

Számítógépes rendszerek

13. RSA

©Illés Zoltán

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.

Encryption cipher selection policy:

AES (SSH-2 only)
ChaCha20 (SSH-2 only)
3DES
-- warn below here --
DES
Blowfish

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

```

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 : 0x10001,0xab89dd2ee61a5443dacd4ce25e5bec57053568d6c991d896ea19dc506299ebfb442c7f64200c94d6a
2622efa688475355898b5485e3a74e12dd12677f00adf7c6e31643e139cb4aefae1a13263f592b5bc98d5a6ab309
423dd13cf1b62d3afac687918c50a4705dbd5020536ee01546fd82981ef0a0c6e44bed805ce6d9b78006856e0426
382752e41a19399f16ccf40df44d54375bd080822872dfe7f66c5352b08c60076504f557d746c934e10f354c525f
0a6ce588949209bc6a118b102836b46cb7ec714b564e2cea814b0fb1ee86869f85ea55d0d6eb9a5b86cf6037a98b
07bfb2ecebfa95120dbf677d86a275bebc84eb8e52e206c117b7db00adf91
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

```


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

Oszthatóság definíciója:

$$a, b \in \mathbb{N} \quad a|b \Leftrightarrow \exists x \in \mathbb{N} \ni a \cdot x = b$$

maradékosztályok

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:

$$19 \equiv 7 \pmod{3}$$

c) 3; 6; 9; 12; 15; 18; 21

Vagyis ugyan abban a maradékosztályban vannak mod 3

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

Jelölés: **$a \equiv b \pmod{m}$**

Kongruencia tulajdonságai

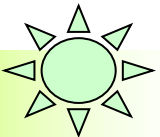
1. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ és $a - b \equiv 0 \pmod{m}$
2. $a \equiv b \pmod{m}$ és $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$
3. $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m} \Rightarrow a \cdot x + c \cdot y \equiv b \cdot x + d \cdot y \pmod{m}$
4. $a \equiv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

m-hez relatív prímmel szorozhatók, oszthatók

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

$$\Rightarrow \dots \Rightarrow a^n \equiv b^n \pmod{m}$$

Hatványozhatom a kongruenciát!



Később még szükség lehet rá ☺

Állítás:

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

továbbá $x \not\equiv y \pmod{m} \Rightarrow a \cdot x \not\equiv a \cdot y \pmod{m}$

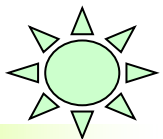
Bizonyítás:

$x \not\equiv y \pmod{m}$ jelenti: $m \nmid (x - y)$

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

$a \cdot x \not\equiv a \cdot y \pmod{m}$

Ezek nem feltétlenül
vannak ugyanabban
a maradékosztályban



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 számhármast: 33; 16; 26



Ezek a számok teljes maradékrendszert alkotnak mod 3

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

φ függvény

Euler-féle φ függvény: $\varphi(m)$ 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

$$\varphi(24) = 8$$

$m = 7$

hozzá relatív prímek: 1; 2; 3; 4; 5; 6

$$\varphi(7) = 6$$

Mennyi $\varphi(11)$, $\varphi(13)$, $\varphi(23)$? (10, 12, 22)

redukált maradékrendszer
mod 24

Fontos! Ha p prím, akkor $\varphi(p) = p - 1$

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

Egy kis feladat

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

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

$$\varphi(15) = 8$$

$$\varphi(3) = 2 \ ; \ \varphi(5) = 4 \quad \text{és} \quad 2 \cdot 4 = 8 \quad \text{Véletlen?}$$

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

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

Biz.:

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

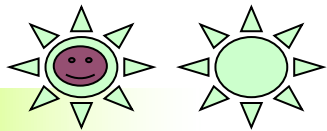
$a \cdot r_1; a \cdot r_2; \dots a \cdot r_{\varphi(m)}$ is redukált maradék rendszer mod m

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

$$r_j \equiv a \cdot r_k \pmod{m}$$

$$r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \equiv a \cdot r_1 \cdot a \cdot r_2 \cdot \dots \cdot a \cdot r_{\varphi(m)} \pmod{m} \quad (4. \text{ tul.})$$

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



$$\begin{array}{ll}
 m = 24 & \Rightarrow 1, 5, 7, 11, 13, 17, 19, 23 \\
 \varphi(24) = 8 & \\
 (24; 7) = 1 & \Rightarrow 7, 35, 49, 77, 91, 119, 133, 161
 \end{array}$$

Fermat tétele

$$\begin{aligned} p \text{ prím és } (a; p) = 1 &\Rightarrow a^{p-1} \equiv 1 \pmod{p} \\ &\Rightarrow a^p \equiv a \pmod{p} \end{aligned}$$

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!

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

$$(a; m) = 1$$

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

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

$b \in \mathbb{Z}$ esetén:

$$(a^{\varphi(m)})^b \equiv 1^b = 1 \Rightarrow a^{b \cdot (p_1-1) \cdot (p_2-1)} \equiv 1 \pmod{m}$$

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

$$4.tul. \Rightarrow a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$$

Folytatás

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

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

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

$$a^{\alpha \cdot \beta} = (a^\alpha)^\beta \equiv a \pmod{m}$$

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

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

$$15 = 3 \cdot 5$$

$$\varphi(15) = 2 \cdot 4 = 8$$

$$b \cdot 8 + 1 = 11 \cdot \beta$$

Rövid próbálgatás után:

$$b = 4 \quad \beta = 3$$

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

$$527 = 17 \cdot 31$$

$$\varphi(527) = 16 \cdot 30 = 480$$

$$b \cdot 480 + 1 = 13 \cdot \beta$$

Rövid próbálgatás után:

$$b = 1 \quad \beta = 37$$

Feltörhető?

- $M = P_1 * P_2$ – P_1, P_2 1024, 2048 bites

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

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

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

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

(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



Köszönöm a figyelmet!

©Illés Zoltán

