

Modern Cryptography: **the art of the impossible**

Csirmaz László
Deli Eszter Kinga
CEU
2007

The beginning of modern cryptography: asymmetric encoding

A lock has two keys:



locks only



unlocks only

I know how to encrypt

I know how to decrypt



NO SECRET

If I see this



this can be determined



A JOB FOR ENGINEERS



CONCLUSION: asymmetric encoding is IMPOSSIBLE

No such animal exists:



Or does it?

**[Flying Jackalope,
Well, South Dakota]**

New concepts:

Computable in theory

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

~ 1930

HERE DOES NOT

Computable in practice

- Leonid Levin
- Richard Karp

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

~ 1960

HERE DOES

EXIST ASYMMETRIC CRYPTOGRAPHY

Impossible? Or not?

R.S.A

- Don RIVEST
- Ali SHAMIR
- Leonard ADLEMAN

1976

D.H.

- Whitfield DIFFIE
- Martin HELLMAN

1976



Adleman

Shamir

Rivest

Hellman



Diffie

DH: p is a prime,
 g , $1 < g < p$ generator,
 $y \equiv g^x \pmod{p}$
public: p, g, y
secret: x

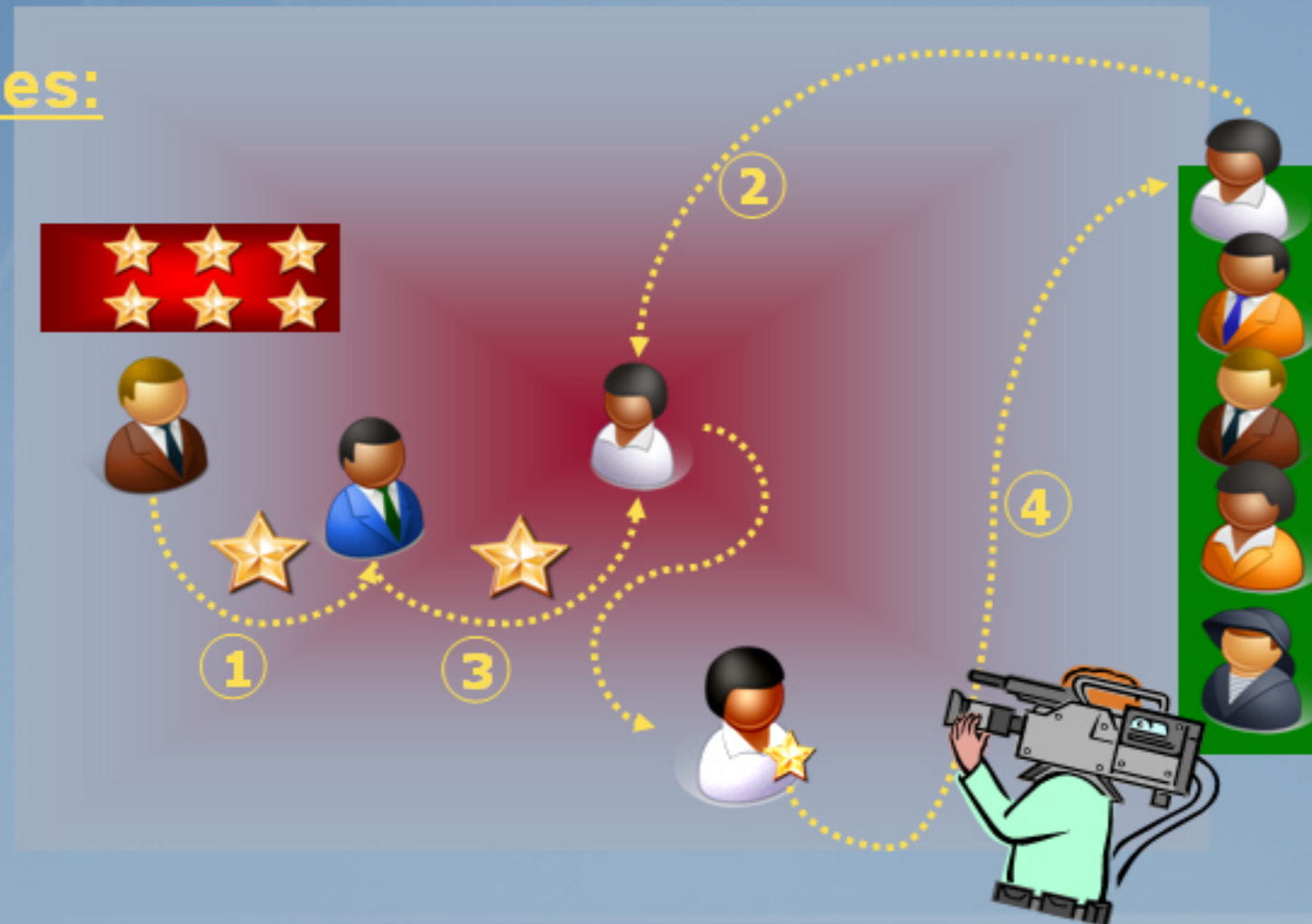
RSA: p, q primes, $n = p \cdot q$,
 $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$

If $y \equiv x^e \pmod{n}$,
then $x \equiv y^d \pmod{n}$

public: n, e
secret: d

Protocol: What should be done and how?

Awarding prizes:



1. Assistant passes the award to president
2. Awardee arrives from left
3. President hands over the award, they shake hands
4. Awardee leaves on to the right

Participants in a protocol:

1. Honest, **OR**
2. Honest, but interested (semihonest), **OR**
3. Corrupt, dishonest

Two - party  Multiparty

We don't know who is corrupt/dishonest

- ➡ Awardee refuses to shake hands
- ➡ President refuses to shake hands



The protocol should protect the honest participants!

CAN IT BE ALWAYS DONE?

Example: Identification

A: It`s me ... *B*: Who are you?

passport
password
credit card



B checks them
OK!



If *B* is honest: *A* cannot cheat as *B* requests valid documents
If *A* is honest: *B* should be unable to use the info received
(e.g. copying credit cards)

How to protect *A* ? **Is it IMPOSSIBLE?**

Proof of knowledge (Adi Shamir)

A: "I know the password"

B: "What is it?"

A: "It`s none of your business!"

Use **Diffie–Hellman cryptosystem**: p, g are public, y is given

A claims: "I know an x for which $g^x \equiv y$ "

Proof of knowledge – cont.

1. A chooses a random $1 < r < p - 1$, computes $a \equiv g^r \pmod{p}$

$A \xrightarrow{a} B$ *“commitment”*

2. B chooses a random b value with $1 < b < p - 1$

$A \xleftarrow{b} B$ *“challenge”*

3. A finds a c , with $a \cdot y^c \equiv g^b \pmod{p}$ (e.g. $c = b - r \cdot x$ is such a number), then

$A \xrightarrow{c} B$ *“response”*

4. B checks whether $a \cdot y^c \equiv g^b$

ZK: zero knowledge protocol

1. If A knows the secret, she can respond correctly to all challenges
2. If A does not know the secret, she can answer to at most one challenge $\Rightarrow B$ is protected.
3. B does not know anything about A 's secret $\Rightarrow A$ is protected

Nothing: B can create the transcript of the protocol without actually talking to A .

Example:

Peter's mother (A): "I know how to pair socks."

Peter (B): "I don't believe you."

Commitment: $A \rightarrow B$: here are 5 pairs of socks matched.

Challenge: labels attached to socks, matching recorded, socks mixed,
 $B \rightarrow A$: Pair them again!

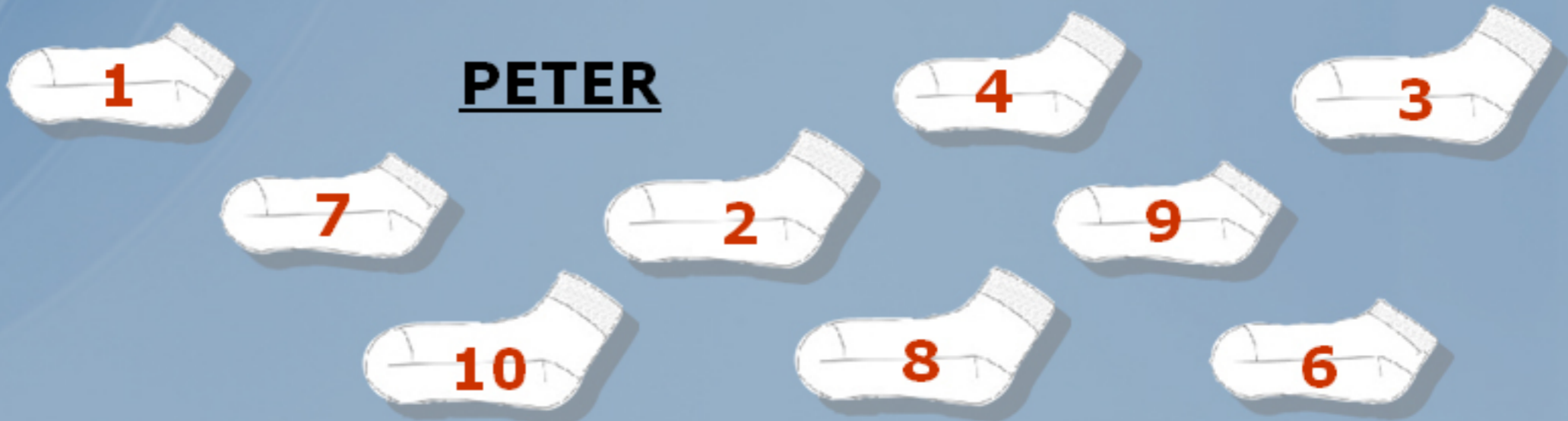
Response: $A \rightarrow B$: socks matched, B checks if pairing agrees with the record.

Can be repeated many times. *B still has no idea how to match the socks.*

RANDOM NUMBERS:

6	4	10	9	7
3	2	1	8	5

PETER



PETER'S MOTHER



SPY

VS

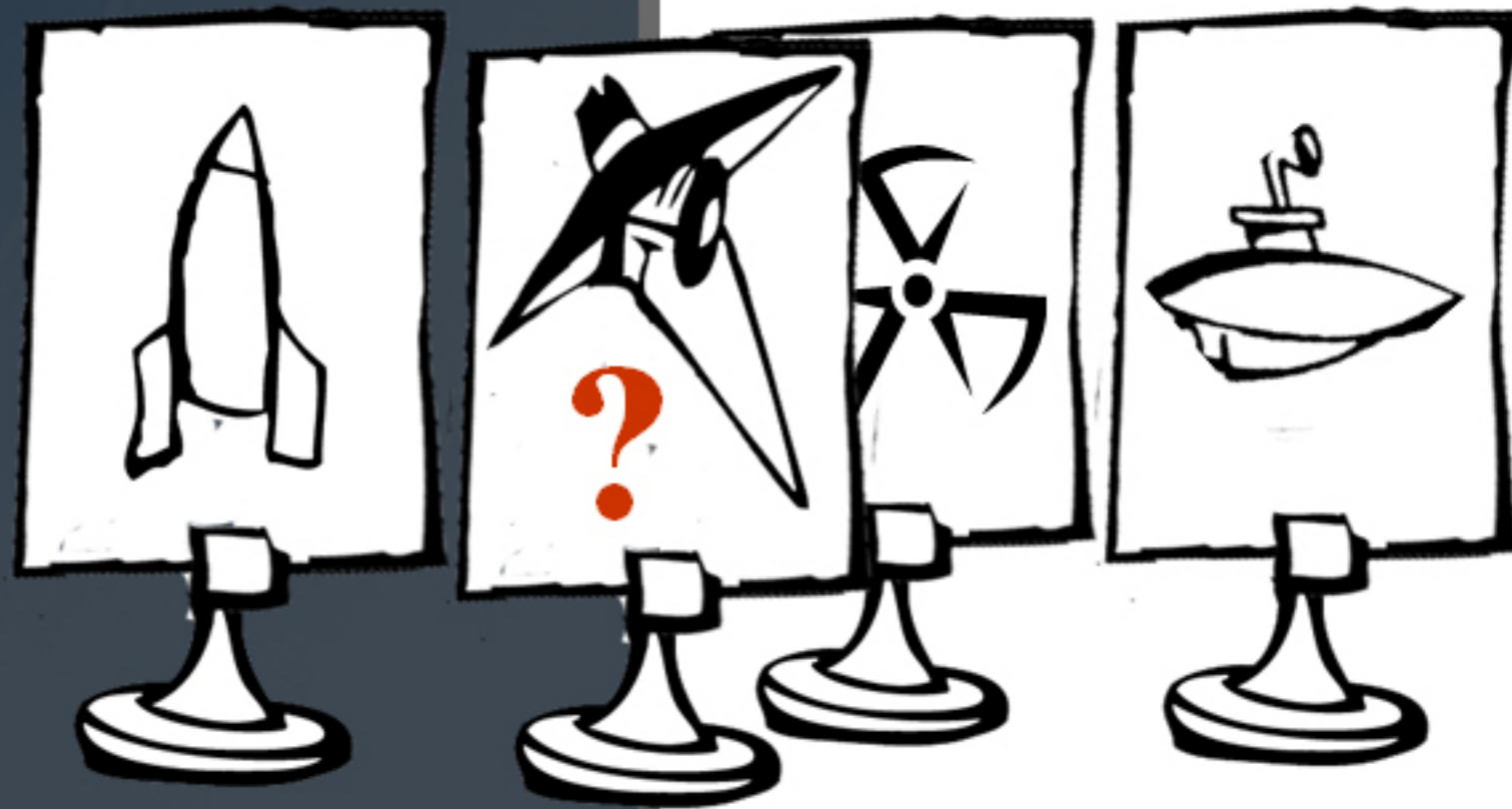
SPY



SPY


VS


SPY




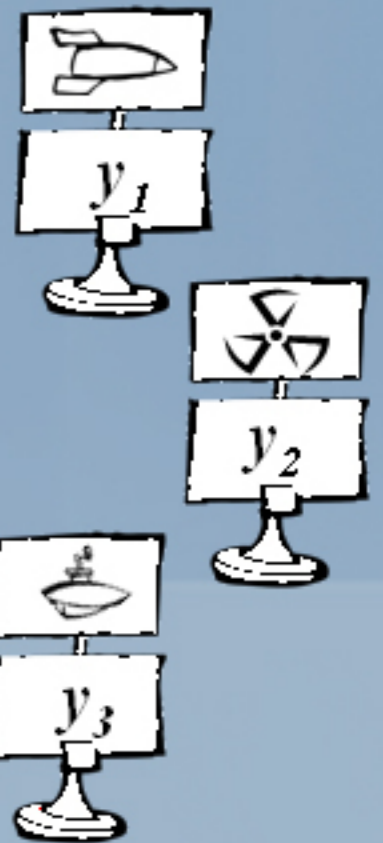
Apply RSA:

$(x^e)^d \equiv x \pmod{n}$ (e, n are public) e.g.: $e = 1256412345464674$
 $n = 3415443516435156$

 x_1 is the key to the 1st secret, $y_1 \equiv x_1^e \pmod{n}$

 x_2 is the key to the 2nd secret, $y_2 \equiv x_2^e \pmod{n}$

 x_3 is the key to the 3rd secret, $y_3 \equiv x_3^e \pmod{n}$



Buying a secret

r is random $z = r^e \cdot y_i \pmod n$

“Please decrypt z , here is the fee”

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

The required key is the result divided by r .

Poker on the phone

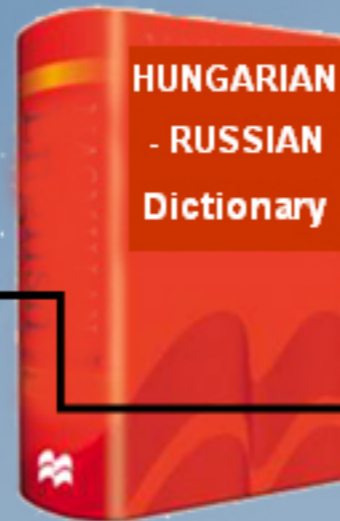


How to distribute a deck of cards such that

1. everyone knows his/her own cards
2. no one knows how the rest is distributed between the other two.

IS IT IMPOSSIBLE?

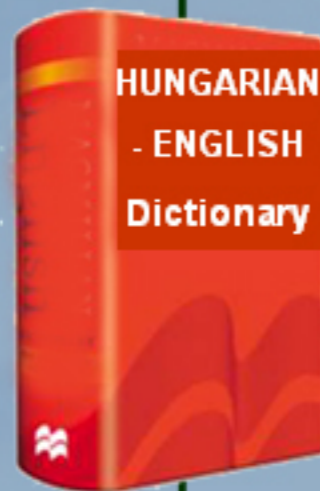
Imre Bárány, Zoltán Füredi (1992)



All Cards in Hungarian



H
R
E

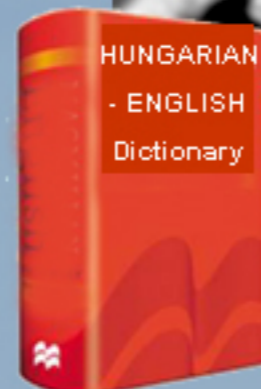




Your cards in Hungarian

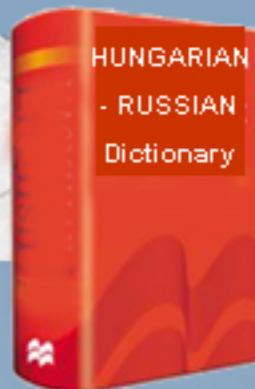
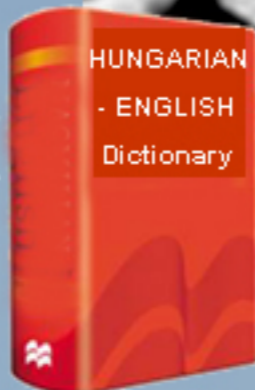


**Your cards in Russian
(From the H - R dictionary)**





My cards in Hungarian



**Your cards in English
(From the H - E dictionary)**

Electronic money

- sequence of bits in your laptop, smartcard, PDA
- you can spend it anywhere
- behaves like cash (internet shopping, vending machines, transport tickets, parking)
- unforgeable (digital signature), **but**
- **CAN BE DUPLICATED** (these are bits only)

UNTRACEABLE – the money should have no indication whose hands it went through

Spending once: I am untraceable

Spending twice: I can be identified

IS IT IMPOSSIBLE?

Idea:

User names are along the Y axis; the electronic coin is a line going through the spender's name.

During spending the merchant chooses x , the value above x is revealed.

Spending once:

the money is a line passing through this point:
anyone can be the spender.

Spending twice:

two points are known on the line – the spender is revealed on the Y axis.

Who has thought of a bigger number?

During price negotiation who should speak first?

Reveal only whether price offered \geq price asked; not the amount

Coin flipping over telephone: you throw the coin, I choose

Yao`s millionaire problem:

Determining who is richer without revealing one's fortune

If there are more millionaires, who is the richest?

MPC: (multiparty computation) initial data must be kept secret, only the result is public

PIR: (private information retrieval) searching in a database without revealing what we are looking for (something spies like to do...)

And this should work with corrupt participants as well...

IS IT IMPOSSIBLE?



?



What is our average salary?

1st member:

- writes a random number (e.g. 43452197) on the top sheet
- tears it off, puts it away
- adds to it her monthly salary, writes the result on the top page, passes it to the next participant

2nd member:

- tears off the top sheet, adds her salary to the number on it, writes down the result, passes on the block

block arrives back:

- the 1st member subtracts her random number.

Cryptography for dummies

Without computations...

“I solved this extremely hard sudoku puzzle, but I won't show you the solution!”

Equipment: several copy of the solved puzzle, scissors

(Benny Pinkas)

“This mass of inkspots was in my luggage, the other was received by fax”

Equipment: transparent slides (Adi Shamir)

“Are you satisfied with your boss's work?”

Equipment: a deck of cards (Sid Stamm, Markus Jakobsson)

Thank you for your attention!
