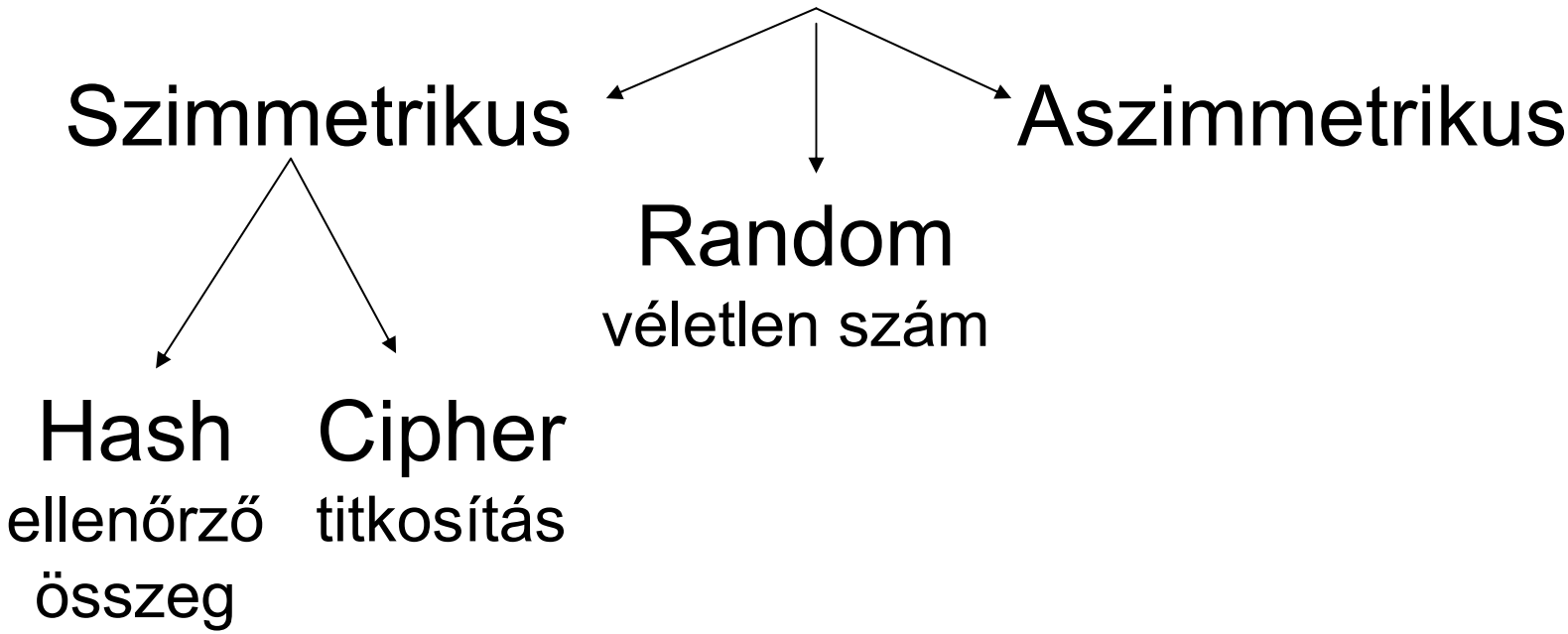
Digitális Kriptográfia

kriptográfiai algoritmusok



Random

Véletlen(szerű) számok előállítása…

- Ha gép készíti, akkor valahogy kiszámolja…
- Igazi véletlen források: fehér zaj, radioaktív bomlás, politikai bejelentések (© Schneier)

Szimmetrikus kódolás

Mindkét fél ugyan azt a számolást hajtja végre, így ugyan arra az eredményre jutnak egymástól függetlenül…

Hash: xor, ±, crc16, crc32, sha1, md2, md4, md5, rmd160, stb…

Cipher: aes, blowfish, cast, des, rc2, rc4, rc5, rc6, mars, twofish, stb…

Példa szimmetrikus kódolásra

Szerver
kulcs=12
adat=1,2,3
cipher= ±
1+*12*=**13**
2+*12*=**14**
3+*12*=**15**

Kliens
kulcs=12
cipher= ±
13-*12*=*1*
14-*12*=*2*
15-*12*=3
adat=1,2,3

prímek

Nehéz találni…
kis-fermat: a=rnd; a^{p-1}-1 mod p≠0; 50%
vannak módszerek…

2^{127}-1=170141183460469231731687303715844105727

Valahol itt kezdődik a nagy prím… ☺

109074813561941592945029492935978450034815512495317221177410110696615016892278563902853247384883681
776971216416907643296922469875267467766273999426578543723359615704597092233804069810050786103304731
233182398243527947570019986097161273254052879655450286791974677698375939147598714252131587871957751
914881183087991942693995848708754096571641916746749932615622652967520917227700137759124814756378288
055886108332717415401497513489312511601577631889029596069801161415772128252753946881651931933333750
311477719236041228172101895583437761548046847925274886732036238535559660179512280675621771357981987
063432156190781325515370395079527123265240489498386949217448165230380349888136621050864726366837651
413103110233683748899977574404673365182723939535354034841487285463971929469432345018688418982254454
064722698729216069318473465494190693664657613026097219328031717169641897155395416144619175909371952
495111670557736207348131929604120128351615426904438925772770028968411946028348045230620413002491387
998113590802698386820596931816781968085099864969441690795271290496240493777578969891720735635522745
506618381584766913553054975543981948032173292586906913614608532638233462874545639807160305805163420
938670870330654590319960852382451372962513665912822110096773545051995240424819826281383109737426165
038001727791697532413484657468130733701738083035368062321633694947130619168643824930568641338023104
609645095359408937554028503729247092939511402830554745258496207430943815182543790297601289174935519
867842060372203490031136489304649576140433393868614003784803091629254327368453364003263763910077450
237154247930247369838869289242094647894773380038778274141778648477019010886787977899163321862864053
398261932246615488301145229189025233648723608665439609385389862880581317755916207636315443649447750
787129411984163786770172216660983120184548407807051804133686980839845462558692120130818563888808269
940868653604519264956919811035365994311180230063610650986502394366182943642656300791728205089442938
884174888539829070774305297360535927751574961973082377321589475512176146788786532770711557380426451
920634921585019519536481338752681174247413154980213024650634120702033579770678070540694527543880626
597851620970679570257924407538049023174103086261496878330620786968786810842363997198320907762475808
049998827559139278726762718244289280964687422826317243564236858826013916196283612148196609274532548
864105423883929513899297933544611009032523095527687052461135912491839274035315429485838335 9

Aszimmetrikus kódolás

Mindkét fél különböző adatokból indul ki, de végül ugyan arra az eredményre jut.
Bizonyíthatóan megoldhatatlan problémák…
Kulcscsere vagy kódolás…
algoritmusok: rsa, diffie-hellman, dsa, elliptic-curve, stb…

aszimmetrikus algoritmusok

rsa: $m^e \bmod p$

dsa-sig: $r=(g^k \bmod p) \bmod q$; $s=(k^{-1}(M+xr)) \bmod q$

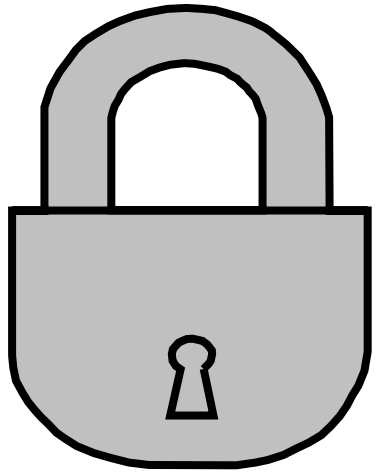
dsa-ver: $(g^{Ms^{-1}}\ y^{Ms^{-1}}) \bmod p) \bmod q \ \ ?=?\ r$

dh: $e=g^x \bmod p$; $f=g^y \bmod p$; $k=e^y \bmod p=f^x \bmod p$

ec-sig: r=x(k*F)+M; s = k - Ak*r

ec-ver: r-x(s*F+r*AP) ?=? M

A Diffie-Hellmann kulcscsere



Hozzávalók:

- Egy nagy prím szám (p)
- Egy generátor a prímhez (g)
- Egy biztonságos véletlen szám generátor (rnd)
- Egy biztonságos változó megsemmisítő (clr)

Diffie-hellman algoritmus

Szerver

Kliens

p prím, g generátor

rnd(x)

$e=g^x \bmod p$

rnd(y)

$f=g^y \bmod p$

$e=g^x \bmod p$

$f=g^y \bmod p$

$K=f^x \bmod p$

clr(x)

$K=e^y \bmod p$

clr(y)

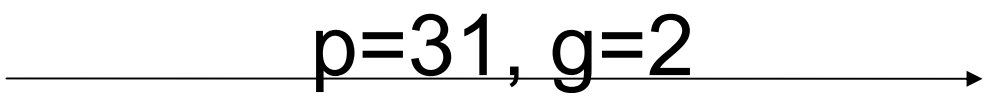
Diffie-hellman példa

prím: p=31

generátor: g=2

szerver oldali véletlen szám: x=24

kliens oldali véletlen szám: y=22



x=24

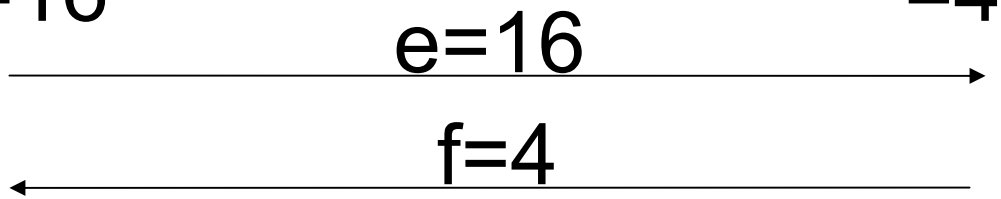
$e=2^{24} \bmod 31$

$=16$

y=22

$f=2^{22} \bmod 31$

$=4$



$K=4^{24} \bmod 31$

$=8$

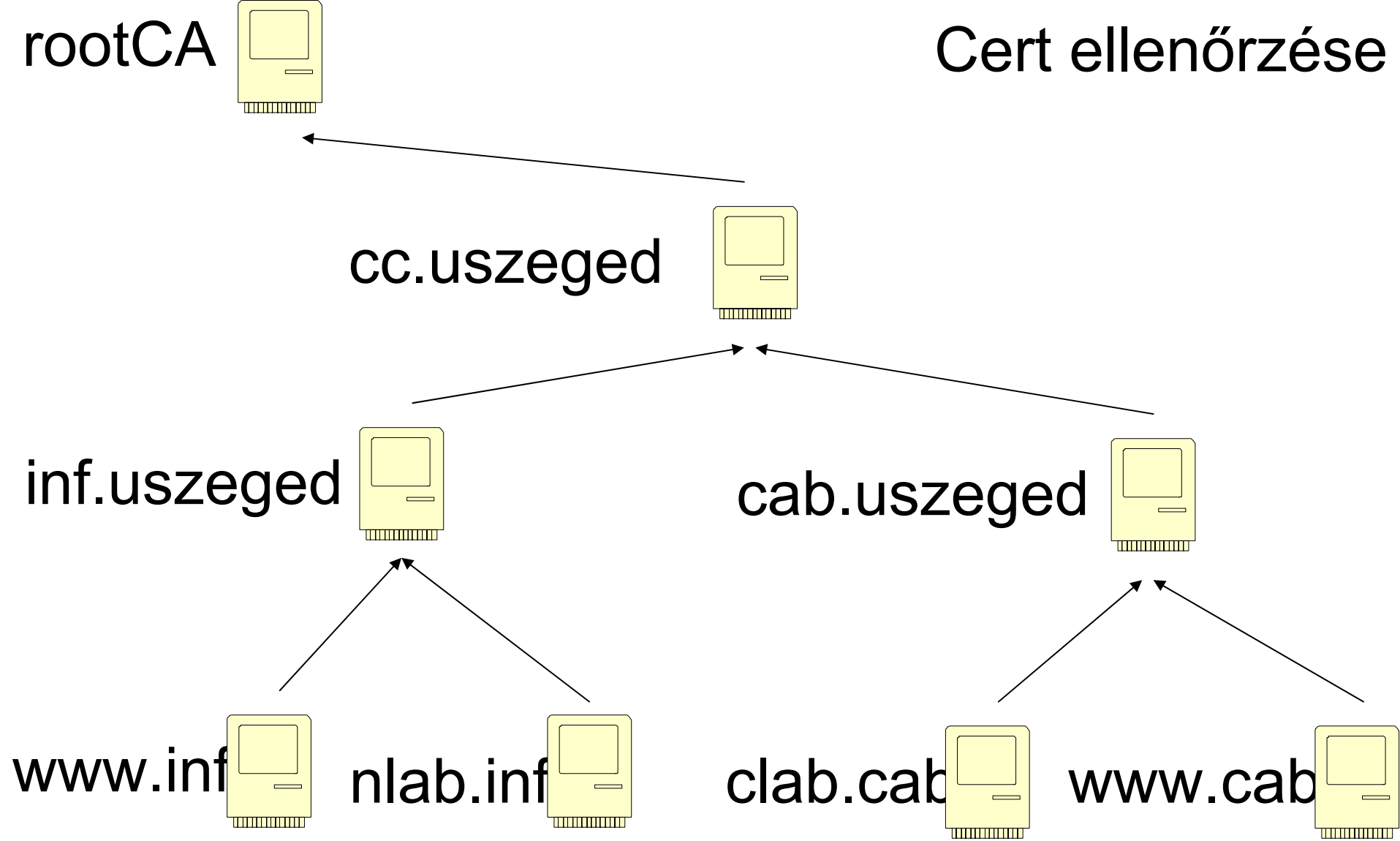
$K=16^{22} \bmod 31$

$=8$

Titkosított kapcsolat

1. Kulcscsere (dh, rsa)
2. Szerver ellenőrzése (cert; dsa, rsa)
3. Cipher és hash bekapcsolása

Pl.: ssh, ssl, tls


rootCA
Cert ellenőrzése
cc.uszeged
inf.uszeged
cab.uszeged
www.inf
nlab.inf
clab.cab
www.cab

referenciák

A TE barátod…

Köszönöm a figyelmet!