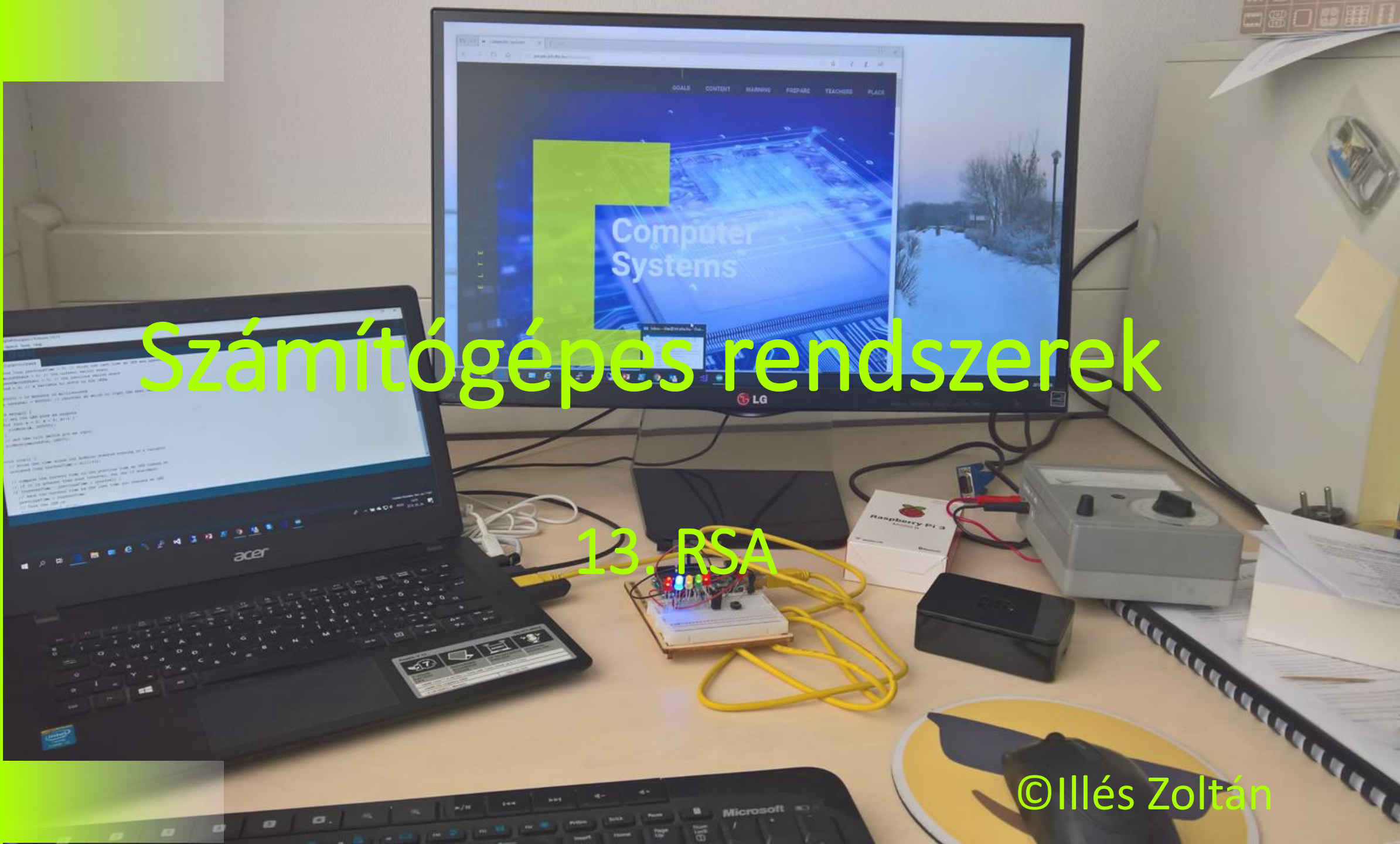
ELTE INFORMATIKA

Számítógépes rendszerek

13. RSA



Visszatekintés

- Számítógépek, számábrázolás, kódolás,felépítés, fájlrendszerek
- Alapvető parancsok, folyamatok előtérben, háttérben
- I/O átirányítás, szűrők,reguláris kifejezések
- Változó, parancs behelyettesítés,aritmetikai, logikai kifejezések
- Script vezérlési szerkezetek,Sed,AWK
- Hálózatok jellemzői
- Powershell

Mi jön ma?

- Kódolás – Titkosítás
- Szimmetrikus – Aszimmetrikus titkosítás
- Terminál kapcsolódás
  - Windows Terminál – SSH
  - PUTTY - SSH
- RSA – Egyszerűen

Kódolás - Titkosítás

- Fontos: A számítógép (jelenleg) csak számokat tárol a memóriában!
- Ahhoz, hogy szöveget kapjunk, kódtáblára van szükség. PL. ASCII
  - 41h(65) -> A, 4Ch(76) ->L, 4Dh(77) -> M, 41h(65) -> A
- Amíg általános kódtáblákat használunk, egyszerű szöveges ábrázolásról van szó.
- Ha módosított, speciális kódtábláról, akkor titkosításról beszélünk.

Alap ASCII kódtábla

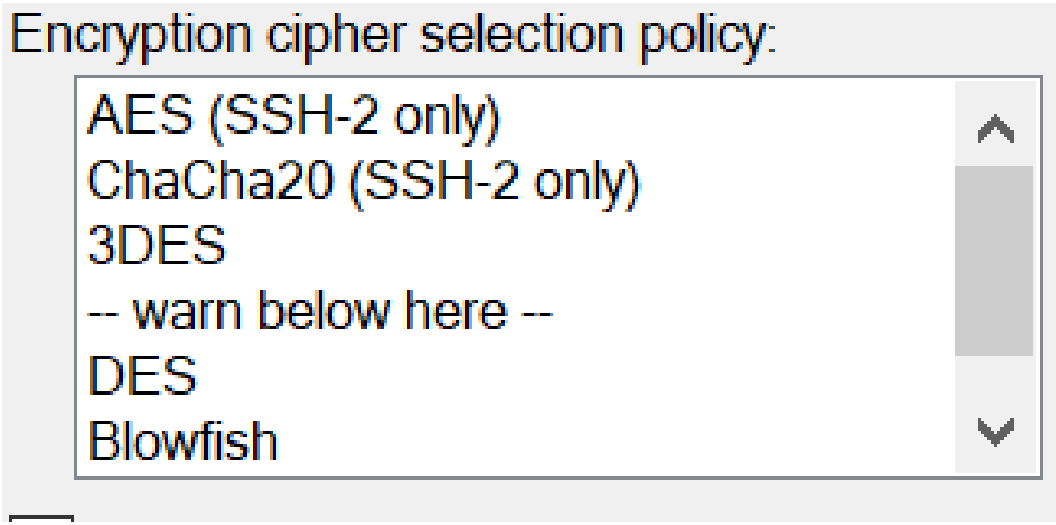
ASCII Code Chart

	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

- Módosítható ez „saját használatra”?
  - Miért ne?- Ekkor nem kódolás - Titkosítás

Szimmetrikus – Aszimmetrikus titkosítás

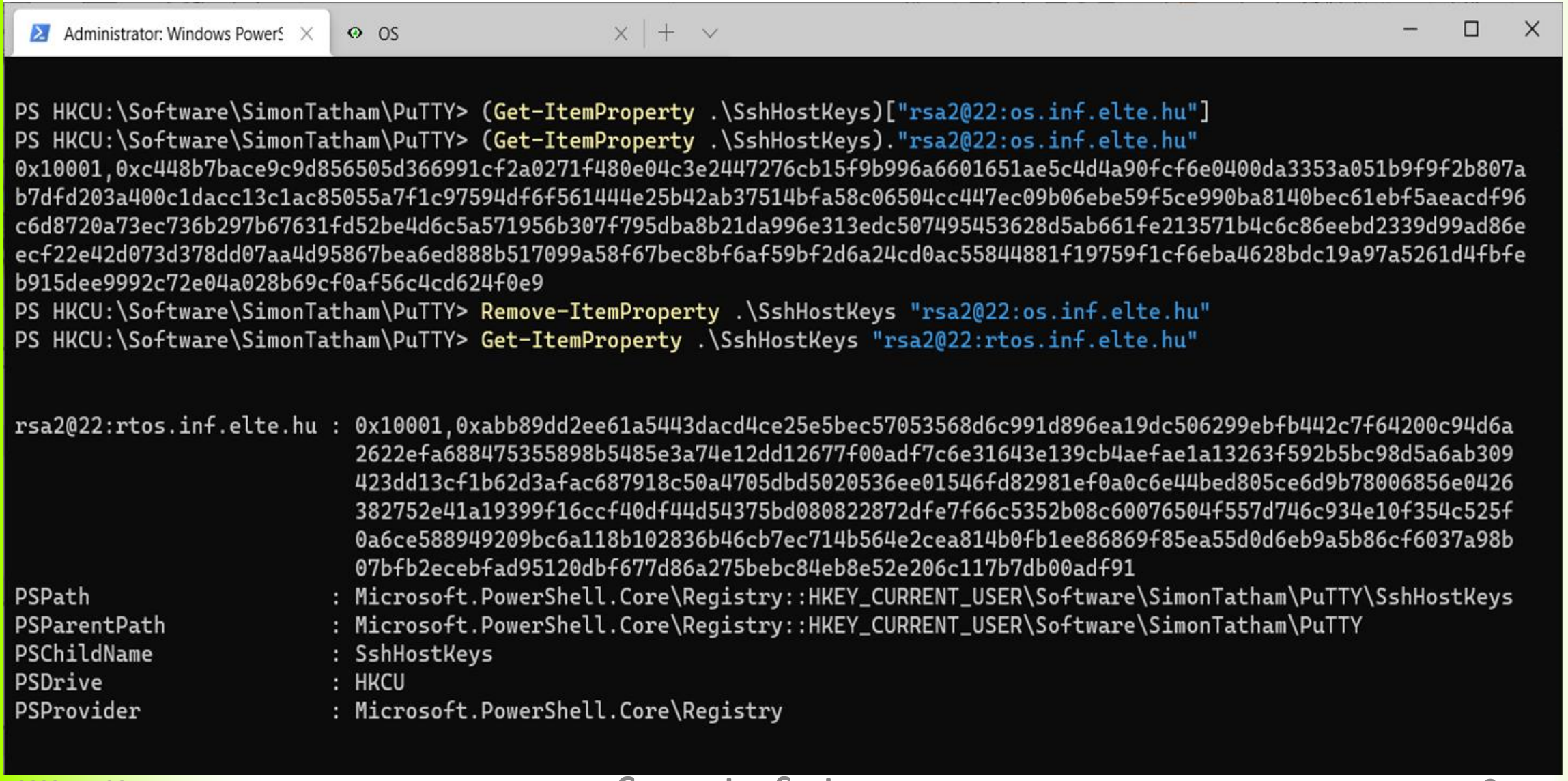
- Hogyan hozhatunk létre speciális kódtáblákat?- Sokféle módszer ismert
- Legegyszerűbb változat: módosított karakter tábla
- Kicsit rafináltabb, pl. megadott könyv alapján, a küldött számsorozat megadja a könyv karaktereit, ami lesz a valódi üzenet.
- Ma általánosan elterjedt, egy kulcs alapján valamilyen matematikai módszert használva
- Legegyszerűbb: XOR
- Mind szimmetrikus –egy kulcs
- Aszimmetrikus – 2 kulcs.



Terminál kapcsolat – Mit használ?

- Windows Terminal
  - Users\.ssh\known_hosts tárolja az ismert host kulcsokat
  - PUTTY: Registry: HKCU\Software\SimonTatham\PuTTY
    - Módosítás
    - Regedit vagy
    - PS

Registry HKCU kulcs



ELTE INFORMATIKA

Mitől vagyunk biztonságban?

RSA algoritmus

avagy: a mindennapok során sem csak az összeadást használjuk a matematika órán tanultakból

(lásd: boltban, pénztárnál)

Oszthatóság

Mi a közös bennük?

4; 7; 10; 13; 16; 19; 22 — 3-mal osztva 1 a maradék

14; 5; 17; 8; 11; 20; 23 — 3-mal osztva 2 a maradék

3; 66; 9; 12; 135; 18; 6 — 3-mal osztva 0 a maradék

maradékosztályok

Oszthatóság definíciója:

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

a,b természetes számok esetén azt mondjuk, hogy az ***a*** osztója a ***b***-nek (vagy ***b*** osztható ***a***-val), ha található olyan ***x*** természetes szám, hogy ***a·x=b***

Maradékosztályok

Vizsgáljuk meg a maradékosztályokat!

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

$8-5=3$

$11-8=3$

$17-8=9$

$7-4=3$

$10-4=6$

$19-7=12$

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

$6-3=3$

$12-6=6$

$18-6=12$

Tehát például:

19 ≡ 7 mod 3

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

Vagyis ugyan abban a maradékosztályban vannak mod 3

Def.: Ha az ***m*** (≠0) egész osztja az ***a-b*** különbséget, akkor azt mondjuk, hogy az ***a*** szám **kongruens** ***b***-vel modulo ***m*** *(→ ugyan abban a maradékosztályban vannak mod m)*

Jelölés: ***a≡b mod m***

Kongruencia tulajdonságai

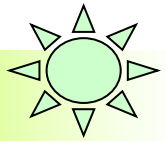
1. $a \equiv b \bmod m \quad \Rightarrow \quad b \equiv a \bmod m \quad \text{és} \quad a - b \equiv 0 \bmod m$
2. $a \equiv b \bmod m \quad \text{és} \quad b \equiv c \bmod m \quad \Rightarrow \quad a \equiv c \bmod m$
3. $a \equiv b \bmod m \quad \text{és} \quad c \equiv d \bmod m \quad \Rightarrow \quad a \cdot x + c \cdot y \equiv b \cdot x + d \cdot y \bmod m$
4. $a \equiv b \bmod m \quad \text{és} \quad c \equiv d \bmod m \quad \Rightarrow \quad a \cdot c \equiv b \cdot d \bmod m$
5. $a \equiv b \bmod m \quad \text{és} \quad d \mid m \quad \text{és} \quad d > 0 \quad \Rightarrow \quad a \equiv b \bmod d$
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 :* $a \cdot x \equiv a \cdot y \bmod m \quad \Leftrightarrow \quad x \equiv y \bmod m$

m-hez relatív prímmel szorozhatok, oszthatok

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

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

Hatványozhatom a kongruenciát!



Később még szükség lehet rá ☺

Ezek nem feltétlenül vannak ugyanabban a maradékosztályban

Állítás:

legyen $(a;m)=1$ *és* $(x;m)=1$ *és* $(y;m)=1$

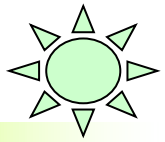
továbbá $x \not\equiv y \bmod m \Rightarrow a \cdot x \not\equiv a \cdot y \bmod m$

Bizonyítás:

$x \not\equiv y \bmod m$ *jelenti*: $m \nmid (x-y)$

ekkor: $m \nmid a \cdot (x-y) = a \cdot x - a \cdot y$, *tehát*

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



Ha két szám nem kongruens egymással, akkor m-hez relatív prímmel szorozva őket, továbbra sem lesznek egymással kongruensek!

Maradékrendszerek

Nézzük a következő számokat: 3; 4; 5

Egy másik számhármas: 33; 16; 26

Ezek a számok teljes maradékrendszert alkotnak mod 3

Def: $x_1; x_2; \ldots x_m$ teljes maradékrendszer *mod m*, ha tetszőleges ***y*** egész számhoz pontosan egy olyan x_j található, amelyre $\boldsymbol{y} \equiv x_j \ \textit{mod m}$

φ függvény

Euler-féle φ függvény: ***φ(m)*** az ***m***-nél nem nagyobb, ***m***-hez relatív prím pozitív egészek száma

Például: m = 24 hozzá relatív prímek: 1; 5; 7; 11; 13; 17; 19; 23

φ(24) = 8

m = 7 hozzá relatív prímek: 1; 2; 3; 4; 5; 6

φ(7) = 6

redukált maradékrendszer mod 24

Mennyi φ(11), φ(13), φ(23) ? (10, 12, 22)

Fontos! Ha ***p*** prím, akkor ***φ(p) = p - 1***

Redukált maradékrendszer: a teljes maradékrendszerből csak azokat az elemeket hagyjuk meg, amelyek ***m***-hez relatív prímek

Egy kis feladat

Legyen $m = p_1 \cdot p_2$ $\varphi(m) = ?$

m= 15 = 3 · 5 hozzá relatív prímek: 1; 2; 4; 7; 8; 11; 13; 14

$\varphi(15) = 8$

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

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

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

$p_1 \cdot p_2$ db számból p_1 db p_2 többszörösét és p_2 db p_1 többszörösét vonjuk ki, de a $p_1 \cdot p_2$ -t így kétszer is kivontuk.

Euler tétele

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

Biz.:

$r_1; r_2; \ \ldots r_{\varphi(m)}$ *redukált maradék rendszer* mod m

$a \cdot r_1; a \cdot r_2; \ \ldots a \cdot r_{\varphi(m)}$ *is redukált maradék rendszer* mod m

(*ugyan annyi elem van itt is, ott is, ill. itt van szükség a tételre*!)

$r_j \equiv a \cdot r_k \mod m$

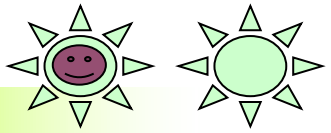
$r_1 \cdot r_2 \cdot \ \ldots \cdot r_{\varphi(m)} \equiv a \cdot r_1 \cdot a \cdot r_2 \cdot \ \ldots \cdot a \cdot r_{\varphi(m)} \mod m$ (4. *tul.*)

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

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

$\varphi(24) = 8$

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



ELTE INFORMATIKA

Fermat tétele

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

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

Biz.: Az előző tétel következménye

Eszerint ha ***a < p***, akkor ha ***a***-t ***p***-edik hatványra emeljük, majd a kapott értéket elosztjuk ***p***-vel, az osztási maradékként éppen ***a***-t kapjuk vissza.

Egyesítsük a tételeket!

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

$$(a;m) = 1$$

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

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

$b \in Z \quad esetén:$

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

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

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

Folytatás

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

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

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

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

2. tulajdonság alapján a^{α} helyett bármilyen vele mod m kongruens számot is írhatok a számolás során

(α,m), (***β,m)*** lesznek a kulcsok, ***a*** pedig a titkosítandó szám (relatív prím m-hez)!

Alkalmazzuk az eddigieket!

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

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

$$\varphi(m) = 8$$

$\varphi(m) + 1 = 9 = 3 \cdot 3$ 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!

Titkosítsunk!

Legyen a nyilvános kulcs: (11;15)

Ekkor a titkos kulcs: (3;15)

Ne felejtsük el: $a \in \{1; 2; 4; 7; 8; 11; 13; 14\}$

Például a titkosítandó számsor: 2 4 8 7

Kódolás

A titkosítandó szám: 2 4 8 7

A nyilvános kulcs: (11;15)

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

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

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

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

Az eredmény: 8 4 2 13

Dekódolás:

A titkos üzenet: 8 4 2 13

A titkos kulcs: (3;15)

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

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

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

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

Tehát az eredeti üzenetet visszakaptuk: 2 4 8 7

Fejtsétek meg!

Kódtáblázat:

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

Privát kulcs: (7;187) (Ezzel dekódolunk!)

RSA kódolt üzenet:

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

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

Mi lehet a publikus kulcs?(Ezzel kódoltunk!)

- Kis segítség
  - (7,187)
  - (23,187)

$$187 = 17 \cdot 11$$

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

$$161 = 7 \cdot 23$$

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

$$321 = 3 \cdot 107$$

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

$$481 = 13 \cdot 37$$

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

$$641 = \textit{prím}$$

Feltörhető? – Kis számok esetén...igen

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

$15 = 3 \cdot 5$

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

Rövid próbálgatás után: $b = 4 \quad \beta = 3$

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

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

Rövid próbálgatás után: $b = 1 \quad \beta = 37$

Feltörhető?

- M = P1 * P2 – P1,P2 1024, 2048 bites

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

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

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

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

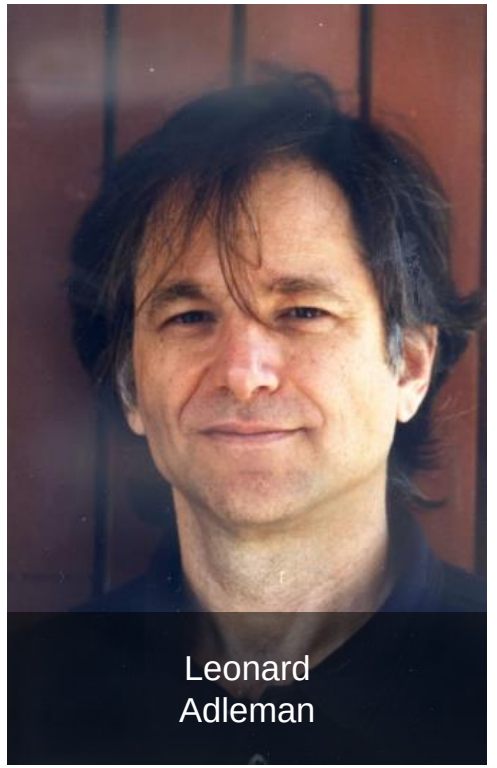
(α,m), (*β**,m)* lesznek a kulcsok, ***a*** pedig a titkosítandó szám (relatív prím m-hez)!

- A módszer egyszerű, de a számolásigény óriási, évek.

Mit jelent az elnevezés? - RSA


Ronald L. Rivest


Adi
Shamir


Leonard
Adleman

ELTE INFORMATIKA

Köszönöm a figyelmet!

©Illés Zoltán