Modern kriptográfia:
a lehetetlen művészete

Csirmaz László
Deli Eszter Kinga
CEU
2007

A modern kriptográfia kezdete: asszimetrikus titkosírás

Egy zárhoz két kulcs tartozik:

csak bezárni

csak kinyitni

Tudom hogyan kell titkosítani

Tudom hogyan kell visszafejteni

NINCS TITOK

Ha ezt látom

ez meghatározható

MÉRNÖKI FELADAT

TEHÁT: asszimetrikus titkosírás NEM LÉTEZIK

Ilyen állat nincs:

Vagy mégis?

Új fogalmak:

Elvben kiszámítható

- Alan Turing
- Stephen Kleene
- Péter Rózsa
- Kalmár László

~ 1930

ITT NINCS

Gyakorlatban kiszámítható

- Leonid Levin
- Richard Karp

$P \stackrel{?}{=} NP$

~ 1960

ITT VAN

ASSZIMETRIKUS TITKOSÍRÁS

Lehetetlen? Vagy mégsem?

R.S.A

- Don RIVEST
- Ali SHAMIR
- Leonard ADLEMAN

1976

D.H.

- Whitfield DIFFIE
- Martin HELLMAN

1976


Shamir
Adleman
Rivest

Hellman

Diffie

DH: *p* prímszám,

g, $1 < g < p$ generátor,

$y \equiv g^x \pmod{p}$

ismert: p, g, y

titok: x

RSA: p, q prímek, $n = p \cdot q$,

$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$

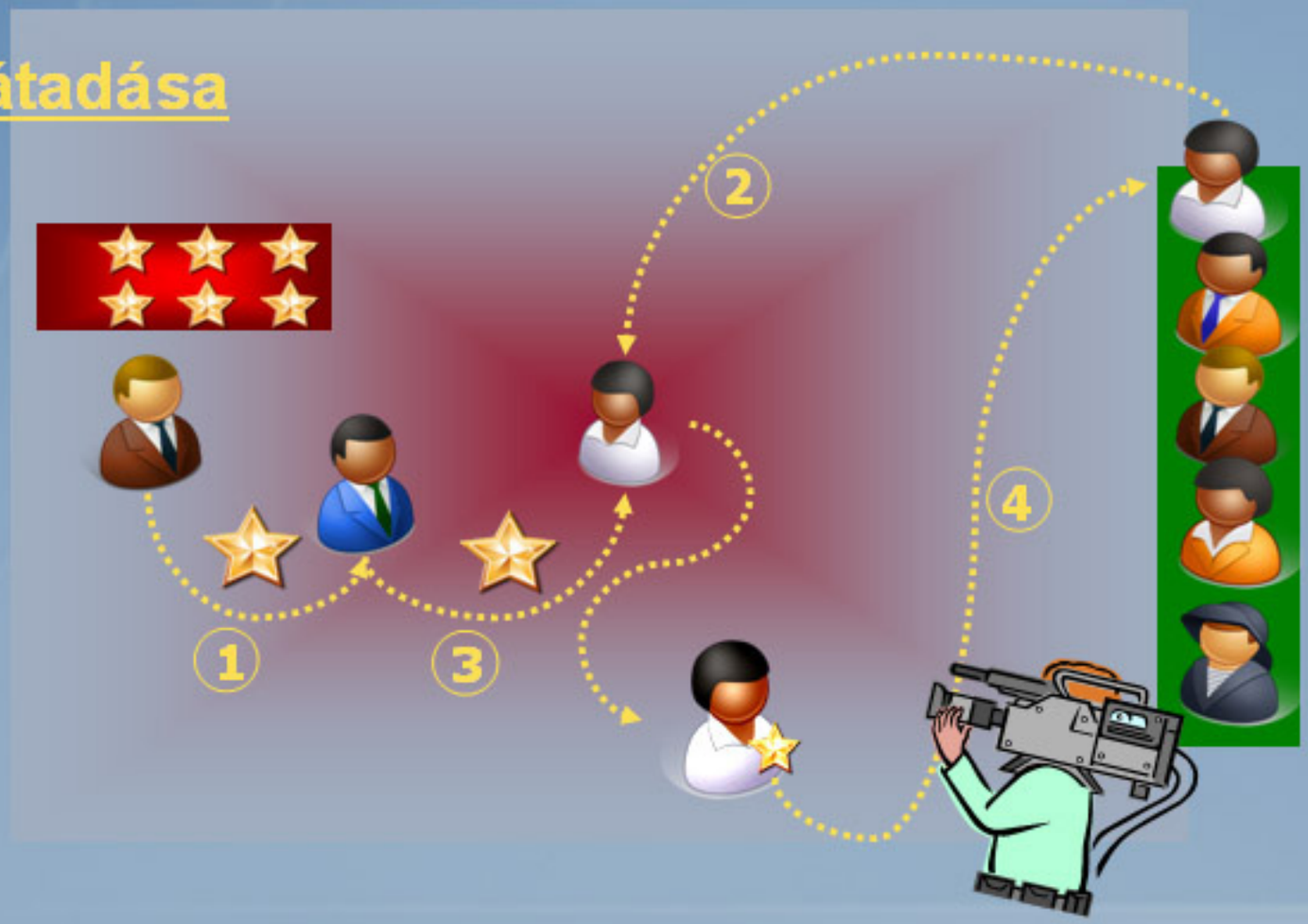
Ha $y \equiv x^e \pmod{n}$,
akkor $x \equiv y^d \pmod{n}$

ismert: n, e

titok: d

Protokoll: Mi hogyan történjen?

Kitüntetések átadása



1. Az asszisztens az elnök kezébe adja a dobozt
2. A kitüntetett balról érkezik
3. Az elnök átadja a kitüntetést, kezet fognak
4. A kitüntetett jobbra távozik

A protokoll résztvevői:

1. Becsületesek VAGY
2. Becsületesek, ámde érdeklődők VAGY
3. Gonoszok

Két résztvevő ⟷ Több résztvevő

Nem tudjuk ki a gonosz:

- A kitüntett nem fog kezet
- Az elnök nem fog kezet

↓

A protokollnak a becsületes résztvevőt kell védenie!

DE MEG LEHET-E EZT MINDIG CSINÁLNI?

Példa: azonosítás

A: Én vagyok Én ... B: Ki vagy Te?

útlevél
jelszó
hitelkártya

ellenőrzi...
Rendben!

Ha B becsületes: A nem tudja átverni: érvényes dokumentumok
Ha A becsületes: B ne tudja felhasználni a kapott információt
(pl. kártya lehúzás)

A-t hogyan lehet védeni? **LEHETETLEN?**

Tudás bizonyítása (Adi Shamir)

A: "tudom a jelszót"

B: "mi az?"

A: "mi közöd hozzá?"

Használjuk a Diffie–Hellman titkosírást: p és g ismert, y adott

A állítja: "ismerek olyan x-et, amire $g^x \equiv y$"

Tudás bizonyítása - folytatás

1. A választ egy $1 < r < p - 1$ véletlent, kiszámítja $a \equiv g^r \pmod{p}$

$A \xrightarrow{\quad a \quad} B$ *"elkötelezettség"*

2. B választ egy véletlen b értéket, amire $1 < b < p - 1$

$A \xleftarrow{\quad b \quad} B$ *"kihívás"*

3. A keres olyan c-t, amire $a \cdot y^c \equiv g^b \pmod{p}$ (például $c = b - r \cdot x$ jó), majd

$A \xrightarrow{\quad c \quad} B$ *"válasz"*

4. B ellenőrzi, hogy tényleg $a \cdot y^c \equiv g^b$?

ZK: zero knowledge (nulla ismeretet közlő) protokoll

1. Ha A ismeri a titkot, minden kihívásra tud jól válaszolni

2. Ha A nem ismeri a titkot, legfeljebb 1 kihívásra tud jól válaszolni (tippelhet) ➡ B védve van

3. B nem tud meg semmit A titkáról ➡ A védve van

"Semmi": a párbeszéd jegyzőkönyvét B elő tudja állítani anélkül, hogy A-val beszélt volna.

Példa:

A: Gábor mamája, "tudom hogyan kell zoknikat párosítani"

B: Gábor: "nem hiszem"

Elkötelezettség: $A \rightarrow B$: itt van 5 pár zokni összerakva

Kihívás: zoknikra cimkék, párosítás felírva, zoknik összekeverve, $B \rightarrow A$: tessék összerakni!

Válasz: $A \rightarrow B$: zoknik párosítva, B ellenőrzi, hogy ez a felírás szerint történt-e.

Többször ismételhető. B *nem tudja meg, hogyan kell a zoknikat összerakni.*

RANDOM SZÁMOK:

6 3	4 2	10 1	9 8	7 5

GÁBOR

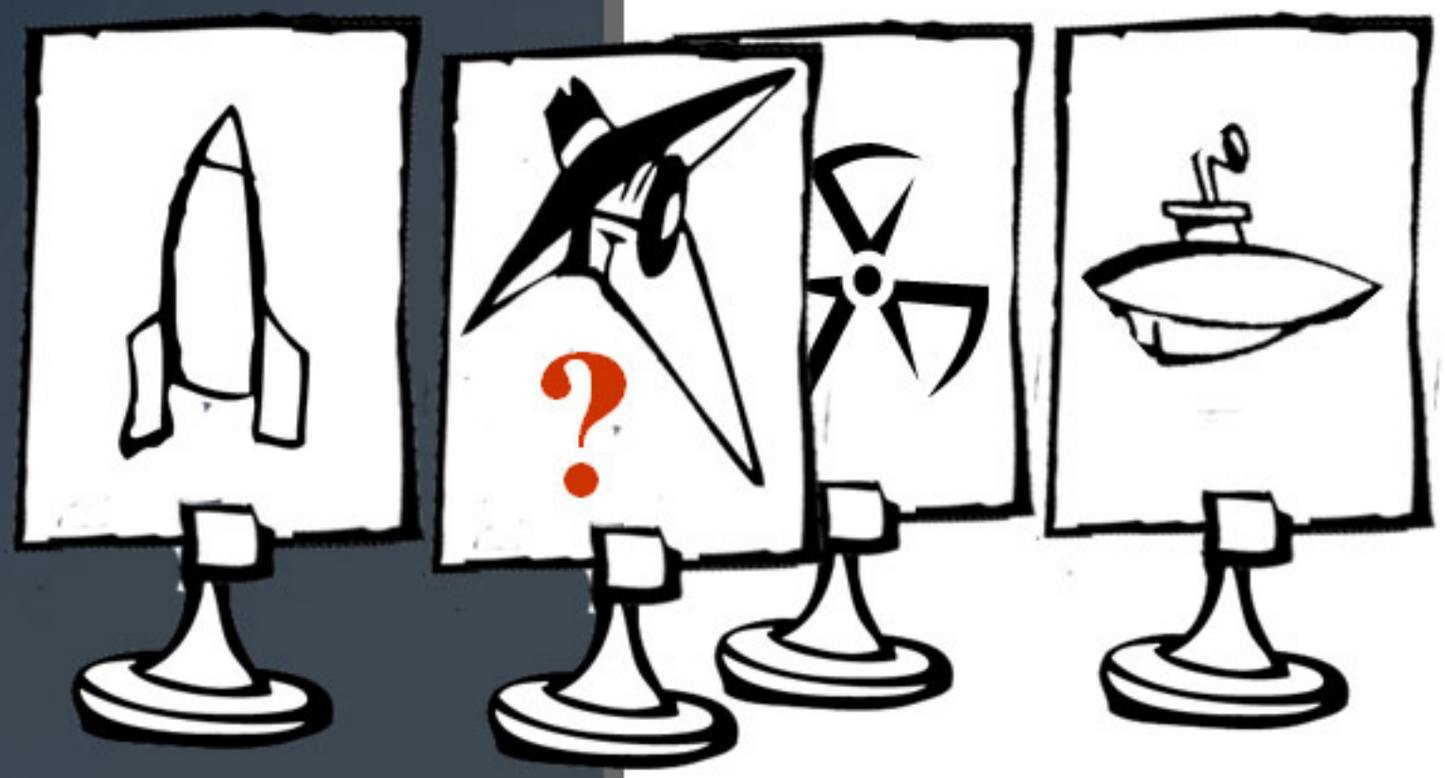
1 4 3 7 2 9 10 8 6

GÁBOR MAMÁJA

1 10 | 3 6 | 4 2 | 9 8 | 7 5

KÉM VS KÉM

KÉM VS KÉM

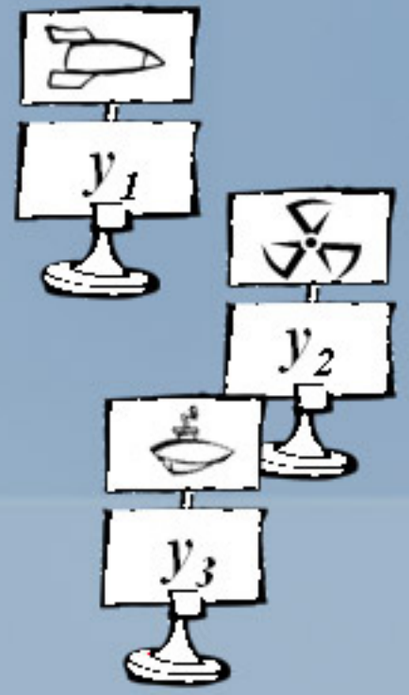


Alkalmazzuk az RSA-t:

$(x^e)^d \equiv x \pmod{n}$ **(e, n nyilvános)** pl.: e = 1256412345464674

n = 3415443516435156

1. titok kulcsa: x_1, $y_1 \equiv x_1^e \pmod{n}$
2. titok kulcsa: x_2, $y_2 \equiv x_2^e \pmod{n}$
3. titok kulcsa: x_3, $y_3 \equiv x_3^e \pmod{n}$



Vásárlás:

r véletlen, $z = r^e \cdot y_i \pmod{n}$

"Kérem dekódolni z-t":

$$z^d \equiv r^{ed} \cdot y_i^d \equiv r \cdot x_i \pmod{n}$$

az eredményt r-rel elosztva a kulcsot megkapjuk.

Kártya telefonon

Hogyan osszák el a pakli kártyát úgy, hogy

1. mindenki tudja milyen kártyát kapott
2. senki nem tudja, hogy a maradék a másik kettő között hogyan oszlik el.

LEHETETLEN?

Bárány Imre, Füredi Zoltán (1992)

Kártyák magyarul

MOA

Kártyáid magyarul

Kártyáid oroszul
(M - O szótárból)

ÉN kártyáim magyarul

TE kártyáid angolul
(M - A szótárból)

Elektronikus pénz

- bitsorozat, gépben, csipkártyában ül
- költhető
- mint a készpénz (internetes vásárlás, italautomata, villamosjegy, parkolás)
- nem hamisítható (digitális aláírás), de
- MÁSOLHATÓ (hiszen csak bitek)

"A pénznek nincs szaga" – akinek adtam, nem tudja bizonyítani, hogy tőlem jött.

Ha egyszer költök: nem következő vissza
Ha kétszer költöm el: azonosítható vagyok.

LEHETETLEN?

Ötlet:

Az Y tengelyen a felhasználók nevei; az elektronikus érme egy egyenes, ami átmegy felhasználó nevét jelző ponton.

Vásárláskor a boltos választ egy x helyet, az egyenesen az x fölötti pontot meg kell mondani.

Egy költés:

az érme ezen a ponton átmenő egyenes, akárki lehet a tulajdonos

Két költés:

az érme átmegy mindkét ponton, a tulajdonost kimetszi az Y tengelyből

Megvalósítás:

g_1, g_2 generátorok, ismertek

A egy érméje:

s_1, s_2, t titkos véletlen számok

$$m = g_1^{s_1} \cdot g_2^{s_2}$$
$$g = (g_1^{A\ \text{neve}} \cdot g_2)^t$$

(m, g) + bank aláírása + érme értéke

Költés:

1. $A \xrightarrow{(m,\, g)} B$

2. B ellenőrzi, hogy helyes értékeket kapott, d véletlen,

$A \xleftarrow{d} B$

3. A kiszámolja r_1-et és r_2-t: $r_1 = A \cdot t \cdot d + s_1, r_2 = t \cdot t + s_2$

$A \xrightarrow{r_1,\, r_2} B$

4. B ellenőrzi, hogy $g_1{}^{r1} \cdot g_2{}^{r2} \stackrel{?}{=} g^d \cdot m$,

5. ha igen, (d, r_1, r_2)-et elküldi a banknak.

Kétszeres költés:

A bank megkapja (d, r_1, r_2)-t és (d', r'_1, r'_2)-t:

$$r_1 = Atd + s_1 \qquad r' = Atd' + s_1$$
$$r_2 = Atd + s_2 \qquad r' = Atd' + s_2$$

négy ismeretlen (At, t, s_1, s_2), négy egyenlet

⇓

A kiszámítható

Ki gondolt nagyobb számra?

Vásárláskor ki mondjon először árat: a vevő vagy a vásárló?
Csak annyi derüljön ki: magasabb-e az ajánlott mint a kért ár!

Pénzfeldobás telefonon: te feldobod a pénzt, én választok

Yao milliomos problémája: ki a gazdagabb? Ha többen vannak ki a leggazdagabb?

MPC: (multiparty computation) a kezdeti adatok maradjanak titokban, csak a végeredmény publikus

PIR: (private information retrieval) adatbázisban keresés anélkül, hogy az adatbázis gazdája tudná, mit keresek (mint a kémeknél...)

Persze mindez működjön gonosz résztvevőkkel is ...

LEHETETLEN?

?

Hölgykoszorú átlagéletkora

1.hölgy:

- felsö lapra felír egy 6 jegyű véletlen számot (például 452197)
- letépi, elrakja
- hozzáadja saját életkorát, felírja a felső oldalra, továbbadja

2.hölgy:

- letépi a felső lapot, hozzáadja életkorát, felírja, továbbadja

körbe ért:

- az 1. hölgy levonja a számból az általa kitalált véletlen számot.

Látványos kriptográfia

Számítások nélkül...

"Meg tudtam oldani ezt a nehéz sudoku-t, de nem mutatom meg hogyan!"
Kellék: több kitöltött példány és egy olló (Benny Pinkas)

"Ezt a maszatot magammal hoztam, a másikat faxon kaptam"
Kellék: írásvetítő fóliák (Adi Shamir)

"Meg van elégedve a főnöke munkájával?"
Kellék: egy pakli kártya (Sid Stamm, Markus Jakobsson)

Köszönöm a figyelmüket!