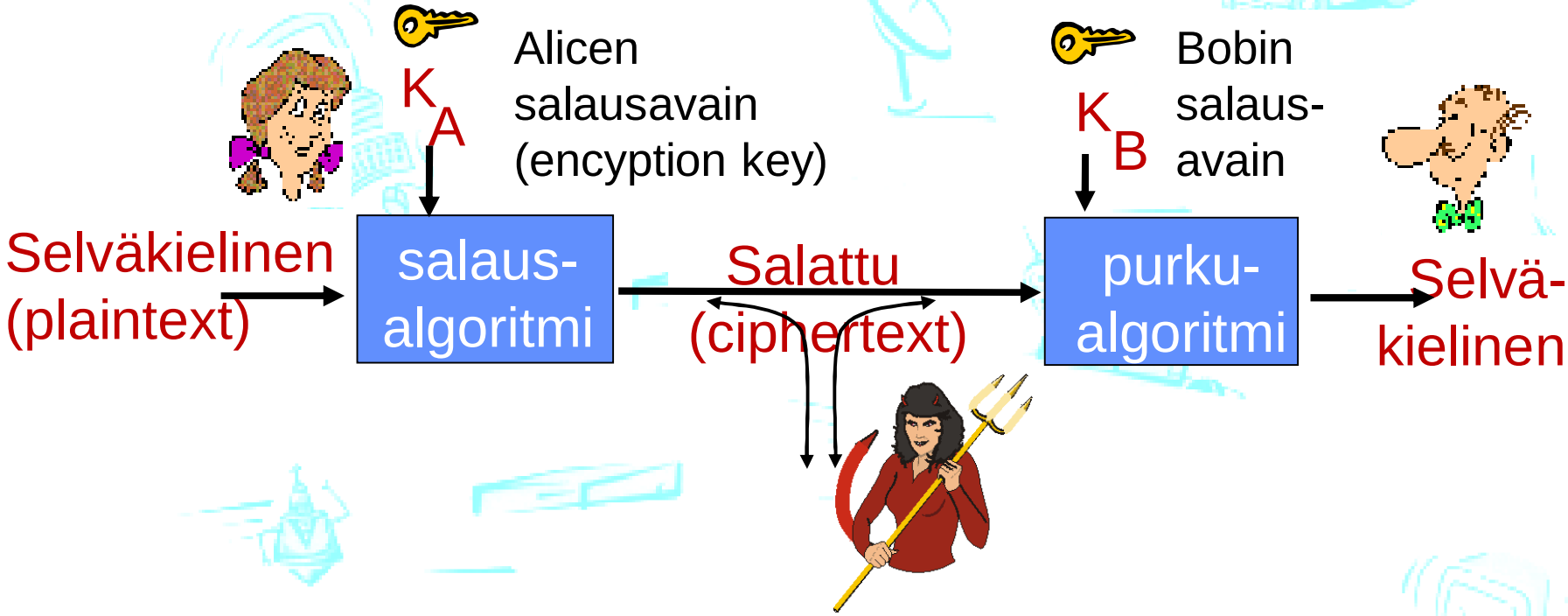
Transaktio (transaction) – tapahtumaketju tai toimenpidesarja,
Joka tehdään kokonaan tai ei ollenkaan. (Voi olla osatransaktioita)
Erityisesti pankkitoiminnot, tietokannat käyttävät käsitettä

Mitä Trudy puuhii?

- Koputtelee koneen portteja (mapping)
  - Turva-aukkojen löytämiseksi ja koneen valtaamiseksi
- Salakuuntelee (eavesdropping, sniffing)
  - Sieppaa sanoman matkalla ja tutkii sisällön
- Väärentää, “peukaloi”, “tekeytyy” (impersonation, spoofing)
  - Vaihtaa paketin tietoja, esim. IP-osoitteen
  - Tekeytyy toiseksi osapuoleksi
- Tehtailee sanomia, “satuilee” (fabrication)
  - Tekee ja lisää liikenteeseen ylimääräisiä sanomia
- Kaappaa yhteyden (hijacking)
  - Vaihtaa oman IP-osoitteen lähettäjän / vastaanottajan tilalle
- Estää palvelun (DoS, Denial of Service)
  - Kuormittaa palvelinta, jotta se ei ehdi palvella oikeita käyttäjiä

VÄHÄN KRYPTOGRAFIAA

Kryptografian merkintätapa (~ kieli)



m selväkielinen viesti

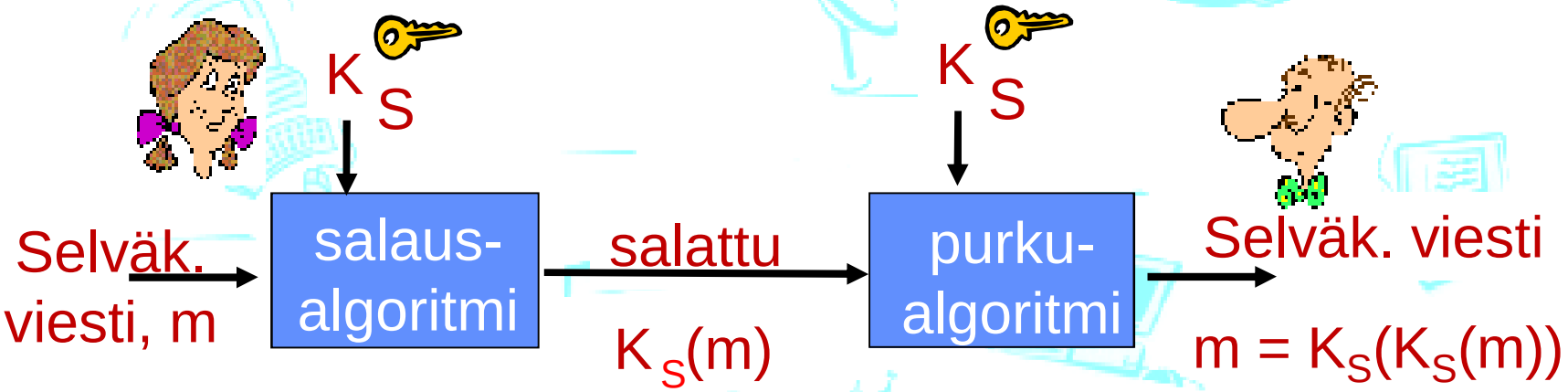
$K_A(m)$ salattu viesti, salattu avaimella K_A

$m = K_B(K_A(m))$ salatun viestin purku avaimella K_B

Salauksen murtaminen (break)

- Vain salattu viesti (cipher-text only)
  - Trudyllä on vain salattu viesti, jota hän voi tutkia
  - Kaksi vaihtoehtoa:
    - Raaka voima (brute force): kokeile kaikki mahdolliset avaimet
    - Tilastollinen analyysi (statistical analysis)
- Tunnettu selväkielinen teksti (known-plaintext)
  - Trudyllä on salatun viestin lisäksi sisältöä vastaavaa selväkielistä tekstiä
  - esim, kirjainten vaihtoon perustuvassa salauksessa Trudy voi päätellä kirjaimet, a,l,i,c,e,b,o
- Valittu selväkielinen (chosen-plaintext): Trudy voi saada haluamaansa selväkielistä vastaavan salatun (esim. huijaamalla Alicea)

Symmetrisen avaimen salakirjoitus



Symmetrisen avaimen salaus (symmetric key crypto): Bob ja Alice jakavat saman (symmetrisen) avaimen: K_S

- Esim. Avain on kirjaintenvaihtotaulukko (mono alphabetic substitution cipher)

Q: Miten Alice ja Bob sopivat avaimesta?

Yksinkertainen salaus: kirjainvaihto

Vaihtosalaaja (substitution cipher): Vaihda jokin asia toiseksi

- monoalphabetic cipher: Vaihda kirjain toiseen kirjaimeen

```
Selväk.:  abcdefghijklmnopqrstuvwxyz

Salattu:  mnbvcxzasdfghjklpoiuytrewq
```

e.g.:

```
Selväk.: bob. i love you. alice
salattu: nkn. s gktc wky. mgsbc
```

Salausavain (Encryption key): Kuvaus kirjainjoukosta toiseen kirjainjoukkoon

Hiukan kehittyneempi salaus

- n kpl vaihtosalauksia: $M_1, M_2, \ldots, M_n$
- Jaksollinen käyttömalli (cycling pattern):
  - e.g., n=4: M_1, M_3, M_4, M_3, M_2; M_1, M_3, M_4, M_3, M_2; ..
- Käytä aina seuravalle symbolille, seuraavaa vaihtosalausta
  - dog: d from M_1, o from M_3, g from M_4

Salausavain: n vaihtosalaaja, ja jaksollinen käyttömalli

- Avaimen ei tarvitse olla vain n-bittinen.

Symmetrisen avaimen salaus: DES

DES: Data Encryption Standard

- US encryption standard [NIST 1993]
- 56-bittinen salausavain, 64-bittinen selväk. viesti
- Lohkosalaus (block cipher) ja lohkojen ketjutus
- DESin turvallisuus?
  - DES Challenge III, 1999: 56-bittisellä avaimella salattu viesti purettiin 22 tunnissa (brute force –menetelmällä)
  - Ei tunneta hyviä analyyttisiä menetelmiä
- DESistä turvallisempi:
  - 3DES: salaa 3 kertaa käyttäen 3:a eri avainta
- Uudempia ja parempia vaihtoehtoja on olemassa, AES

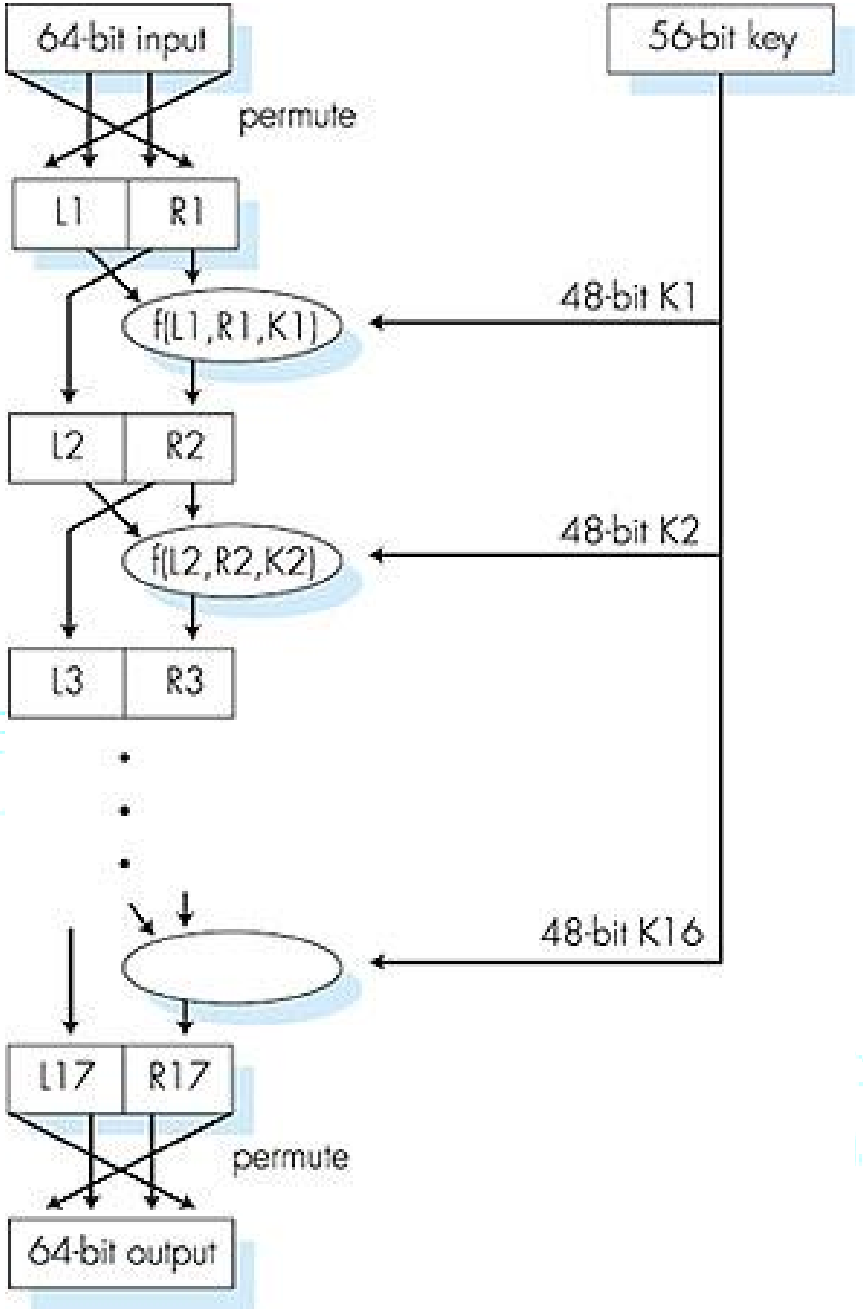
DES
lohkon salaus

DES operation

initial permutation

16 identical “rounds” of function application, each using different 48 bits of key

final permutation



Lohkojen ketjutus
Cipher Block Chaining (CBC)

- Aloituslohko (lohko c(0)) - satunnaisvektori, joka lähetetään selväkielisenä
- Kullekin datalohkolle M(i)
  - Laske XOR (M(i), C(i-1)) ja sitten salaa yhdistetty lohko

$$C(i) = K_S(m(i) \oplus c(i-1))$$

- Täydennä tarvittaessa viimeinen lohko satunnaisella sisällöllä

AES: Advanced Encryption Standard

- Symmetrisen avaimen salaus, korvasi DESin (2001)
- NIST standardi
  - National Institute of Standards and Technology
- Käsittelee dataa 128 bitin lohkoina
- Avaimen pituus: 128, 192, tai 256 bittiä
- NIST 2001 väitti, että jos DES salauksen purku raakaa voimaan käyttäen vie 1s, veisi AESin purku 149 biljoonaa vuotta (engl. 149 trillion years)

Julkisen avaimen salaus
Public Key Cryptography

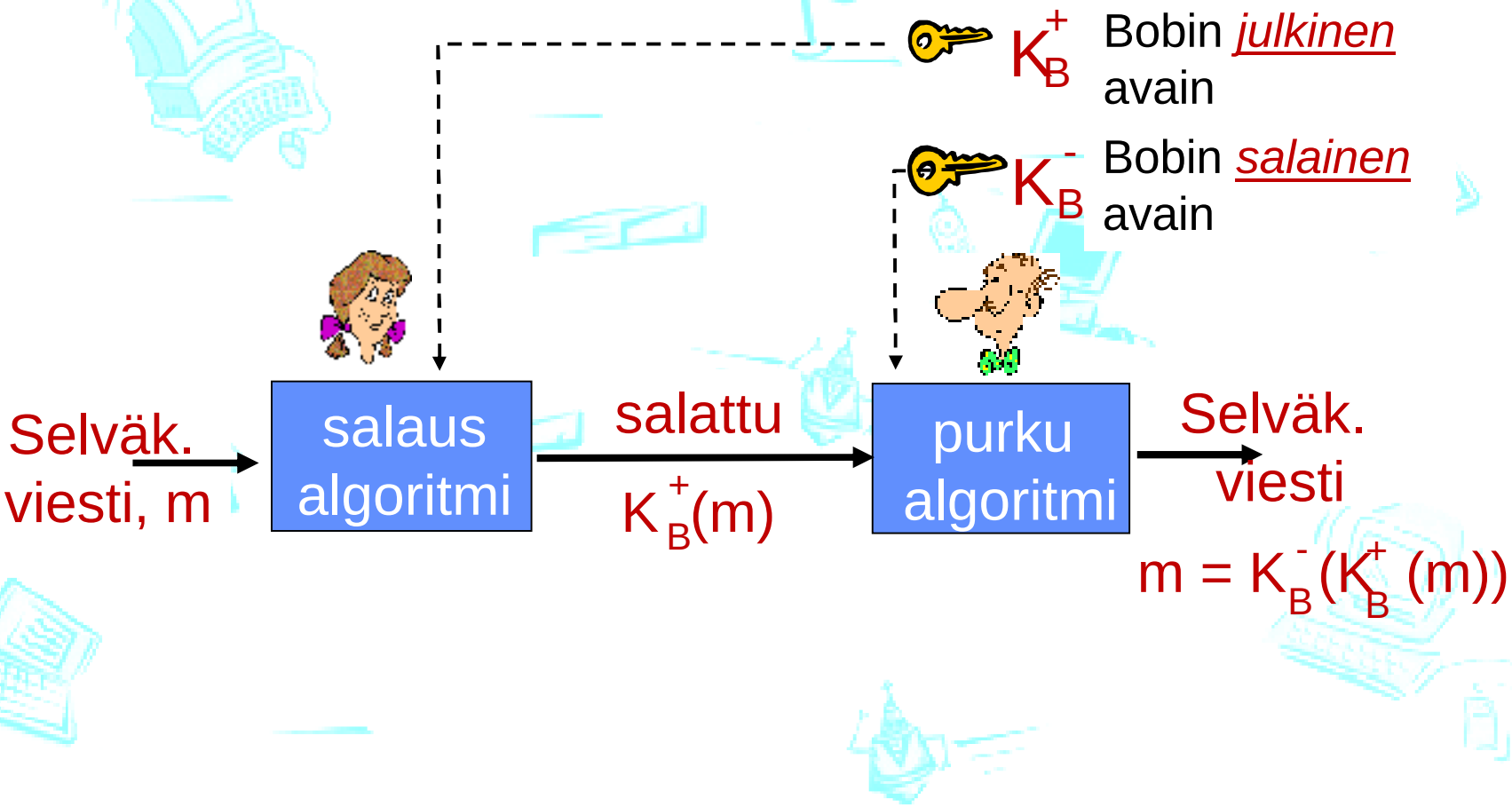
Symmetrinen avain

- Lähettäjän ja vastaanottajan tunnettava salainen symmetrinen avain
- Q: Kuinka avaimesta sovitaan viestinnän alussa (varsinkin, jos ei koskaa “tavata”) ?

Julkinen avain

- Erilainen idea [Diffie-Hellman76, RSA78]
- **Ei jaettua** salaista avainta
- *Julkinen (public)* salaus-avain **kaikkien** tiedossa
- *Salainen, yksityinen (private)* salausavain vain vastaanottajan tiedossa

Julkisen avaimen salaus



Julkisen avaimen salausalgoritmi

vaatimuksia:

1. tarvitaan $K_B^+( )$ ja $K_B^-( )$ siten, että

$$K_B^-(K_B^+(m)) = m$$

2. Julkisesta avaimesta K_B^+ ei pidä voida päätellä salaista avainta K_B^-

RSA: Rivest, Shamir, Adleman algoritmi

Esitietoa: moduloaritmetiikka

- x mod n = jakojäännös, kun x jaetaan n:llä
- peruskaavoja:

  $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

  $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$

  $[(a \bmod n) * (b \bmod n)] \bmod n = (a*b) \bmod n$
- joten

  $(a \bmod n)^d \bmod n = a^d \bmod n$
- lasketaan : x=14, n=10, d=2:

  $(x \bmod n)^d \bmod n = 4^2 \bmod 10 = 6$

  $x^d = 14^2 = 196 \quad x^d \bmod 10 = 6$

RSA: taustaideaa

- viesti: vain jono bittejä, bittijono
- Kukin bittijono voidaan kuvata yhdellä kokonaisluvulla
- Näin ollen viestin salaus on ekvivalentti kokonaisluvun salaukselle.

esimerkki:

- m= 10010001 . Tätä viestiä vastaa kokonaisluku 145.
- Viestin m salaamiseksi, salataan vastaava kokonaisluku ja näin saadaan uusi numero (eli salattu viesti) .

RSA: Julkinen/salainen avainpari

1. Valitse kaksi suurta alkulukua *p, q.* (e.g., 1024 bits each)
2. Laske $n = pq$, $z = (p-1)(q-1)$
3. Valitse e $(e<n)$ s.e. ei yhteisiä jakajia luvun z kanssa (*e, z* ovat “keskenään alkulukuja”).
4. Valitse d s.e. $ed-1$ on tasan jaollinen *z:lla*. (toisin sanoen: $ed \bmod z = 1$).
5. *Julkinen* avain on $\underbrace{(n,e)}_{K_B^+}$. *Salainen* avain $\underbrace{(n,d)}_{K_B^-}$.

RSA: salaus ja purku

0. Avaimet (n,e) ja (n,d) laskettu kuten edellä

1. Sanoman m ($<n$) salaus: laske

   $c = m^e \bmod n$

2. Vastaanotetun sanoman c purku: laske

   $m = c^d \bmod n$

magic happens!

$$m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$$

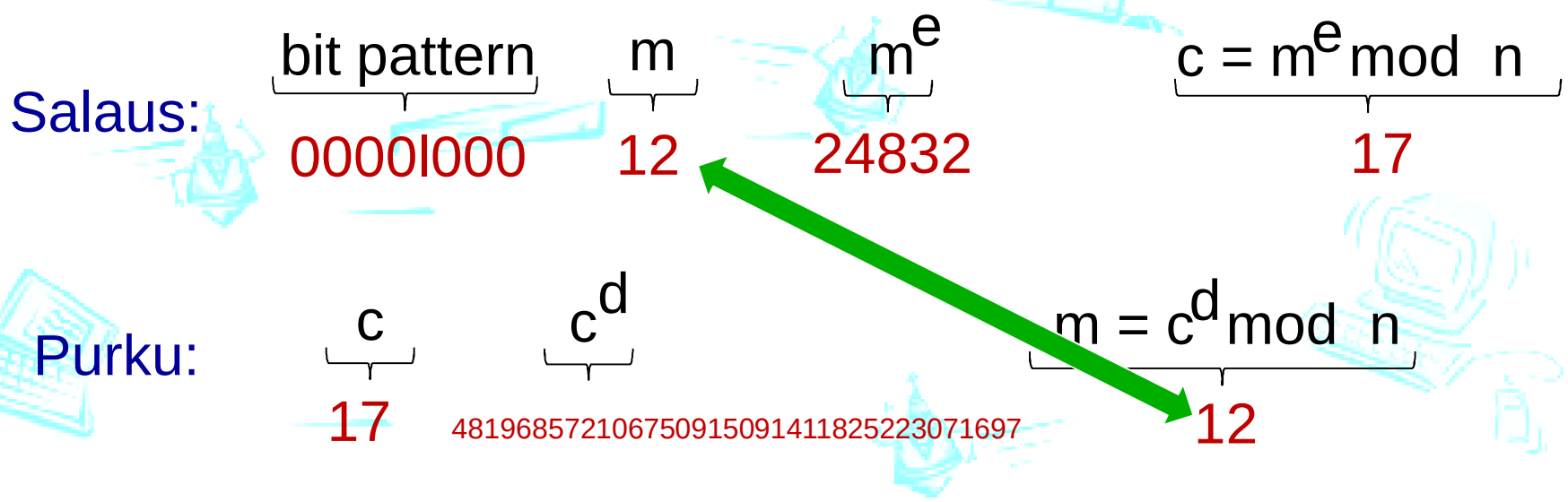
RSA esimerkki:

Bob valitsee *p=5, q=7*. Silloin *n=35, z=24*.

e=5 (*e ja z* ei yhteisiä jakajia).

d=29 (*ed-1* tasan jaollinen z:lla).

Alice salaa 8-bittisen viestin



Miksi RSA toimii?

- Täytyy osoittaa, että $c^d \bmod n = m$ kun $c = m^e \bmod n$
- tiedetään: Kaikille x ja y: $x^y \bmod n = x^{(y \bmod z)} \bmod n$
  - kun n= pq ja z = (p-1)(q-1)
- siten,

$$c^d \bmod n = (m^e \bmod n)^d \bmod n$$
$$= m^{ed} \bmod n$$
$$= m^{(ed \bmod z)} \bmod n$$
$$= m^1 \bmod n$$
$$= m$$

RSA: toinen tärkeä piirre!

Avainten vaihdettavuus on
erittäin hyödyllinen ominaisuus

$$K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$$

Ensin julkinen avain ja sitten salainen avain

Ensin salainen avain ja sitten julkinen avain

Lopputulos on sama!

Miksi $K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$?

Perustuu puhtaasti moduloaritmetiikkaan:

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$
$$= m^{de} \bmod n$$
$$= (m^d \bmod n)^e \bmod n$$

Miksi RSA on turvallinen?

- Oletetaan, että tiedät Bobin julkisen avaimen (n,e). Kuinka vaikeaa on selvittää d?
- Periaatteessa tarvitaan vain tekijöihinjako. Täytyy löytää luvun n tekijät p ja q, kun emme tiedä niitä.
  - Tekijöihin jako on laskennallisesti vaativa ongelma, kun selvitettävänä on suuri numero.

Wikipedia: Kokonaislukujen tekijöihinjako

RSA käytännössä: istuntoavaimet

- RSAn käyttämä potenssiin korottaminen on laskennallisesti haastavaa
- DES on ainakin 100 kertaa nopeampi kuin RSA
- Siispä: Käytetään julkisen avaimen salausta suojatun yhteyden muodostamiseen, sitten käytetään toista, erillistä – symmetristä istuntoavainta – salaukseen suojatun yhteyden aikana

Istuntoavain (session key), K_S

- Bob ja Alice käyttävät RSA:ta symmetrisestä avaimesta K_S sopimiseen
- Kun molemmilla on K_S, käytetään sitä salaamiseen

KÄYTTÄJÄN TODENTAMINEN (AUTENTIKOINTI)

Todentaminen (authentication)

Tavoite: Bob haluaa, että Alice todentaa henkilöllisyytensä

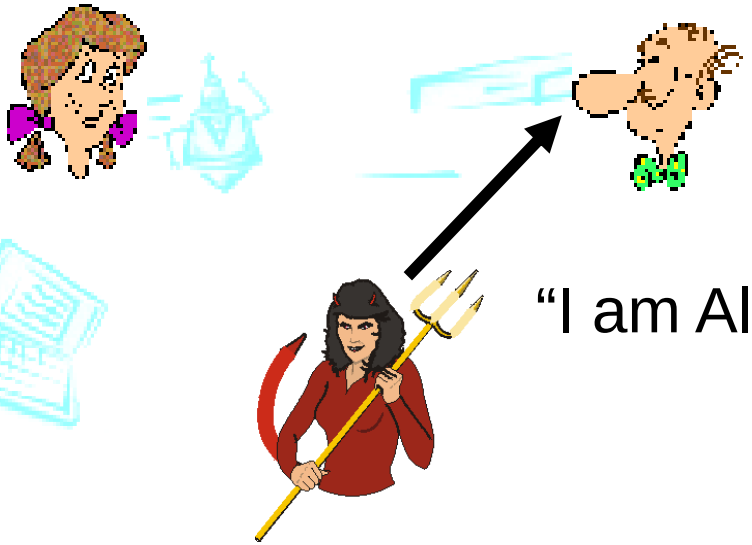
Protokolla ap1.0: Alice väittää “I am Alice”

Virhetilanteita/ epäonnistumisia??

Todentaminen (authentication)

Tavoite: Bob haluaa, että Alice todentaa henkilöllisyytensä

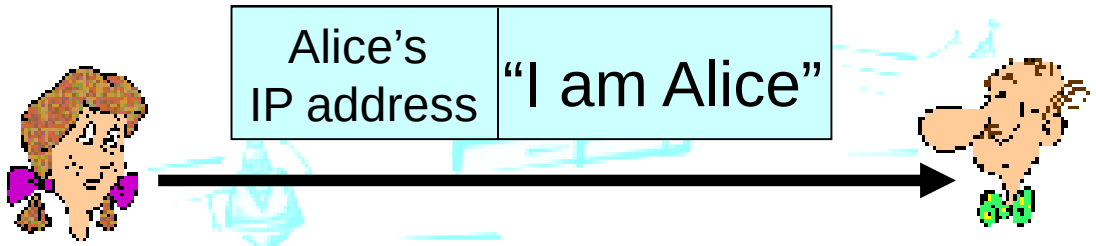
Protokolla ap1.0: Alice väittää “I am Alice”



Verkossa Bob ei voi “nähdä” Alicea, joten Trudy voi vain väittää “I am Alice”

Todentaminen: Uusi yritys

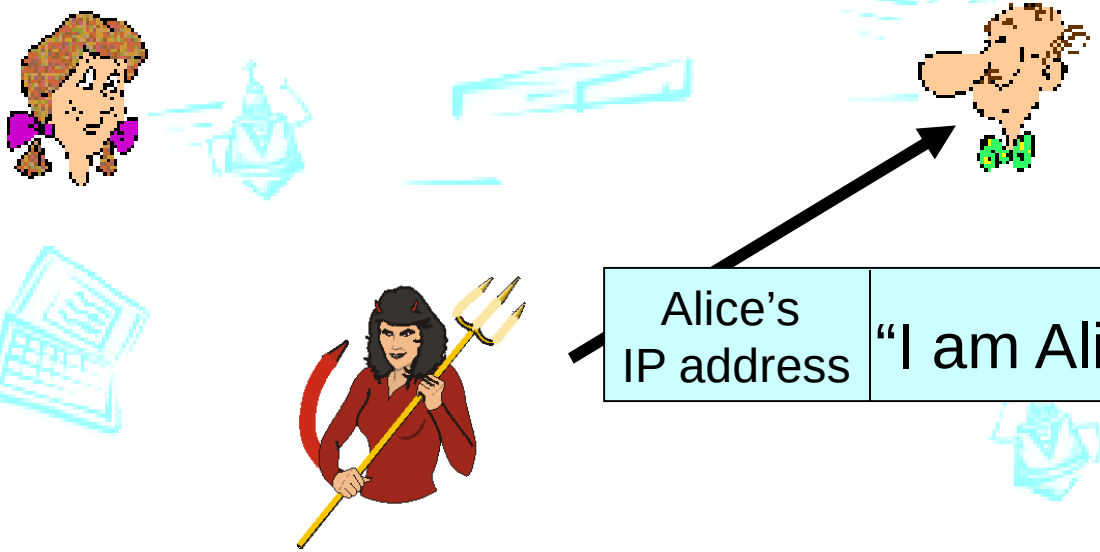
Protokolla ap2.0: Alice väittää “I am Alice” IP-paketissa, jossa mukana lähettävän koneen (=Alice) IP.



Virhetilanteita/
epäonnistumisia??

Todentaminen: Uusi yritys

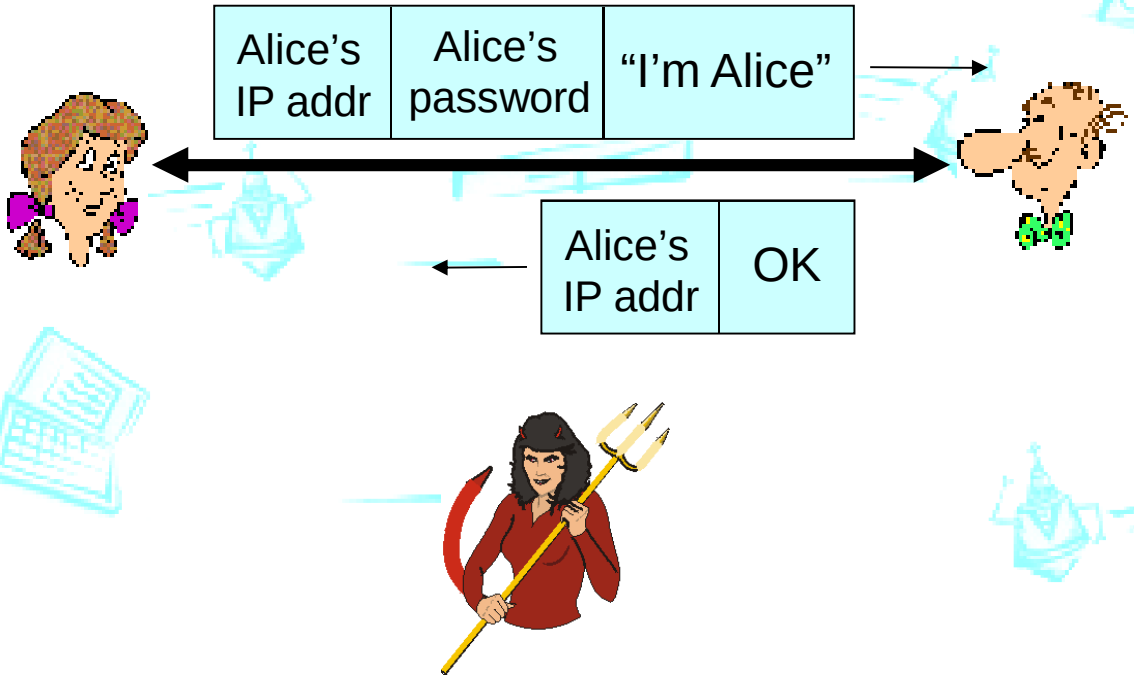
Protokolla ap2.0: Alice väittää “I am Alice” IP-paketissa, jossa mukana lähettävän koneen (=Alice) IP.



Trudy luo IP-paketin, jossa väärennetty lähettäjän osoite (IP spoofing)

Todentaminen: kolmas yritys

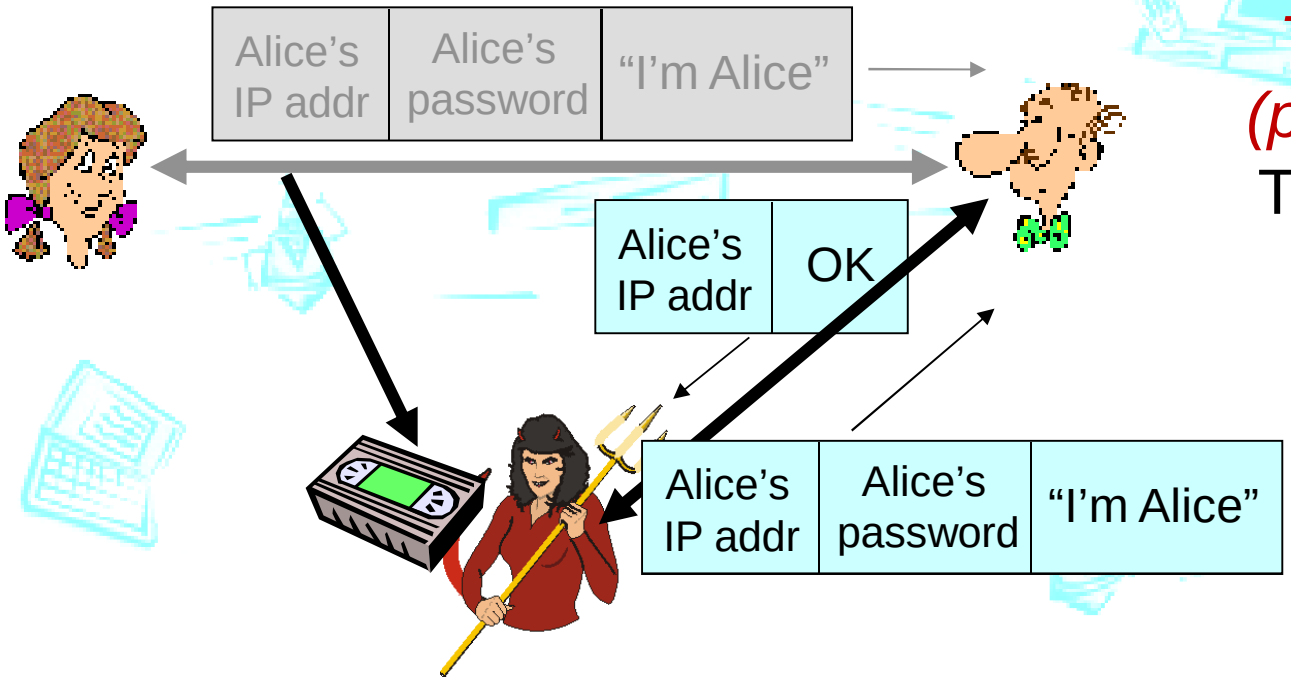
Protokolla ap3.0: Alice väittää “I am Alice” ja lähettää salaisen salasanansa todentaakseen sen.



Virhetilanteita/ epäonnistumisia??

Todentaminen: kolmas yritys

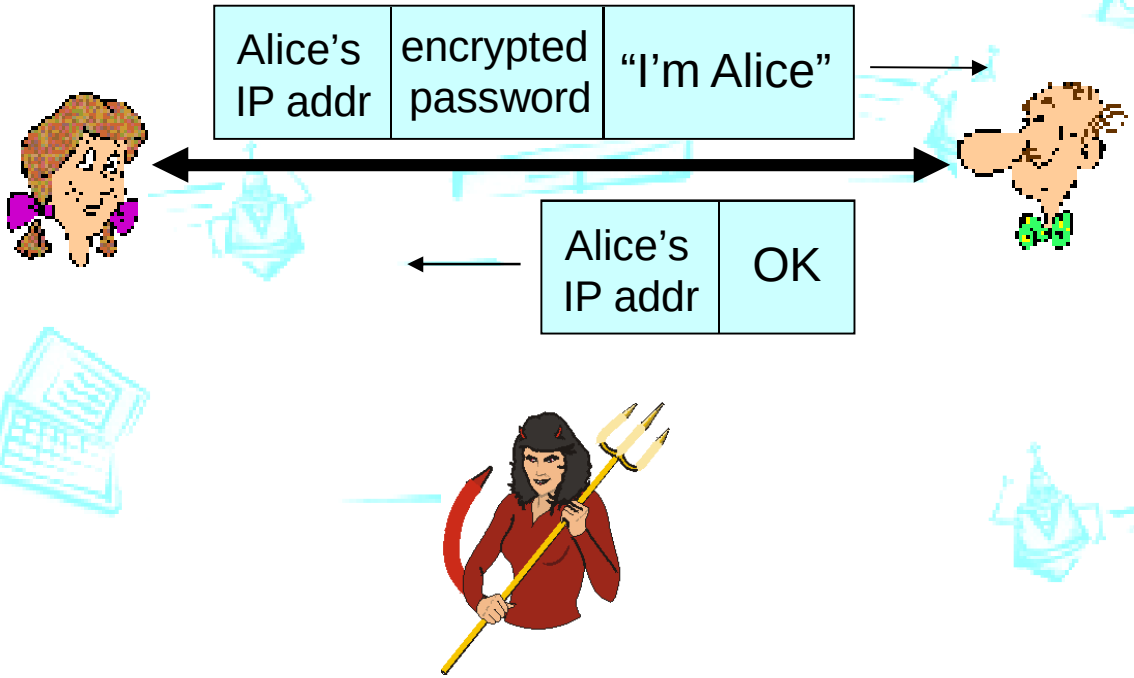
Protokolla ap3.0: Alice väittää “I am Alice” ja lähettää salaisen salasanansa todentaakseen sen.



Toistohyökkäys (playback attack): Trudy nauhoittaa Alicen viestit ja toistaa ne Bobille

Todentaminen: yritys 3.1

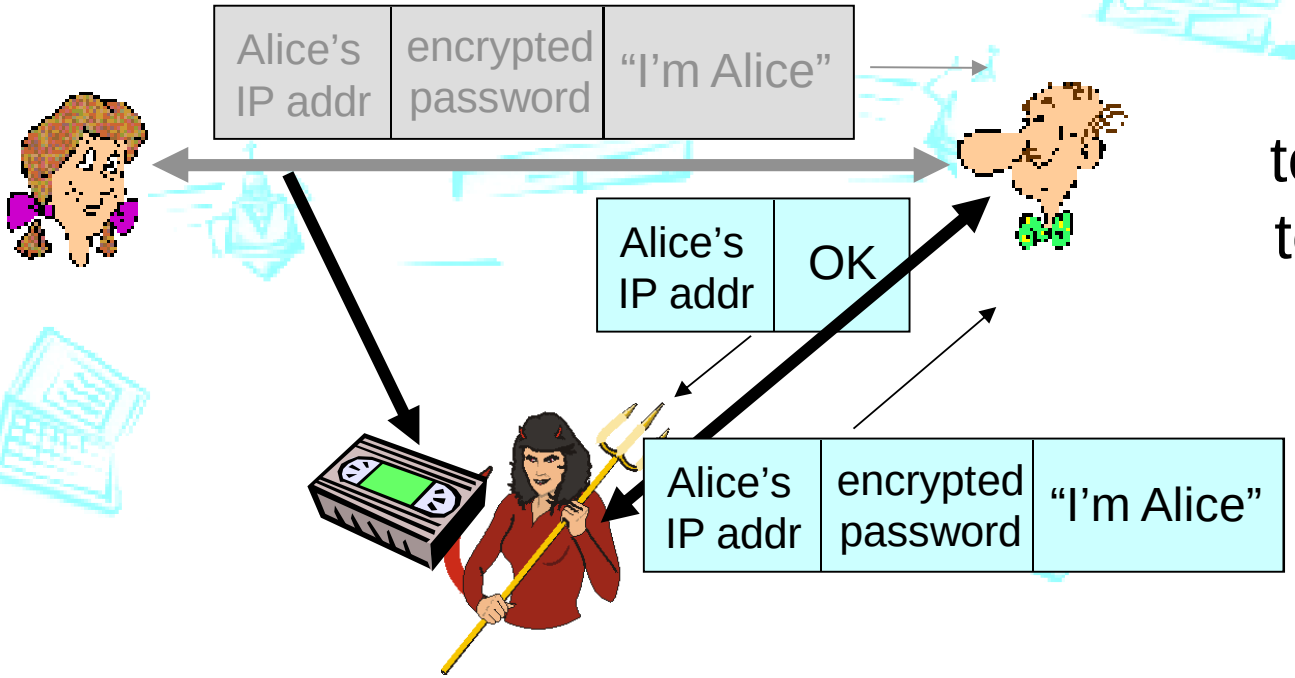
Protokolla ap3.1: Alice väittää “I am Alice” ja lähettää *salatun* salasanansa todentaakseen sen.



Virhetilanteita/ epäonnistumisia??

Todentaminen: yritys 3.1

Protokolla ap3.1: Alice väittää “I am Alice” ja lähettää *salatun* salasanansa todentaakseen sen.



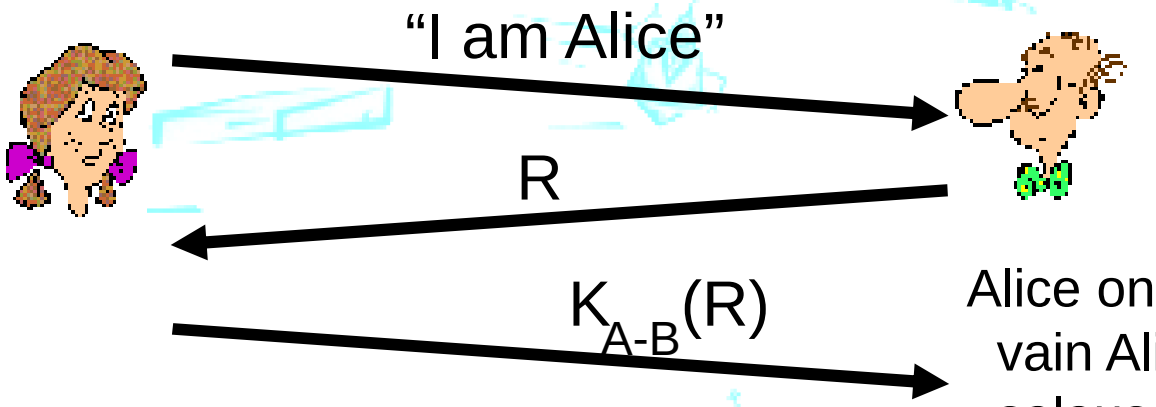
Nauhoitus ja toistohyökkäys toimii *edelleen*!

Todentaminen: neljäs yritys

Tavoite: Estetään toistohyökkäys

Haaste (nonce): numero (R) vain kerran, *ei saa esiintyä uudelleen*

ap4.0: varmistaakseen Alicen olemassaolon, Bob lähettää *haasteen (nonce)* R. Alice palauttaa R:n salattuna jaetulla salaisella avaimella



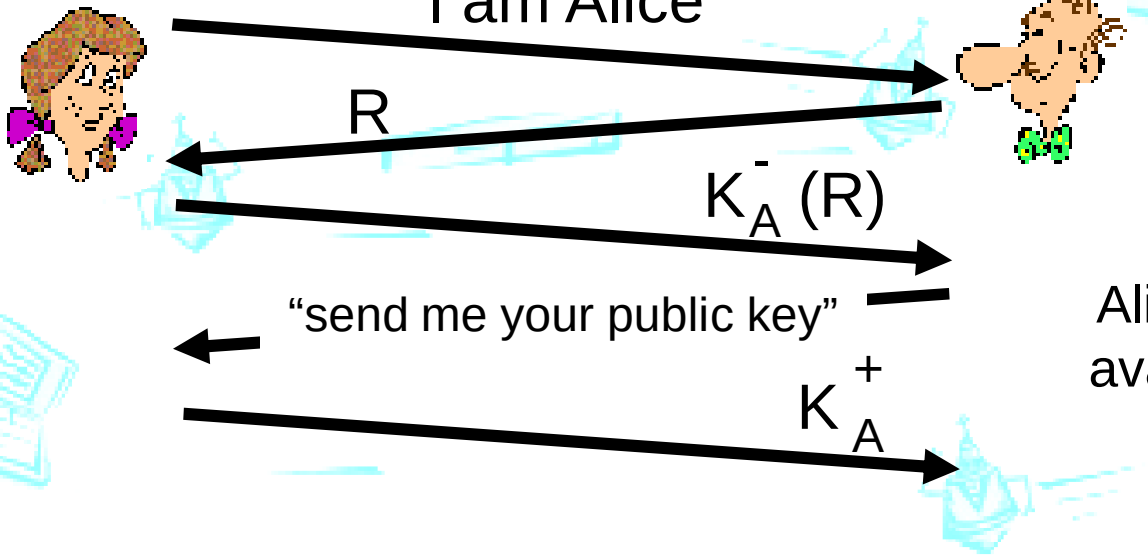
Virhetilanteita, ongelmia?

Todentaminen: ap5.0

ap4.0 käyttää jaettua salaista avainta

- Voisiko todentamisen tehdä julkisen avaimen avulla?

ap5.0: käyttää haastetta ja julkisen avaimen salausta



Bob laskee

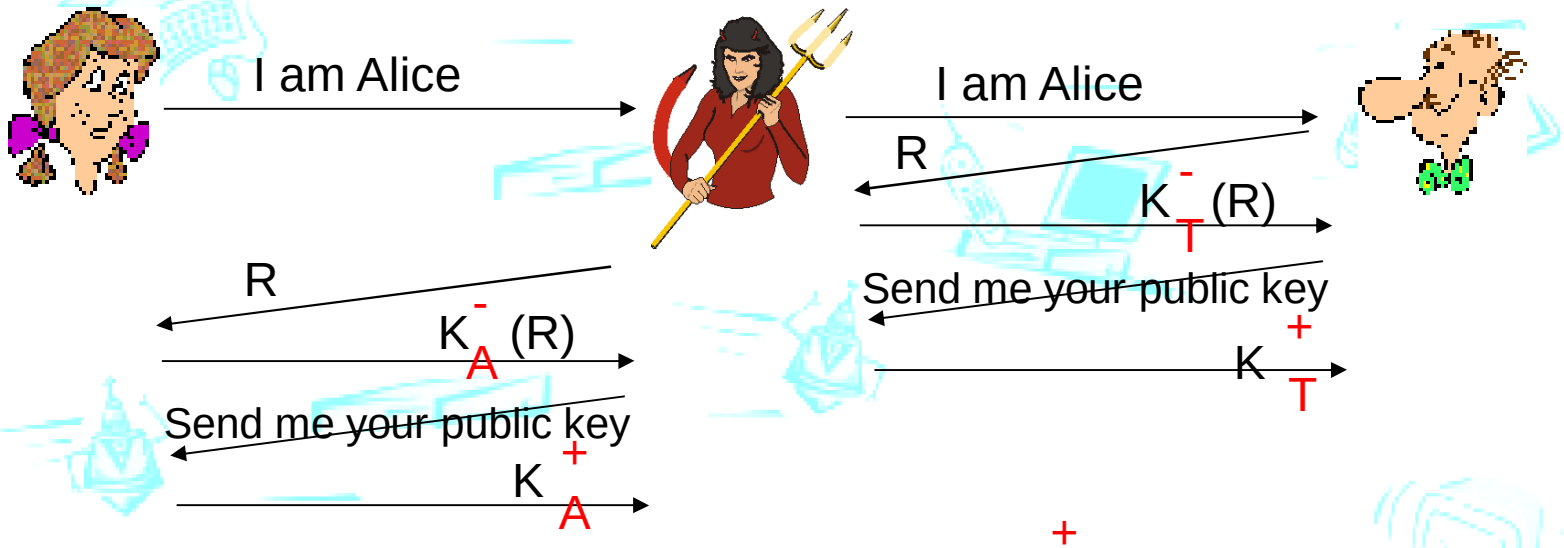
$K_A^+(K_A^-(R)) = R$

ja olettaa, että vain Alicella voi olla salainen avain, jolla R salattu s.e.

$K_A^+(K_A^-(R)) = R$

ap5.0: turvallisuusaukko

man (or woman) in the middle hyökkäys: Trudy tekeytyy Aliceksi (Bobille) ja Bobiksi (Alicelle)



Trudy saa $K_T^+(m)$

$m = K_T^-(K_T^+(m))$

ja lähettää m:n Alicelle salattuna Alicen julkisella avaimella

$K_A^+(m)$

$m = K_A^-(K_A^+(m))$

ap5.0: turvallisuusaukko

man (or woman) in the middle hyökkäys: Trudy tekeytyy Aliceksi (Bobille) ja Bobiksi (Alicelle)

Vaikea havaita:

- Bob vastaanottaa kaiken mitä Alice lähettää, ja päin vastoin. (Bob ja Alice voivat tavata myöhemmin ja palauttaa keskustelun mieleensä!)
- Ongelma on, että myös Trudy saa kaikki viestit!

Ratkaisu: varmenteet, mutta luotatko varmentajaan?

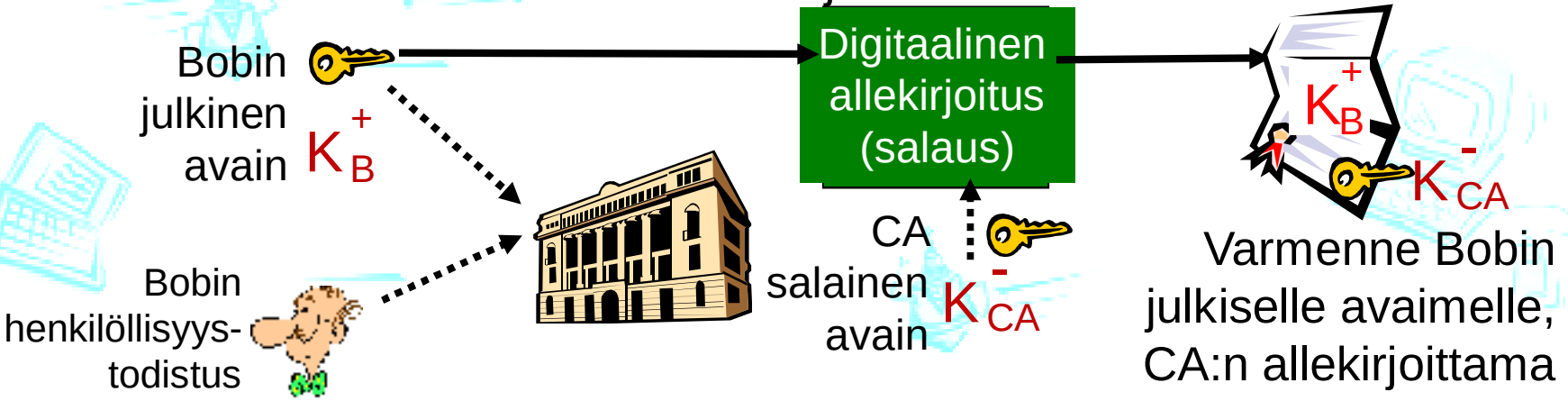
Hyökkäys: julkisen avaimen salaus

- Trudy ‘pilailee’ pizzatilauksella Bobin nimissä
  - Trudy tekee sähköposti tilauksen:
    Hyvä Pizzapalvelu, Toimittaisitteko minulle 4 pepperoni pizzaa. T. Bob
  - Trudy allekirjoittaa tilauksen omalla salaisella avaimellaan
  - Trudy lähettää tilauksen Pizzapalveluun
  - Trudy toimittaa Pizzapalveluun myös oman julkisen avaimensa, mutta väittää sitä Bobin julkiseksi avaimeksi
  - Pizzapalvelu varmentaa allekirjoituksen ja toimittaa 4 pepperonipizzaa Bobille
  - Bob ei syö pepperonipizzaa

Ongelma: Miten Pizzapalvelu voi varmistua julkisen avaimen ja henkilön yhteydestä?

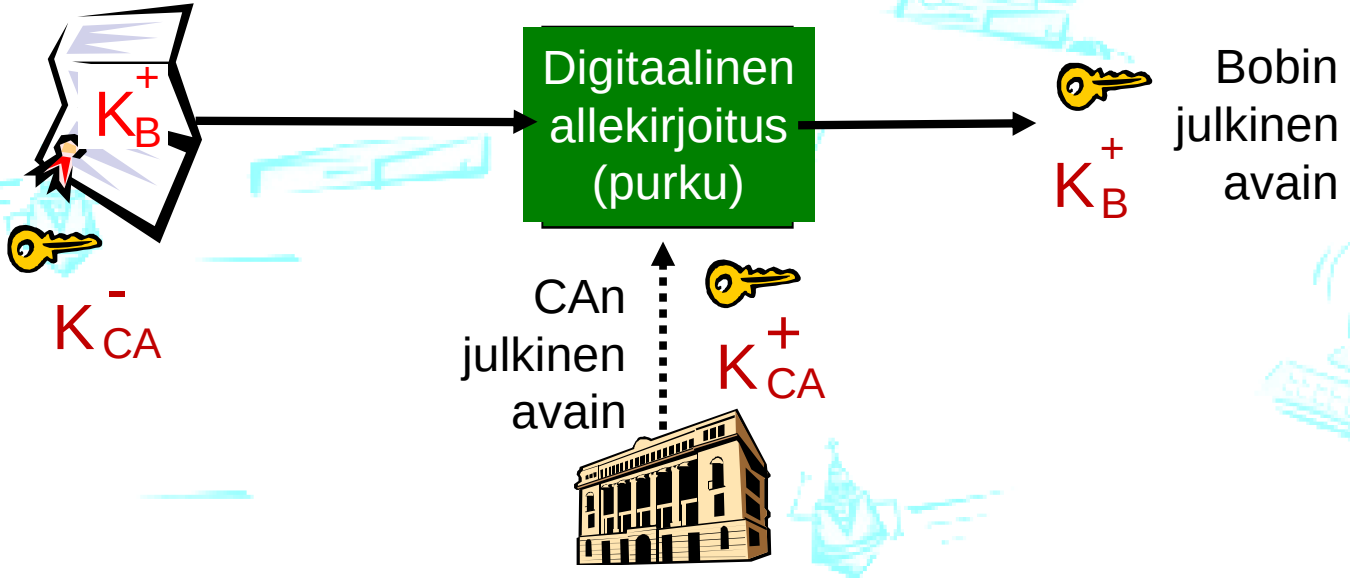
Varmennepalvelu

- *Varmentaja (certification authority, CA):* sitoo julkisen avaimen ja entiteetin, E, identiteetin toisiinsa.
- E (henkilö, reititin, palvelu) rekisteröi julkisen avaimensa varmentajalle CA.
  - E todistaa “henkilöllisyytensä” varmentajalle CA.
  - CA luo varmenteen (certificate), joka sitoo E:n ja sen julk. avaimen (Varmenne ~ “Tämä on E:n julkinen avain”)
  - Varmenne on salattu varmentajan salaisella avaimella.



Varmennepalvelu

- Kun Alice haluaa tietää Bobin julkisen avaimen:
  - Hän hakee/saa Bobin varmenteen (Bobilta tai muualta).
  - Purkaa varmenteen CAn julkisella avaimella ja saa näin puretun sisällön, joka on Bobin julkinen avain



VIESTIN EHEYS, DIGITAALINEN ALLEKIRJOITUS

Digitaalinen allekirjoitus (digital signature)

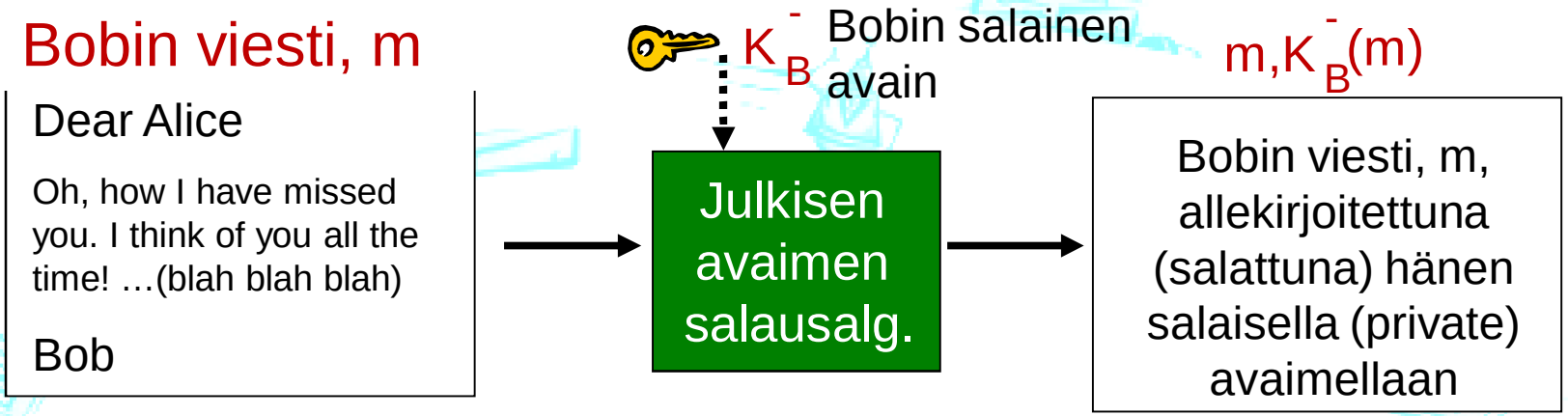
Salaustekniikka, joka analoginen käsintehdyn allekirjoituksen sitovuuden kanssa:

- Lähettäjä (Bob) digitaalisesti allekirjoittaa dokumentin ja näin todistaa, että hän on dokumentin omistaja/laatija.
- *Todennettavissa (verifiable):* vastaanottaja (Alice) voi todistaa jollekin muulle, että Bob eikä kukaan muu on allekirjoittanut tämän dokumentin
- *ei väärennettävissä (nonforgeable)*

Digitaalinen allekirjoitus

Yksinkertainen digit. allekirjoitus viestille m:

- Bob allekirjoittaa m:n salaamalla sen omalla salaisella avaimellaan K_B^- ja luo näin "allekirjoitetun" viestin $K_B^-(m)$



Digitaalinen allekirjoitus

- Alice vastaanottaa viestin m, jossa allekirjoitus: m, $K_B^-(m)$
- Alice todentaa Bobin allekirjoittaman viestin m käyttämällä Bobin julkista avainta by K_B^+ allekirjoitukseen $K_B^-(m)$ ja tarkistaa että $K_B^+(K_B^-(m)) = m$.
- Jos $K_B^+(K_B^-(m)) = m$, niin allekirjoittaja on käyttänyt Bobin salaista yksityistä avainta (olipa allekirjoittaja kuka tahansa)

Alice siis todentaa, että:

- ✓ Bob on allekirjoittanut viestin m
- ✓ Kukaan muu ei ole allekirjoittanut viestiä m
- ✓ Bob allekirjoitti viestin m eikä viestiä m‘

Kiistämättömyys (non-repudiation):

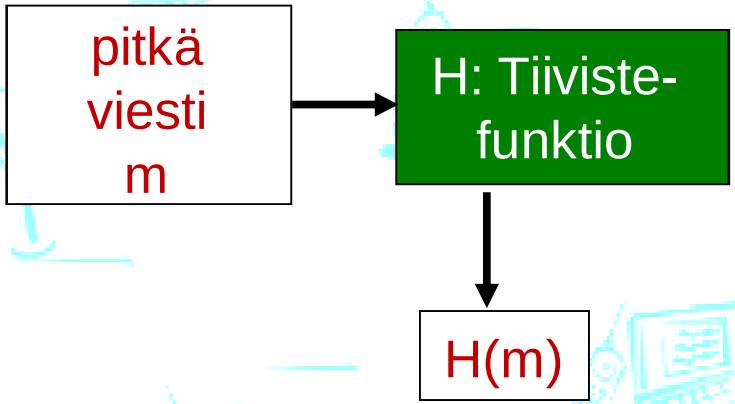
- ✓ Alice voi näyttää viestin m ja allekirjoituksen $K_B^-(m)$ oikeudessa ja näin osoittaa, että Bob on allekirjoittanut viestin m

Viestin tiiviste (*message digest*)

Laskennallisesti vaativaa käyttää julkisen avaimen salausta pitkille viesteille

tavoite: kiinteänmittainen, yksinkertaisesti laskettava “sormenjälki”

- Tee tiivistefunktiolla (cryptographic hash function) H viestille *m* kiinteänmittainen tiiviste *H(m).*



Tiivistefunktion ominaisuuksia:

- Surjektio (monta yhteen)
- Tuottaa kiinteänmittaisen tiivisteen (‘sormenjälki’)
- Jos tunnetaan tiiviste x, on laskennallisesti vaikeaa selvittää m, s.e. x = H(m)

Internetin tarkistussumma : kryptografisesti huono hajautus

Internetin tarkistussumma täyttää osan tiivistefunktion ominaisuuksista:

- ✓Kiinteän mittainen tiiviste (16-bittinen summa) viestille
- ✓Surjektio (monta yhteen)

MUTTA on aivan liian helppoa löytää joku viesti, joka täsmää annettuun tiivisteeseen (=hajautusarvoon):

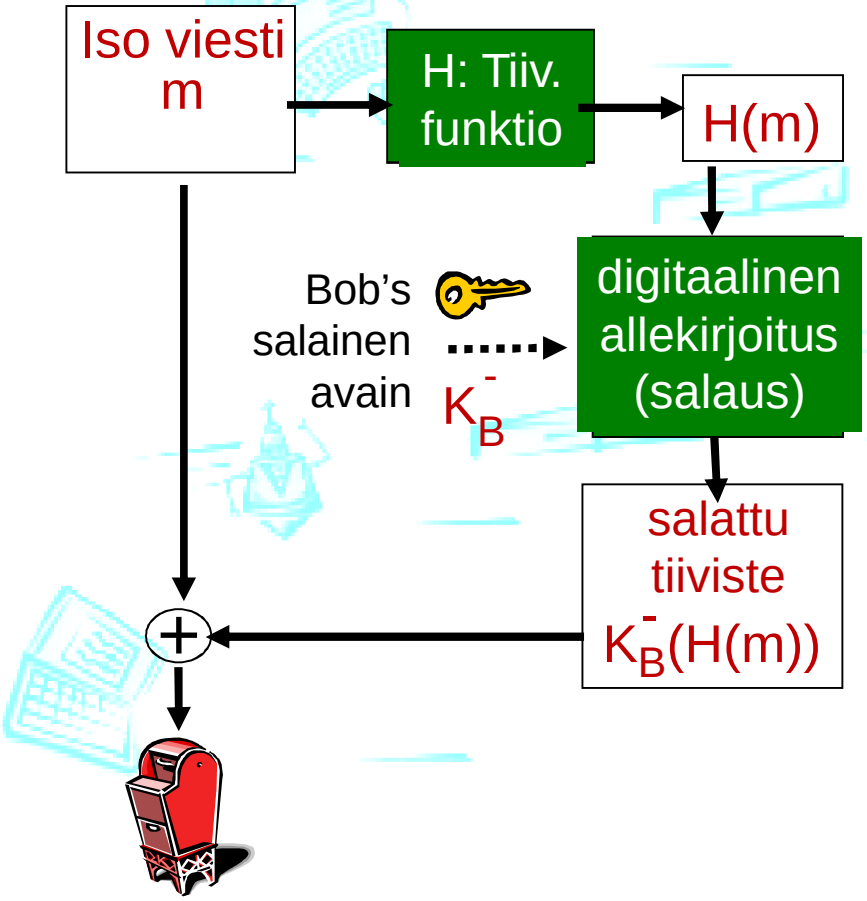
viesti	ASCII merkistöllä
I O U 1	**49 4F 55 31**
0 0 . 9	**30 30 2E 39**
9 B O B	**39 42 D2 42**
	B2 C1 D2 AC

viesti	ASCII:na
I O U 9	**49 4F 55 39**
0 0 . 1	**30 30 2E 31**
9 B O B	**39 42 D2 42**
	B2 C1 D2 AC

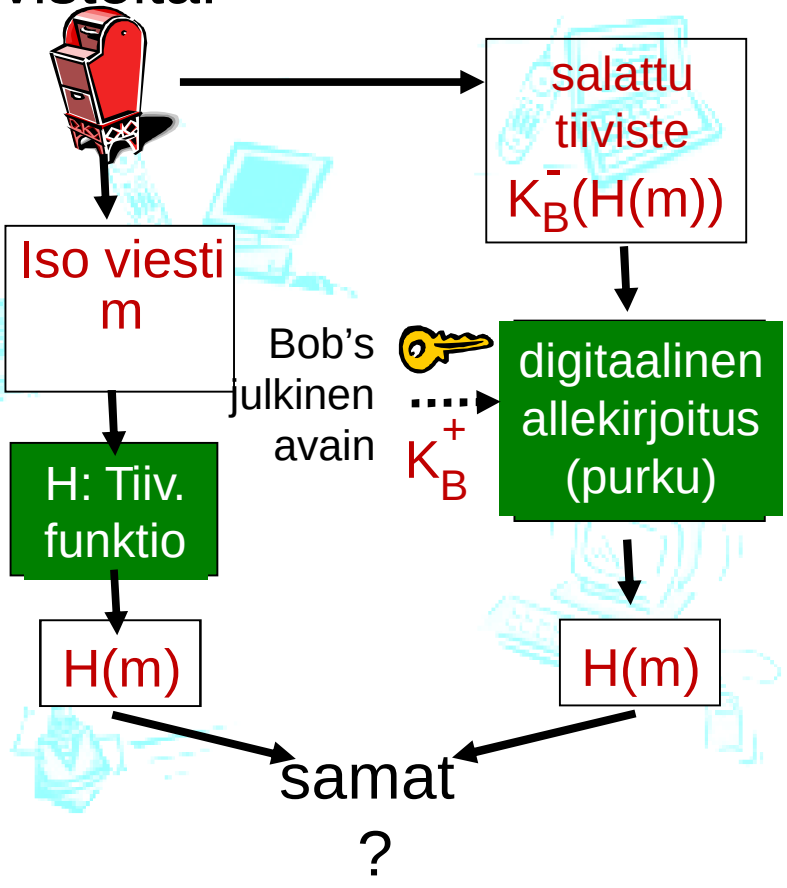
Eri viestit, MUTTA identtinen tarkistussumma!

Digitaalinen allekirjoitus = salattu tiiviste

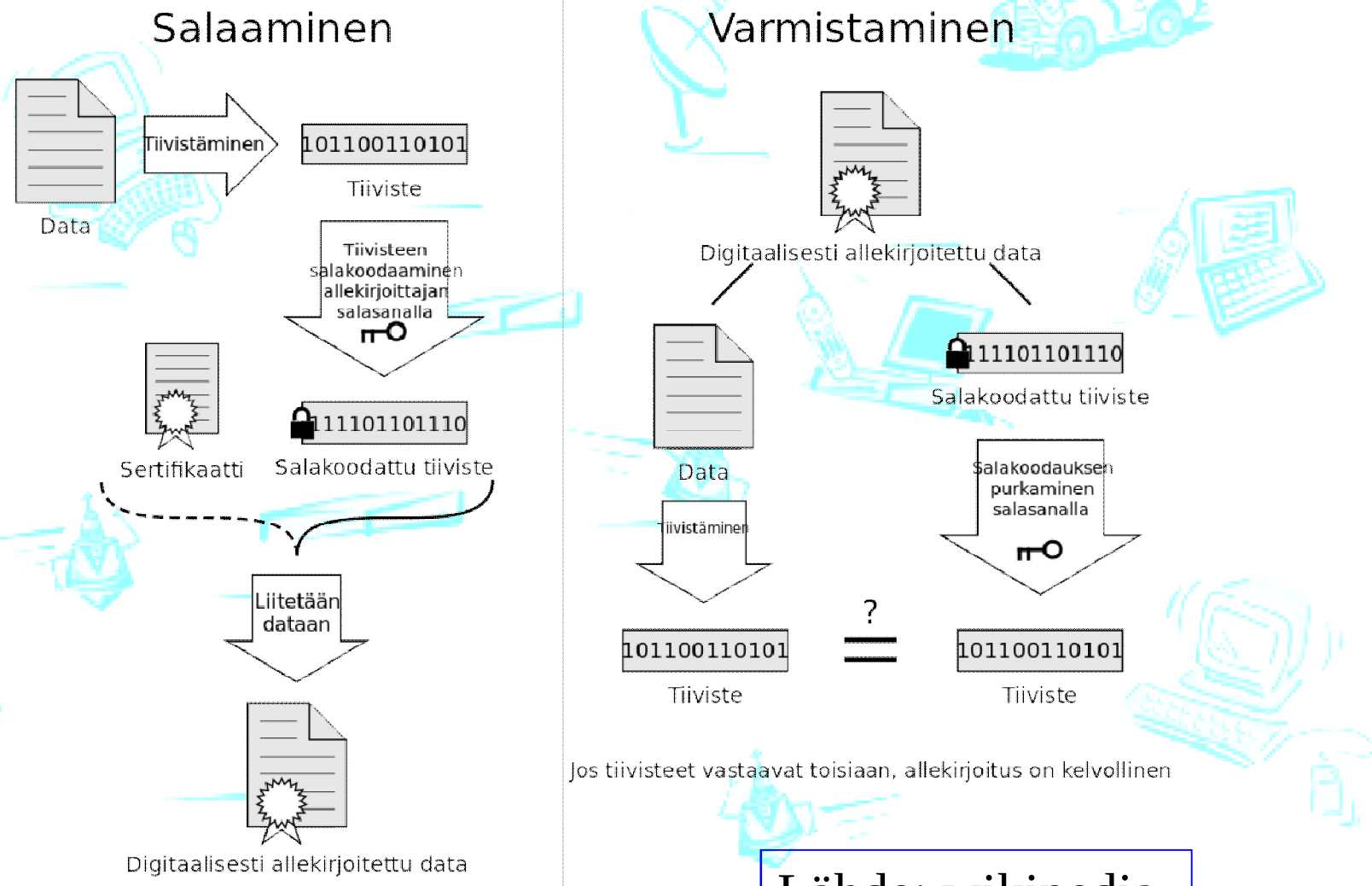
Bob lähettää digitaalisesti allekirjoitetun viestin:



Alice tarkistaa allekirjoituksen oikeellisuuden vertaamalla tiivisteitä:



Digitaalinen allekirjoitus



Lähde: wikipedia

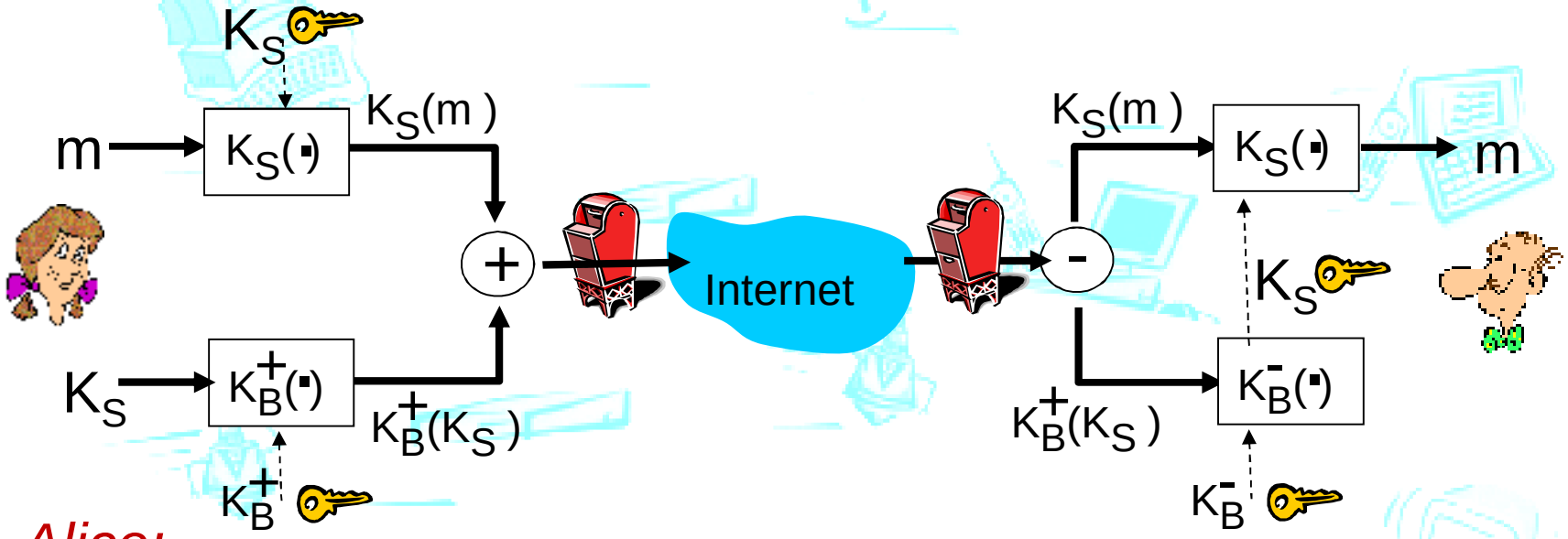
Tiivistefunktioita ja -algoritmeja

- MD5 tiivistefunktio yleisesti käytetty (RFC 1321)
  - laskee 128-bittisen tiivisteen 4-vaiheisella prosessilla
  - Vaikuttaa haastavalta konstruoida viesti m, jonka MD5 tiiviste olisi tietty (ennalta satunnaisesti valittu) x
- SHA-1 myös käytössä
  - US standardi [NIST, FIPS PUB 180-1]
  - 160-bittinen tiiviste

SOVELLUSKERROS: SÄHKÖPOSTIN SUOJAUS

Sähköpostin salaus

- Alice lähettää luottamuksellisen sähköpostin Bobille

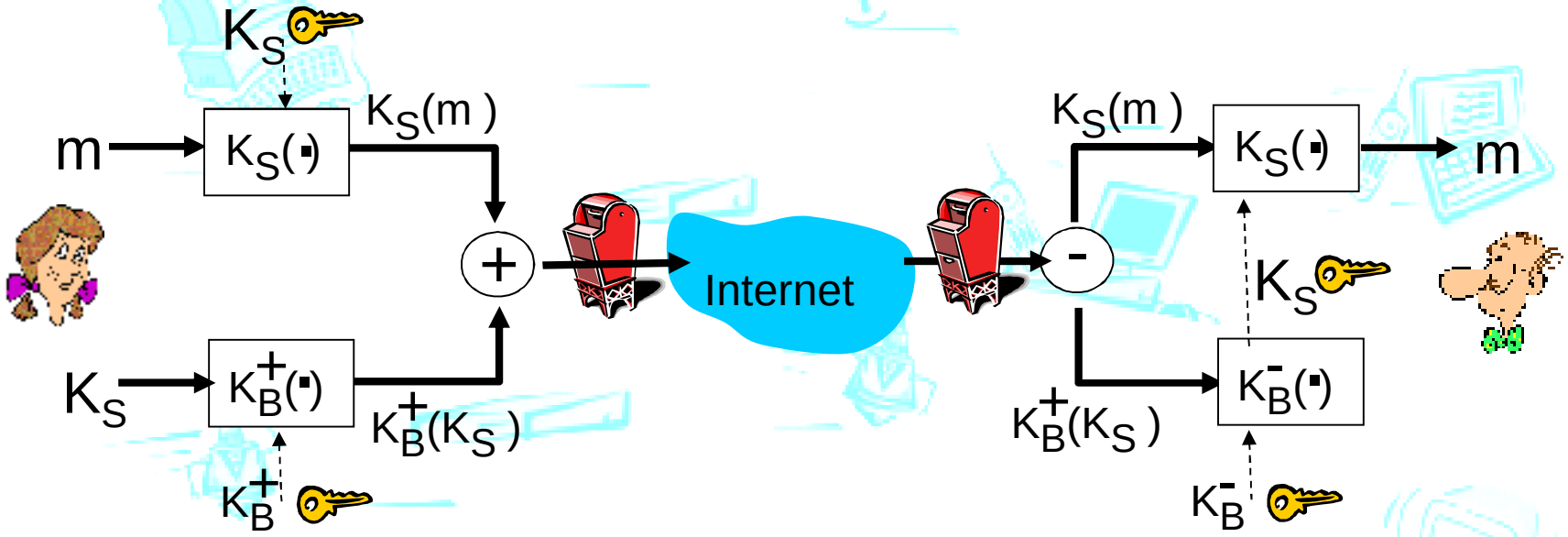


Alice:

- generoi satunnaisen *symmetrisen* salausavaimen K_S
- salaa viesti tällä avaimelle K_S (tehokkuus!)
- salaa avaimen K_S Bobin julkisella avaimella
- lähetä salatun viesti $K_S(m)$ ja avaimen $K_B(K_S)$ Bobille

Sähköpostin salaus

- Alice lähettää luottamuksellisen sähköpostin Bobille

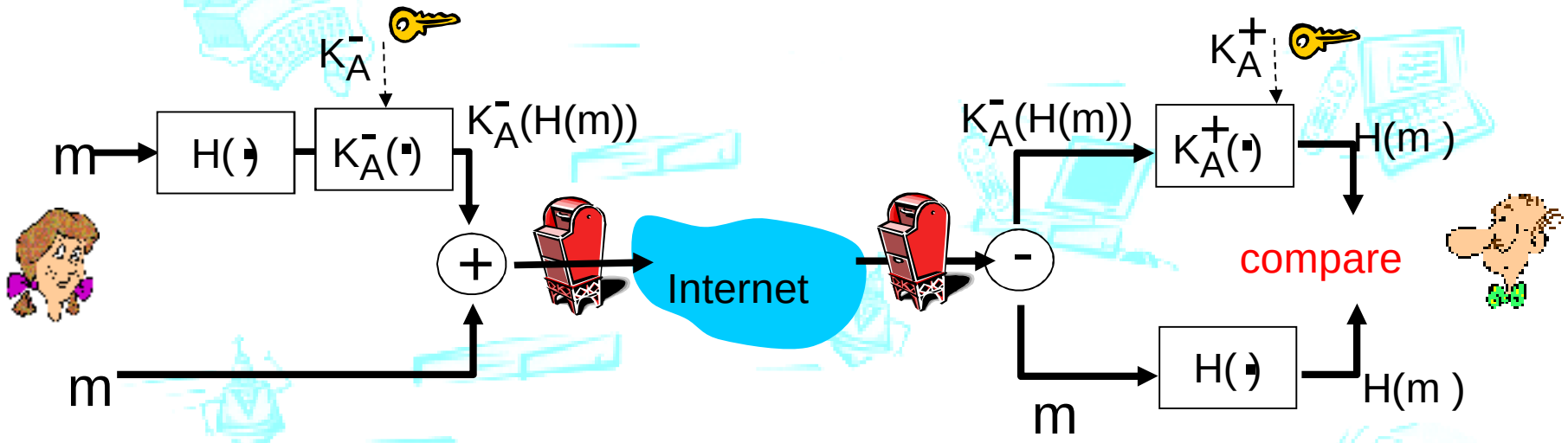


Bob:

- käyttää salaista avaintaan ja purkaa esiin avaimen K_S
- käyttää avainta K_S ja purkaa salatun viestin $K_S(m)$, ja saa näin alkuperäisen viestin m

Sähköpostin suojaus (jatkuu)

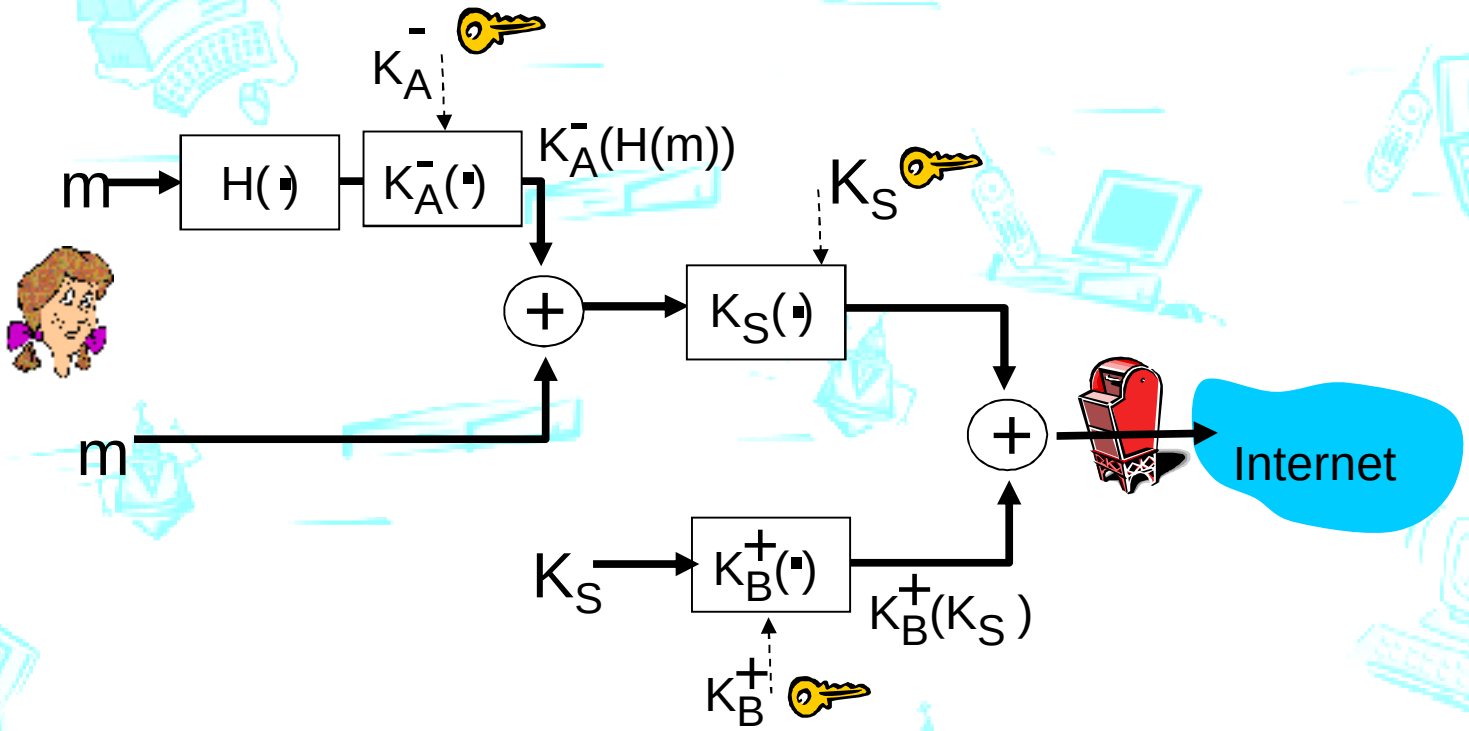
- Alice haluaa varmentaa lähettäjän ja allekirjoittaa viestin



- Alice laatii digitaalisen allekirjoituksen (=tiivisteen) viestille käyttäen omaa salaista avaintaan
- Lähettää sekä (selväkielisen) viestin että allekirjoituksen

Sähköpostin suojaus (jatkuu)

- Alice haluaa lähettää allekirjoitetun ja salatun viestin.



Alice käyttää KOLMEA AVAINTA: oma salainen avain, Bobin julkinen avain, uusi luotu symmetrinen avain

Sähköpostin suojaus (jatkuu)

- Bob purkaa Alicelta saamansa salatun viestin tekemällä operaatiot käänteisessä järjestyksessä
- Bob käyttää myös kolmea avainta:
  - Omaa salaista avaintaan
  - Symmetristä avainta (viestin mukana)
  - Alicen julkista avainta