file: RSA-diak.tex, 2005.04.28

Szalkai István: RSA - titkosírás feladatok

Jelölések

.

$p, q \in \mathbb{P}$ prímszámok, $n = p \bullet q$,
$s = \varphi(n) = (p-1) \bullet (q-1)$,
$ef \equiv 1 \pmod{s}$ ahol e a nyilvános és f a titkos kulcs.

A használt ABC -k: 00 = szóköz mindig, a rövid üzenetek *elejét* 0-val töltjük fel.
Sajnos a különböző példák különböző ABC -ket használnak, ezért a Függelékben megadjuk a használt ABC -ket, valamint minden feladatban megadjuk a példában használt ABC betűszámát (26, 30 vagy 35).

Feladatok

.

0) Faktorizáljuk az alábbi számokat:
a) $n = 440\,747$,
b) $n = 2\,347\,589$,
c) $n = 97\,189\,241$,
d) $n = 17\,967\,876\,255\,379$,
e) $n = 444\,113\,096\,135\,661\,846\,937$

1) a) Kódolja a ”Wir treffen uns am Samstag” [*Találkozzunk szombaton*] üzenetet, ha $n = 55$ és $e = 27$ (26 betűs ABC).
b) Dekódolja a 24, 14, 34, 51, 05 RSA üzenetet, ha $n = 55$ és $f = 17$ (35 betűs ABC).
c) Dekódolja a 10, 62, 64, 34, 62 60 RSA üzenetet, ha $n = 77$ és $f = 7$ (35 betűs ABC).
(Ezek csak betűnkénti kódolások, ld. a 7. feladatot.)

2) Adottak a $p = 269$ és $q = 241$ prímszámok és az $e = 53201$ nyilvános kulcs.
a) Számolja ki $s = \varphi(n)$ értékét,
b) ellenőrizze, hogy e és s relatív prímek, majd számolja ki f értékét,
c) kódolja az $x = 48055$ üzenetet,
d) dekódolja az előbb kapott titkos üzenetet (azaz ellenőrizze a fenti számításokat),
e) kódolja a ”HELLO” = 0008 0512 1215 üzenetet (26 betűs ABC),
f) dekódolja a 36376 28210 53334 üzenetet.

3)a)-d) Oldja meg az előző feladatot a $p = 109$, $q = 271$, $e = 13201$ és $x = 11418$ értékekkel.
e) kódolja a ”HELLO” = 0008 0512 1215 üzenetet (26 betűs ABC),
f) dekódolja a 424 20621 üzenetet.

4) Tegyük fel, hogy a mi kódrendszerünk p=23, q=37, n=851, s=792, e=13, f=61, egy társunké p=29, q=31, n=899, s=80, e=29, f=29 . Hitelesítsük aláírásunkat részére a ”ZSEBSZÁMOLÓGÉP” szöveggel (35 betűs ABC).

5) Legyenek $n = 49,891,381$, $e = 209$, míg f , p , q és s titkosak, használjuk a 30 betűs ABC -t.
a) Kódolja az ”ANNA ÖRÖK” = 00000001 16160100 18211813 üzenetet.

b) Kódoljuk az ”OLVASD EL” üzenetet (26 betűs ABC) .
c) Ellenőrizze az $z \equiv x^f \equiv 49691150 \pmod{n}$ aláírás hitelességét.
d) Törje fel a kódot $(f, p, q, s =?)$, majd dekódolja az $y = x^e \equiv 37791786\ ,\ 01150082\ ,\ 32137718 \pmod{n}$ üzenetet.

6) Ha n a 0)e) feladatbeli szám(footnote) és $f = 2039$ akkor mennyi e értéke és mennyi az $x = 32$ kódja?

7) Milyen hosszú blokkokat (hány betűt egyszerre) lehet kódolni ha az n kulcs k -jegyű?

8*) Törje fel az alábbi kódrendszert: $e = 9007$,
$n = 11438162\ 5757888867\ 6692357799\ 7614661201\ 0218296721\ 2423625625\ 6184293570\ 6935245733\ 8978305971\ 2356395870\ 50589890751\ 4759929002\ 6879543541$ (129 jegyű), a titkosított üzenet:
$C = 9686\ 9613754622\ 06147714092\ 2254355882\ 90575999112\ 4574319874\ 6951209308\ 16298225145\ 70835693147\ 6622883989\ 6280133919\ 9055182994\ 5157815154$ (26 betűs ABC)

Megoldások

.

0) a) $440\ 747 = 613*719$,
b) $2\ 347\ 589 = 1483*1583$,
c) $97\ 189\ 241 = 7151*13591$,
d) $17\ 967\ 876\ 255\ 379 = 81371*220\ 814\ 249$,
e) $444\ 113\ 096\ 135\ 661\ 846\ 937 = 3\ 719\ 977\ 867 * 119\ 385\ 951\ 211$,
f) $2^{67} - 1 = 193\ 707\ 721 * 761\ 838\ 257\ 287$

1) a) a kódolt üzenet = 12 04 17 00 15 17 25 41 41 25 09 00 21 09 24 00 01 07 00 24 01 07 24 15 01 28.
b) $24^f \equiv 24^{17} \equiv 29 =$Ü $\pmod{55}$, ... s.í.t., az üzenet: *ÜGYES* .
c) $10^f \equiv 10^7 \equiv 10 =$H $\pmod{77}$, ... s.í.t., az üzenet: *HELYES* .

2) a) $n = pq = 64829,\ s = \varphi(n) = 268 \bullet 204 = 64320$,
b) az $ef - sy = 1$, azaz $53201 \bullet f - 64320 \bullet y = 1$ Diophantikus egyenletet kell megoldanunk: $f = 28721$,
c) $y \equiv x^e \pmod{n}$ azaz $y \equiv 48055^{53201} \equiv 61606 \pmod{64829}$,
d) $x \equiv y^f \pmod{n}$ azaz $x \equiv 61606^{28721} \equiv 48055 \pmod{64829}$,
e) $8^{53201} \equiv 13745$, $512^{53201} \equiv 57388$ és $1215^{53201} \equiv 18638 \pmod{64829}$, vagyis a ”HELLO” üzenet kódolva = 0008 0512 1215,
f) $36376^{28721} \equiv 16$, $28210^{28721} \equiv 918$, $1519^{28721} \equiv 53334 \pmod{64829}$, vagyis a kódolt üzenet: 0016 0918 1519 = ”PIROS”

3) a) $n = pq = 29539,\ s = \varphi(n) = 29160$,
b) $13201 \bullet f - 29160 \bullet y = 1$ alapján $f = 26041$,
c) $y \equiv 11418^{13201} \equiv 24836 \pmod{29539}$,
d) $x \equiv 24836^{26041} \equiv 11418 \pmod{29539}$,
e) $8^{13201} \equiv 9709$, $512^{13201} \equiv 512$ és $1215^{13201} \equiv 13473 \pmod{29539}$, vagyis a ”HELLO” üzenet kódja: 9709 512 13473 ,
f) $424^{26041} \equiv 112$, $20621^{26041} \equiv 1301$, vagyis a kódolt üzenet: 0112 1301 =”ALMA” .

5) a) $00000001^{209} \equiv 00000001 \pmod{n}$, $16160100^{209} \equiv 00022271 \pmod{n}$, $18211813^{209} \equiv 47610329 \pmod{n}$, tehát a kódolt üzenet = 00000001 00022271 47610329 (eml: $n = 49,891,381$).

b) ”OLVASD EL” = 15 12 22 01 19 04 00 05 12 amit 8 hosszú részekre tördelve $k_1 = 1512220$, $k_2 = 11904000$ és $k_3 = 512$. Ekkor
$k_1^e = 1512220^{209} \equiv 11812012 \pmod{49,891,381}$,
$k_2^e = 11904000^{209} \equiv 4882790 \pmod{49,891,381}$,
$k_3^e = 512^{209} \equiv 42839442 \pmod{49,891,381}$, vagyis a kódolt üzenet : 11812012 4882790 42839442 .

c) $z^e \equiv 49691150^{209} \equiv 19211115 \pmod{n}$ és 19 21 11 15 =”PRIM” értelmes üzenet.

d) $n = 49891381 = 6091 \bullet 8191 = p \bullet q$, $s = (p-1) \bullet (q-1) = 49877100$,
$f = 4056989 = 11110111100111100111101^{(BIN}$; így $(y_1)^f \equiv 37791786^{4056989} \equiv 22\ 30\ 17\ 14$ =”SZOL” $\pmod{n}$, $(y_2)^f \equiv 01150082^{4056989} \equiv 11\ 05\ 01\ 21$ =”IDAR” $\pmod{n}$,
$(y_3)^f \equiv 32137718^{4056989} \equiv 11\ 23\ 02\ 22$ =”ITÁS” $\pmod{n}$, azaz a feltört üzenet: ”SZOLIDARITÁS” .

6) Ha n = 444 113 096 135 661 846 937 = 3 719 977 867 * 119 385 951 211 és $f = 2039$ akkor e= 217 809 267 294 044 099 és $x = 32$ kódja $y \equiv x^e \equiv$ 316 326 629 379 980 725 998 $\pmod{n}$.

7) Ha $n \in \mathbb{N}$, akkor az egy részként kódolható betűsorozatok hossza k -jegyű szám, azaz k/2 betűt tartalmazhat ha az n szám k-jegyű, feltéve hogy n legalább 35-tel kezdődik. Vagyis n<3535 esetén csak betűnként tudunk kódolni, ami könnyen feltörhető. Ne feledkezzünk még meg a kódolás utáni (dekódolás előtti) szóközökről sem!

8*) A történet az [M] cikk szerint a következő: Rivest, Shamir és Adleman a *Scientific American* 1977. augusztusi számában tűzte ki ezt a feladatot (az első megfejtőnek 100$ jutalmat ajánlottak fel. 1994 áprilisában gazdája akadt a 100$-nak.)

n -et a következőképpen sikerült faktorizálni:
n = 3490 5295108476 5094914784 9619903898 1334177646 3849338784 3990820577 * 32769 1329932667 0954996198 8190834461 4131776429 6799294253 9798288533 .

A ”titkos” kitevő:
f = 106 69861436857 8024442868 7713289201 54780709906 63393786280 1226224496 63106312591 17744708733 4016859746 23065539685 4451327710 9053606095 .

A hatványozás után az eredeti rejtjelezett üzenet:
P = 20.08.05 00 13.01.07.09.03 00 23.15.18.04.19 00 01.18.05 00 19.17.21.05.01.13.09.19.08 00 15.19.19.09.06.18.01.07.05 = ”THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE” azaz A VARÁZSSZÓ A KÉNYESGYOMRÚ HALÁSZSAS.

A faktorizáció (1994-ben!) azáltal vált lehetségessé, hogy írtak egy programot, amely a számításokat képes volt sok számítógépre szétosztani s a részeredményeket a központba elküldeni, s több mint 600-an, amikor éppen nem volt szükség számítógépükre, ezt a programot futtatták. A munka így 8 hónapig tartott. A befutott részeredmények egy 569466 x 524338 mátrixot alkottak, amelyet Gauss-féle eliminációval 188614 x 188160-ra csökkentettek. Ennek alapján a faktorizáció 16K MasPar P-1-es gépen 45 óráig tartott. Ez az első eset, hogy sikerült RSA kódban írt szöveget feltörni; mint láthatjuk, elég szép munka volt.

Függelék

A használt ABC -k:

01=A, 02=B, 03=C, 04=D, 05=E, 06=F, 07=G, 08=H, 09=I, 10=J, 11=K, 12=L, 13=M, 14=N, 15=O, 16=P, 17=Q, 18=R, 19=S, 20=T, 21=U, 22=V, 23=W, 24=X, 25=Y, **26**=Z.

01=A, 02=Á, 03=B, 04=C, 05=D, 06=E, 07=É, 08=F, 09=G, 10=H, 11=I, 12=J, 13=K, 14=L, 15=M, 16=N, 17=O, 18=Ö, 19=P, 20=Q, 21=R, 22=S, 23=T, 24=U, 25=Ü, 26=V, 27=W, 28=X, 29=Y, **30**=Z .

01=A, 02=Á, 03=B, 04=C, 05=D, 06=E, 07=É, 08=F, 09=G, 10=H, 11=I, 12=Í, 13=J, 14=K,

15=L, 16=M, 17=N, 18=O, 19=Ó, 20=Ö, 21=ő, 22=P, 23=Q, 24=R, 25=S, 26=T, 27=U, 28=Ú, 29=Ü, 30=Ű, 31=V, 32=W, 33=X, 34=Y, **35**=Z.

További gyakorló kódrendszerek:

a) $p = 5,\ q = 11,\ n = 55, s = 40, e = 27,\ f = 3$,
b) $p = 7,\ q = 11,\ n = 77, s = 60, e = 11,\ f = 11$,
c) $p = 5,\ q = 13,\ n = 65, s = 48, e = 29,\ f = 5$,
d) $p = 7,\ q = 13,\ n = 91, s = 72, e = 29,\ f = 5$,
e) $p = 11,\ q = 13,\ n = 143, s = 120, e = 11,\ f = 11$,
f) $p = 17,\ q = 19,\ n = 323, s = 288, e = 17,\ f = 17$,
g) $p = 229,\ q = 233,\ n = 53,357, s = 52,896, e = 169,\ f = 313$.

Irodalom

.

[B] **Babai László**: *Prímszámok és titkosírás*, Természet Világa, 112/6 (1981).

[BFK] **Babai László- Freud Róbert- Kunfalvi Rezső**: *Prímszámvadászat számítógéppel*, Természet Világa, 113/5 (1982).

[BB] **Birkhoff**,**G**.-**Bartee**,**T**.**C**.: *A modern algebra a számítógéptudományban*, Műszaki Könyvkiadó 1974.

[G] **Gaizer Tamás**: *A számelmélet két gyakorlati alkalmazása* (vázlat)

[J] **Jackson**,**T**.**H**.: *From Number Theory to Secret Codes*, A Computer Illustrated Text, Adam Hilger, Bristol.

[K] **Koblitz**,**N**.: *A Course in Number Theory and Criptography*,Springer,1988.

[M] **Megyesi Zoltán**: *Titkosírások*, Polygon IV/2, (1994).

[S] **Schulz**,**R**.**H**.: *Primzahlen in öffentlichen Chiffrierverfahren*, Preprint, Freie Univ.Berlin, A2/1993.

[Sz] **Szalay Mihály**: *Számelmélet*, Tankönyvkiadó 1991.

eof