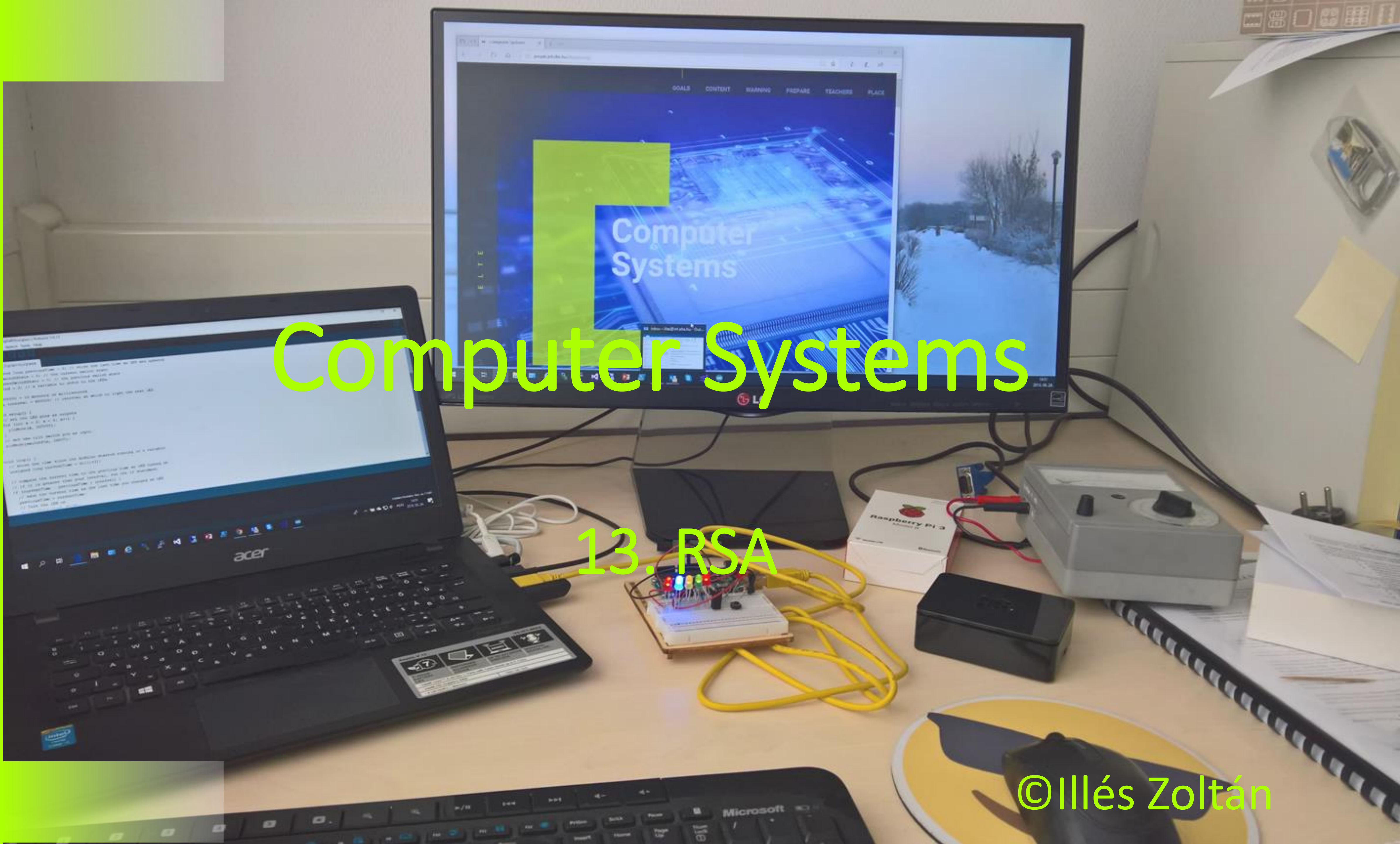
Computer Systems

13. RSA

©Illés Zoltán

ELTE INFORMATIKA



Review

- Computers, information, number representation, code writing, architecture, file systems
- Base commands, processes, regular expressions
- Variables, command substitution, arithmetical, logical expressions
- Script control structures, sed, awk
- Batch, WSH
- Basic networking (skipped)
- PS overview, PS variables, operations
- Basic Powershell commands, control structures

What next today?

- Coding – Encrypting
- Symmetric – Assymetric encryption
- Terminal connecting- Secure connection
  - No telnet
  - Windows Terminál – SSH
  - PUTTY - SSH
- RSA – Simple, Basic

Coding - Encrypting

- Important: A computer can store only numbers in the memor!
- To store text, chars, we need a code table. E.g. ASCII
  - 41h(65) -> A, 4Ch(76) ->L, 4Dh(77) -> M, 41h(65) -> A
- Using standard code tables, that is simple text storing (text files)
- Using modified tables, in that case we call it as encrypting, encrypted text.
- How can we define modified code table?
  - Based on a dedicated book (E.g. 3 numbers(page, row and column number) means 1 char.)
  - Using Math
    - Symmetric (pl. XOR, AES,BlowFish…)– Assymetric encoding (RSA)

Basic ASCII codetable

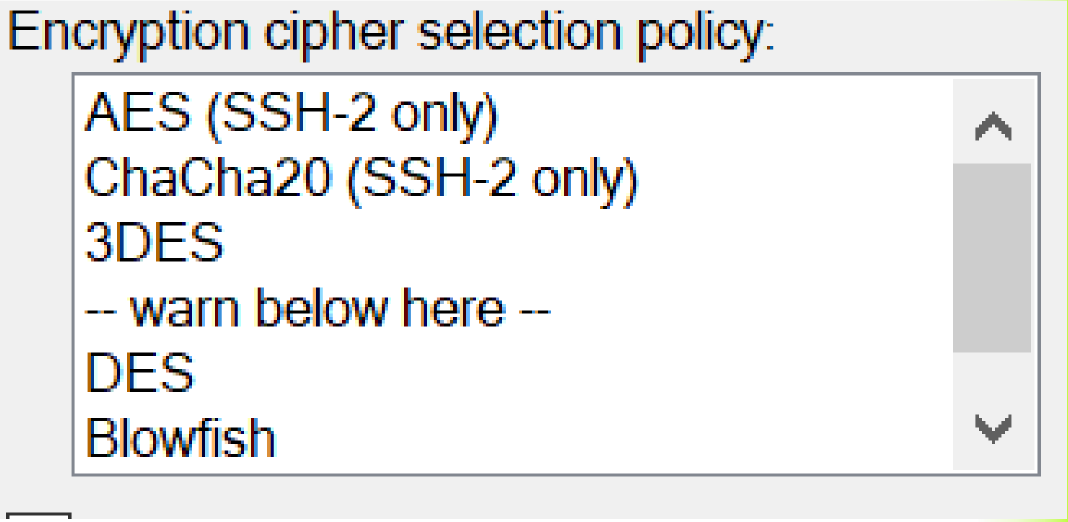
ASCII Code Chart

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

- Can we modify it for „personal” use?
  - Why not?- Thus we define – Enryption table

Symmetric– Assymmetric encrytion

- How can we define a new encryption method?-We have a lot of methods!
- Most simple way: modified code table (e.g. based on ascii)
- A little bit smarter method, eg. Based on a book, sending numbers, and these numbers defines chars, page, row char number, define a real char.
- Today more general is defining a math method, based on a common key.
- Simplest method: XOR
- All previous methods are symmetric
  - Only one key
- Assymetric – 2 keys.



Terminal connection – What is it used?

- Windows Terminal
  - Users\.ssh\known_hosts file store the well known host keys
  - The PUTTY Registry key: HKCU\Software\SimonTatham\PuTTY
  - How to modify?
    - Regedit
    - PS

The registry HKCU key

Administrator: Windows PowerS | OS

```
PS HKCU:\Software\SimonTatham\PuTTY> (Get-ItemProperty .\SshHostKeys)["rsa2@22:os.inf.elte.hu"]
PS HKCU:\Software\SimonTatham\PuTTY> (Get-ItemProperty .\SshHostKeys)."rsa2@22:os.inf.elte.hu"
0x10001,0xc448b7bace9c9d856505d366991cf2a0271f480e04c3e2447276cb15f9b996a6601651ae5c4d4a90fcf6e0400da3353a051b9f9f2b807a
b7dfd203a400c1dacc13c1ac85055a7f1c97594df6f561444e25b42ab37514bfa58c06504cc447ec09b06ebe59f5ce990ba8140bec61ebf5aeacdf96
c6d8720a73ec736b297b67631fd52be4d6c5a571956b307f795dba8b21da996e313edc507495453628d5ab661fe213571b4c6c86eebd2339d99ad86e
ecf22e42d073d378dd07aa4d95867bea6ed888b517099a58f67bec8bf6af59bf2d6a24cd0ac55844881f19759f1cf6eba4628bdc19a97a5261d4fbfe
b915dee9992c72e04a028b69cf0af56c4cd624f0e9
PS HKCU:\Software\SimonTatham\PuTTY> Remove-ItemProperty .\SshHostKeys "rsa2@22:os.inf.elte.hu"
PS HKCU:\Software\SimonTatham\PuTTY> Get-ItemProperty .\SshHostKeys "rsa2@22:rtos.inf.elte.hu"


rsa2@22:rtos.inf.elte.hu : 0x10001,0xabb89dd2ee61a5443dacd4ce25e5bec57053568d6c991d896ea19dc506299ebfb442c7f64200c94d6a
                           2622efa688475355898b5485e3a74e12dd12677f00adf7c6e31643e139cb4aefae1a13263f592b5bc98d5a6ab309
                           423dd13cf1b62d3afac687918c50a4705dbd5020536ee01546fd82981ef0a0c6e44bed805ce6d9b78006856e0426
                           382752e41a19399f16ccf40df44d54375bd080822872dfe7f66c5352b08c60076504f557d746c934e10f354c525f
                           0a6ce588949209bc6a118b102836b46cb7ec714b564e2cea814b0fb1ee86869f85ea55d0d6eb9a5b86cf6037a98b
                           07bfb2ecebfad95120dbf677d86a275bebc84eb8e52e206c117b7db00adf91
PSPath                   : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\SshHostKeys
PSParentPath             : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\SimonTatham\PuTTY
PSChildName              : SshHostKeys
PSDrive                  : HKCU
PSProvider               : Microsoft.PowerShell.Core\Registry
```

ELTE INFORMATIKA

Are we safe? Who guards us?

RSA algorithm

or: in everyday life, we don't just use addition from maths lessons

(eg: in shops, cassa)

Divisibility

What is the common?

4; 7; 10; 13; 16; 19; 22 — Mod 3, the remaining is 1

14; 5; 17; 8; 11; 20; 23 — Mod 3, the remaining is 2

3; 66; 9; 12; 135; 18; 6 — Mod 3, the remaining is 0

Residual class - maradékosztályok

Definition:

$$a, b \in N \qquad a \mid b \quad \Leftrightarrow \quad \exists x \in N \ni \quad a \cdot x = b$$

for natural numbers a,b, we say that a is the divisor of b (or b is divisible by a) if there is a natural number x such that a.x=b

Residual class numbers - Maradékosztályok

Check residual classes!

a) 5; 8; 11; 14; 17; 20; 23

b) 4; 7; 10; 13; 16; 19; 22

c) 3; 66; 9; 12; 135; 18; 6

$$8-5=3$$
$$11-8=3$$
$$17-8=9$$

$$7-4=3$$
$$10-4=6$$
$$19-7=12$$

$$6-3=3$$
$$12-6=6$$
$$18-6=12$$

Example:

19 ≡ 7 mod 3

They are in the same residual class mod 3

Def.: If the integer m (≠0) divides the difference a-b, then we say that the number a is congruent to b modulo m (→ they are in the same residue class mod m)

Jelölés: ***a≡b mod m***

Congruency properties

1. $a \equiv b \bmod m \quad \Rightarrow \quad b \equiv a \bmod m \quad \textit{és} \quad a - b \equiv 0 \bmod m$
2. $a \equiv b \bmod m \quad \textit{és} \quad b \equiv c \bmod m \quad \Rightarrow \quad a \equiv c \bmod m$
3. $a \equiv b \bmod m \quad \textit{és} \quad c \equiv d \bmod m \quad \Rightarrow \quad a \cdot x + c \cdot y \equiv b \cdot x + d \cdot y \bmod m$
4. $a \equiv b \bmod m \quad \textit{és} \quad c \equiv d \bmod m \quad \Rightarrow \quad a \cdot c \equiv b \cdot d \bmod m$
5. $a \equiv b \bmod m \quad \textit{és} \quad d \mid m \quad \textit{és} \quad d > 0 \quad \Rightarrow \quad a \equiv b \bmod d$
6. f *egész együtthatós polinom és* $a \equiv b \bmod m \Rightarrow f(a) \equiv f(b) \bmod m$
7. *ha* $(a;m) = 1$ *akkor*: $a \cdot x \equiv a \cdot y \bmod m \quad \Leftrightarrow \quad x \equiv y \bmod m$

with a relative prime to m we can multiply, divide

$$4.\textit{tul.} \quad \Rightarrow \quad a \equiv b \bmod m \quad \textit{és} \quad a \equiv b \bmod m \quad \Rightarrow \quad a^2 \equiv b^2 \bmod m$$

$$\Rightarrow \quad \ldots \quad \Rightarrow \quad a^n \equiv b^n \bmod m$$

We can power (multiply) the kongruenci!

Maybe later we need it

They are not in the same residual class generally.

$$\textit{Állítás}:$$

$$\textit{legyen} \quad (a;m)=1 \quad \textit{és} \quad (x;m)=1 \quad \textit{és} \quad (y;m)=1$$

$$\textit{továbbá} \quad x \not\equiv y \bmod m \quad \Rightarrow \quad a \cdot x \not\equiv a \cdot y \bmod m$$

$$\textit{Bizonyítás}:$$

$$x \not\equiv y \bmod m \quad \textit{jelenti}: \quad m \nmid (x-y)$$

$$\textit{ekkor}: \quad m \nmid a \cdot (x-y) = a \cdot x - a \cdot y, \quad \textit{tehát}$$

$$a \cdot x \not\equiv a \cdot y \bmod m$$

If two numbers are not congruent, then multiplying them by a relative prime of m, they will still not be congruent!

Residual systems

0 1 2

Look these numbers: 3; 4; 5

0 1 2

Other one: 33; 16; 26

They give a full residual system based on mod 3!

Def: $x_1; x_2; \ldots\ x_m$ <u>teljes maradékrendszer</u> *mod m*, ha tetszőleges ***y*** egész számhoz pontosan egy olyan x_j található, amelyre ***y*** $\equiv x_j$ *mod m*

φ function- definition

Euler φ function: ***φ(m)*** number of prime positive integers not greater than m, relative to m

Example: m= 24 relative primes to m:1; 5; 7; 11; 13; 17; 19; 23

φ(24) = 8

m = 7 relative prímes to 7: 1; 2; 3; 4; 5; 6

φ(7) = 6

Reduced residue system mod 24

How many φ(11), φ(13), φ(23) (10, 12, 22)
?

Important! If ***p*** prime, then ***φ(p) = p - 1***

<u>Reduced residue system: from the total residue system, only those elements are left that are primes relative to m</u>

E L T E I N F O R M A T I K A

A small task

Let $m = p_1 \cdot p_2$ $\qquad\qquad$ $\varphi(m) = ?$

m= 15 = 3 · 5 $\qquad$ to 15 relatív prímes: 1; 2; 4; 7; 8; 11; 13; 14

$\varphi(15) = 8$

$\varphi(3) = 2$; $\varphi(5) = 4$ *és* $2 \cdot 4 = 8$ $\qquad$ *Coincident?*

Lemma: $\boldsymbol{\varphi(m) = (p_1 - 1) \cdot (p_2 - 1)}$

$$\varphi(m) = (p_1 - 1) \cdot (p_2 - 1) = p_1 \cdot p_2 - p_1 - p_2 + 1$$

From p1.p2 we subtract a multiple of p1 of p2 and a multiple of p2 of p1, but we subtract p1.p2 twice.

Euler lemma

$$Tétel: \quad ha \quad (a;m)=1, \quad akkor \quad a^{\varphi(m)} \equiv 1 \quad \mathrm{mod}\, m$$

Biz.:

$$r_1;\, r_2;\quad \dots r_{\varphi(m)} \qquad \textit{redukált maradék rendszer}\ \mathrm{mod}\, m$$

$$a\cdot r_1;\, a\cdot r_2;\quad \dots a\cdot r_{\varphi(m)} \qquad \textit{is redukált maradék rendszer}\ \mathrm{mod}\, m$$

$$(\textit{ugyan annyi elem van itt is, ott is, ill. itt van szükség a tételre!})$$

$$r_j \equiv a\cdot r_k \quad \mathrm{mod}\, m$$

$$r_1\cdot r_2\cdot\quad \dots\cdot r_{\varphi(m)} \equiv a\cdot r_1\cdot a\cdot r_2\cdot\quad \dots\cdot a\cdot r_{\varphi(m)} \quad \mathrm{mod}\, m \quad (4.\, tul.)$$

$$1 \equiv a^{\varphi(m)} \quad \mathrm{mod}\, m \quad (7.\, tul.\, alapján,\, mert \quad (r_i;m)=1)$$

$$m=24 \qquad \Rightarrow \qquad 1, 5, 7, 11, 13, 17, 19, 23$$

$$\varphi(24)=8$$

$$(24;7)=1 \qquad \Rightarrow \qquad 7, 35, 49, 77, 91, 119, 133, 161$$

Fermat lemma

$$p \ \text{prím és} \quad (a;p)=1 \quad \Rightarrow \quad a^{p-1} \equiv 1 \quad \text{mod } p$$

$$\Rightarrow \quad a^{p} \quad \equiv a \quad \text{mod } p$$

Proof.: This comes from Euler lemma

This means that if a < p, then if a is raised to the pth power and then divided by p, the remainder of the division is exactly a.

ELTE INFORMATIKA

Lets join lemmas!

$$m := p_1 \cdot p_2 \quad ekkor \quad \varphi(m) = (p_1 - 1)\cdot(p_2 - 1)$$

$$(a;m) = 1$$

$$a^{\varphi(m)} \equiv 1 \quad \Rightarrow \quad a^{(p_1-1)\cdot(p_2-1)} \equiv 1 \quad \mod m$$

$$a^{\varphi(m)+1} \equiv a \Rightarrow \quad a^{(p_1-1)\cdot(p_2-1)+1} \equiv a \quad \mod m$$

$$b \in Z \quad esetén:$$

$$\left(a^{\varphi(m)}\right)^b \equiv 1^b = 1 \quad \Rightarrow \quad a^{b\cdot(p_1-1)\cdot(p_2-1)} \equiv 1 \quad \mod m$$

$$a^{b\cdot\varphi(m)+1} \equiv a \quad \Rightarrow \quad a^{b\cdot(p_1-1)\cdot(p_2-1)+1} \equiv a \quad \mod m$$

$$4.tul. \quad \Rightarrow \quad a \equiv b \mod m \quad \Rightarrow \quad a^n \equiv b^n \mod m$$

Continue:

$$m := p_1 \cdot p_2 \quad ekkor \quad \varphi(m) = (p_1 - 1)\cdot(p_2 - 1)$$

$$(a;m) = 1, \quad b \in Z \quad esetén \quad a^{b\cdot\varphi(m)+1} \equiv a \bmod m$$

$$b \cdot \varphi(m) + 1 := \alpha \cdot \beta, \quad ahol \quad \alpha, \beta \in N$$

$$a^{\alpha\cdot\beta} = \left(a^{\alpha}\right)^{\beta} \equiv a \bmod m$$

By property 2, I can replace a^{α} by any number congruent to it mod m in the calculation

(α,m), (***β*,m)** are the keys and a is the number to be encrypted (relative prime to m)!

Lets use this method!

$$m := 3 \cdot 5 = 15$$

$$(a;m) = 1 \quad és \quad a < m \quad \Rightarrow \quad a \in \{1;\, 2;\, 4;\, 7;\, 8;\, 11;\, 13;\, 14\}$$

$$\varphi(m) = 8$$

$\varphi(m) + 1 = 9 = 3 \cdot 3$ Nem jó, ugyan az lenne a titkos és a nyilvános kulcs

$2 \cdot \varphi(m) + 1 = 17$ Nem jó, mert prím

$3 \cdot \varphi(m) + 1 = 25 = 5 \cdot 5$ Ez sem jó!

$4 \cdot \varphi(m) + 1 = 33 = 3 \cdot 11$ Végre!

Example, lets encrypt!

Public key: (11;15)

Private key: (3;15)

Do not forget, we can encrypt numbers: $a \in \{1; 2; 4; 7; 8; 11; 13; 14\}$

Encrypt these numbers: 2 4 8 7

Coding

Numbers to encrypt: 2 4 8 7

Public key: (11;15)

$$2^{11} = 2048 = 136 \cdot 15 + 8$$

$$4^{11} = 4\,194\,304 = 279\,620 \cdot 15 + 4$$

$$8^{11} = 8\,589\,934\,592 = 572\,662\,306 \cdot 15 + 2$$

$$7^{11} = 1\,977\,326\,743 = 131\,821\,782 \cdot 15 + 13$$

Result: 8 4 2 13

Decrypting:

Secret, encrypted message: 8 4 2 13

Private key: (3;15)

$$8^3 = 512 = 34 \cdot 15 + 2$$

$$4^3 = 64 = 4 \cdot 15 + 4$$

$$2^3 = 8 = 0 \cdot 15 + 8$$

$$13^3 = 2197 = 146 \cdot 15 + 7$$

So, we got back the original numbers: 2 4 8 7

What is the message!

Codetable:

1	A
2	E
3	É
4	G
5	K
6	R
7	S
8	T
9	Z
10	?

Private key: (7;187) (We have to decrypt with this one.)

RSA encrypted message:

83; 162; 83; 46; 36; 162; 83; 83; 175

162; 64; 181; 46; 36; 46; 181; 64; 162; 83; 162; 180; 150; 162

What is the public key?(We coded with public key!)

- Small help for public key.
  - (7,187)
  - (23,187)

$$187 = 17 \cdot 11$$

$$\varphi(187) + 1 = 16 \cdot 10 + 1 = 161$$

$$161 = 7 \cdot 23$$

$$2 \cdot \varphi(187) + 1 = 2 \cdot 16 \cdot 10 + 1 = 321$$

$$321 = 3 \cdot 107$$

$$3 \cdot \varphi(187) + 1 = 3 \cdot 16 \cdot 10 + 1 = 481$$

$$481 = 13 \cdot 37$$

$$4 \cdot \varphi(187) + 1 = 4 \cdot 16 \cdot 10 + 1 = 641$$

$$641 = prím$$

Can you it crack? – Using small numbers…yes

$m = 15 \qquad \alpha = 11 \quad \beta = ?$

$15 = 3 \cdot 5$

$\varphi(15) = 2 \cdot 4 = 8 \qquad b \cdot 8 + 1 = 11 \cdot \beta$

After a short probe: $b = 4 \quad \beta = 3$

$m = 527 \qquad \alpha = 13 \quad \beta = ?$

$527 = 17 \cdot 31 \qquad \varphi(527) = 16 \cdot 30 = 480 \qquad b \cdot 480 + 1 = 13 \cdot \beta$

After a short probe: $b = 1 \quad \beta = 37$

Can you crack it?

- M = P1 * P2 – P1,P2 1024, 2048 bits

$$m := p_1 \cdot p_2 \quad ekkor \quad \varphi(m) = (p_1 - 1)\cdot(p_2 - 1)$$

$$(a;m) = 1, \quad b \in Z \quad esetén \quad a^{b\cdot\varphi(m)+1} \equiv a \bmod m$$

$$b \cdot \varphi(m) + 1 := \alpha \cdot \beta, \quad ahol \quad \alpha, \beta \in N$$

$$a^{\alpha\cdot\beta} = \left(a^{\alpha}\right)^{\beta} \equiv a \bmod m$$

***(α**,m), **(β,m)** are the keys and a is the number to be encrypted (relative prime to m)!*

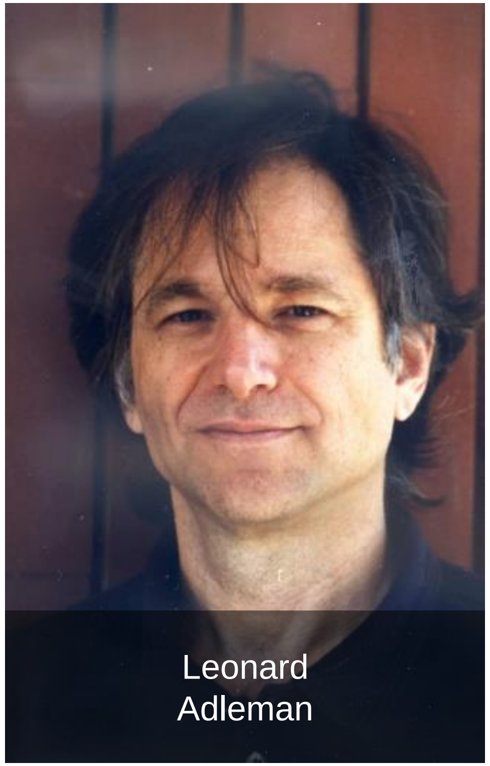
- The methoh is simple, but it need huge compute capacity, years.

ELTE INFORMATIKA

What the name means - RSA


Ronald L. Rivest


Adi
Shamir


Leonard
Adleman

ELTE INFORMATIKA

Thank you!