Temă

~RSA~

1) Ana și Bob folosesc RSA. Ana are cheia secretă ($n=12\,827$, $d=2291$). Determinați cheia sa publica și criptați textul IERI dacă lungimea blocurilor în clar este 2. și lungimea blocurilor criptate este 3

$n = 12827$

$d = 2291$

$$\begin{array}{l|l}
\sqrt{1.28.27} & 113 \\ \hline
\underline{1} & \underline{21 \cdot 1 = 21} \\
=28 & \underline{22\underline{3} \cdot \underline{3} = 669} \\
\underline{21} & \\
=727 & \\
\underline{669} & \\
=58 &
\end{array}$$

$[\sqrt{n}] = [\sqrt{12827}] = 113$

$t^2 - n = 114^2 - 12827 = 12996 - 12827 = 169 = 13^2$

$t^2 - n = 13^2$

$n = t^2 - 13^2 = 114^2 - 13^2 = (114+13)(114-13)$

$n = \underbrace{127}_{p} \cdot \underbrace{101}_{q}$

$\varphi(n) = (p-1)(q-1) = 126 \cdot 100 = 12600$

$e \cdot d \equiv 1 \pmod{\varphi(n)}$

$e \cdot 2291 \equiv 1 \pmod{12600}$

$(2291, 12600) = 1$; $X_{12600} = (1,0)$, $X_{2291} = (0,1)$

Scanned with CamScanner

$12600 = 2291 \cdot 5 + 1145$ | $x_{1145} = (1,0) - 5(0,1) = (1, -5)$

$2291 = 1145 \cdot 2 + 1$ | $x_1 = (0,1) - 2(1,-5) = (-2, 11)$

$$1 = 12600u + 2291v$$

$$2291^{-1} = 11 \Rightarrow \boxed{e = 11}$$

$e = 11$

$n = 12827$ $\mathbb{Z}_{30}$

iE RI

$iE_{(30)} = 30^1 \cdot 8 + 4 \cdot 30^0 = 30 \cdot 8 + 4 = 240 + 4 = 244$

$244^{11} \bmod 12827 = 244 \cdot 244^{10} = 244 \cdot (244^2)^5 = 244 \cdot 8228^5$

$= 244 \cdot 8228 \cdot (8228^2)^2 = 6620 \cdot 11905^2 = 6620 \cdot 3502$

$= 4851 = (5)(11)(21) = FLV_{(30)}$

$4851 : 30 = 161$
30
185
180
==51
30
21

$161 : 30 = 5$
150
=11

$5 : 30 = 0$
0
5

Scanned with CamScanner

(17) (8)

$Ri = 30 \cdot 17 + 8 = 510 + 8 = 518$

$518^{11} \bmod 12827 = 518 \cdot 518^{10} \pmod{12827} =$

$= 518 \cdot (518^2)^5 = 518 \cdot 11784^5 = 518 \cdot 11784 \cdot 11784^4 =$

$= 11287 \cdot (11784^2)^2 = 11287 \cdot 5534 = 7595_{(10)}$

$= (8)(13)(5) = iNF_{(30)}$

$7595 : 30 = 253$
60
159
150
$==95$
90
$=5$

$253 : 30 = 8$
240
$=13$

$8 : 30 = 0$
0
8

$iERi_{(30)} \xrightarrow{criptare} FLViNF_{(30)}$

2. Ama și Bob folosesc RSA - Ama are modulul $n=2733$
Știind că exponentul de criptare este minim posibil și că lungimea blocurilor în clar este 2 și lungimea blocurilor criptate este 3, criptați textul OK.

$n=2733$

$e=?$

$k=2$

$l=3$

$m=OK$

criptare$_{\#}$

(n,e)

$e\in\{3,4,\ldots\ldots,\varphi(n)-1\},\quad (e,\varphi(n))=1$

$$
\begin{array}{r|l}
\sqrt{27.33} & 52 \\ \hline
25 & 102\cdot 2=204 \\ \hline
=233 & \\
204 & \\ \hline
=29 &
\end{array}
$$

$[\sqrt{2733}]=52\ldots$

$2733:3=911 \Rightarrow p=3;\ q=911$

$\varphi(2733)=(p-1)(q-1)=2\cdot 910=1820$

$3\nmid 1820 \Rightarrow (3,1820)=1 \Rightarrow e=3$

$m=OK_{(30)}=O\cdot 30^{1}+K\cdot 30^{0}=14\cdot 30+10=420+10=430$

$430^{3}\ (\mathrm{mod}\ 2733)=430\cdot 430^{2}\ (\mathrm{mod}\ 2733)=430\cdot 1789\ (\mathrm{mod}\ 2733)$

$=1297_{(10)}=(1)(13)(7)=BNH$

$$
\begin{array}{l}
1297:30=43 \\
\underline{120} \\
==97 \\
\underline{90} \\
=7
\end{array}
\qquad
\begin{array}{l}
43:30=1 \\
\underline{30} \\
13
\end{array}
\qquad
\begin{array}{l}
1:30=0 \\
\underline{0} \\
1
\end{array}
$$

Scanned with CamScanner

3) Percy și Charlie comunică folosind criptosistemul RSA. Percy are cheia publică: $n = 187$ și $e = 107$

a. Aflați cheia privată a lui Percy

b. Charlie îi transmite lui Percy mesajul ABACFPFP știind că lungimea blocurilor mesajelor în clar este 1 și a mesajelor criptate este 2, decriptați textul.

a)

$n = 187$

$e = 107$

$d = ?$

$187 = \underbrace{11}_{p} \cdot \underbrace{17}_{q}$

$\varphi(n) = (p-1)(q-1) = 10 \cdot 16 = 160$

$e \cdot d \equiv 1 \pmod{\varphi(n)}$

$107 \cdot d \equiv 1 \pmod{160}$

$(107, 160) = 1$, $x_{160} = (1,0)$, $x_{107} = (0,1)$

$160 = 107 \cdot 1 + 53$ | $x_{53} = x_{160} - x_{107} = (1,-1)$

$107 = 53 \cdot 2 + 1$ | $x_1 = x_{107} - 2x_{53} = (0,1) - 2(1,-1) = (-2,3)$

$1 = 160u + 107v \Rightarrow 107^{-1} = 3 \Rightarrow d = 3$

b)

- $AB = 30^1 \cdot 0 + 30^0 \cdot 1 = 1$; $1^3 = 1 \to B$
- $AC = 30^1 \cdot 0 + 30^0 \cdot 2 = 2$; $2^3 = 8 \to i$
- $FP = 30^1 \cdot 5 + 30^0 \cdot 15 = 150 + 15 = 165$; $165^3 = 11 \to L$

$[165^3 = 165 \cdot 165^2 = 165 \cdot 27225 = 165 \cdot 110 = 18150 = 11 = L$

ABACFP FP $\xrightarrow{\text{decriptare}}$ BiLL

Scanned with CamScanner

4) Alice și Bob doresc să comunice folosind criptosistemul RSA. Alice alege numerele prime $p=3$, $q=11$ pentru a-și determina cheile de criptare / decriptare și alege exponentul de decriptare $d>1$ minimul posibil

a) Aflați cheia de criptare (n, e) a lui Alice.

b) Bob îi transmite lui Alice mesajul B!BTBL

Știind că lungimea blocurilor la citire este 1 și la scriere este 2, decriptați textul.

$p=7$

$q=11$

$n=p\cdot q=7\cdot 11=77$

$\varphi(n)=6\cdot 10=60$

$(d, \varphi(n))=1$

$d=7$

$(n,d)=(77,7)$

$(n,e)=?$

$d\cdot e\equiv 1 \pmod{\varphi(n)}$

$7e\equiv 1 \pmod{60}$

$(7,60)=1,\quad x_{60}=(1,0),\quad x_7=(0,1)$

$60=7\cdot 8+4 \quad\Big|\quad x_4=x_{60}-8x_7=(1,-8)$

$7=4\cdot 1+3 \quad\Big|\quad x_3=x_7-x_4=(0,1)-(1,-8)=(-1,9)$

$4=3\cdot 1+1 \quad\Big|\quad x_1=x_4-x_3=(1,-8)-(-1,9)=(2,-17)$

$$1=2\cdot 60+(-17)\cdot 7 \Rightarrow 7^{-1}\equiv -17=43 \Rightarrow \boxed{e=43}$$

$(n,e)=(77,43)$ → cheia de criptare

Scanned with CamScanner

b) $C = B!BTBL$

$B! = B \cdot 30 + ! = 30+28 = 58$

$58^d \pmod n = 58^7 \pmod{77} = 9 = J$

$BT = 30+19 = 49$

$49^7 \pmod{77} = 0$

$BL = 30+11 = 41$

$41^7 \pmod{77} = 13 = N$

$B!BTBL \xrightarrow{\text{decriptare}} JON$

5) Şeful vostru de grupă a decis să comunice cu voi folosind criptosistemul RSA. Aţi ales cheia publică $K_e = (n=1189,\ e=747)$

a) Determinaţi-vă cheia privată $(d=?)$

$\sqrt{1189}$ | 34

9 | 64·4=256

289

256

=33

$[\sqrt{1189}] = 34$

$35^2 - 1189 = 900+300+25 - 1189 = 325-289 = 36 = 6^2$

$35^2 - 6^2 = 1189$

$\underbrace{29}_{p} \cdot \underbrace{41}_{q} = 1189$

$\varphi(n) = 28 \cdot 40 = 1120$

Scanned with CamScanner

$d \cdot e \equiv 1 \pmod{\varphi(m)}$

$747 \cdot d \equiv 1 \pmod{1120}$

$x_{1120} = (1,0)$, $x_{747} = (0,1)$

$1120 = 747 \cdot 1 + 373$	$x_{373} = (1,-1)$
$747 = 373 \cdot 2 + 1$	$x_1 = (0,1) - 2(1,-1) = (-2,3)$

$$1 = (-2) \cdot 1120 + 3 \cdot 747 \Rightarrow d = 3$$

b) Ştiind că lungimea j a blocurilor în clar verifică $N^j \le m \le N^{j+1}$ şi lungimea blocurilor criptate este dată de $l = j+1$, decriptaţi textul BFCAFNBiW, unde N este lungimea alfabetului.

$N^j \le m \le N^{j+1}$, $l = j+1$

$30^j \le 1189 \le 30^{j+1} \Rightarrow j = 2$, $l = j+1 = 3$

$c = BFCAFNBiW$

$\overline{BFC} = B \cdot 30^2 + F \cdot 30 + C = 30^2 + 5 \cdot 30 + 2 = 900 + 150 + 2 = 1052$

$1052^3 = 454 \pmod{1189} = (15)(4) = PE$

$454 : 30 = 15$
30
154
150
$= 4$

$15 : 30 = 0$
0
15

$\overline{AFN} = 0 \cdot 30^2 + 5 \cdot 30 + 13 = 163$

$163^3 = 409 \pmod{1189} = (30)(19) = NT$

$409 : 30 = 13$
30
109
90
$= 19$

$13 : 30 = 0$
0
13

Scanned with CamScanner

$\overline{BiW} = 1162 = -27$

$1162^3 = (-27)^3 = -27^3 = -659 = 530 = (17)(20) = RU$

```
530 : 30 = 17        17 : 30 = 0
30                    0
230                  17
210
 =20
```

$$\text{BFCAFNBiW} \xrightarrow{decriptare} \text{PENTRU}$$

7) Iulia şi Andrei folosesc criptosistemul RSA. Iulia are cheia publică $K_{eI} = (n_I = 9991, e_I = 3917)$

a) Determinaţi cheia privată a Iuliei.

$n = 9991, \quad e = 3917$

```
√9991 | 99
 81   |______
 1891 | 189·9 = 1701
 1701 |
 =190 |
```

$100^2 - 9991 = 9 \Rightarrow 100^2 - 3^2 = 9991$

$\underbrace{97}_{p} \cdot \underbrace{103}_{q} = 9991$

$\varphi(n) = 96 \cdot 102 = 9792$

$3917 \cdot d \equiv 1 \pmod{9792}$; $x_{9792} = (1,0)$, $x_{3917} = (0,1)$

$9792 = 3917 \cdot 2 + 1958$ | $x_{1958} = (1,-2)$

$3917 = 1958 \cdot 2 + 1$ | $x_1 = (0,1) - 2(1,-2) = (-2,5)$

$1 = 9792 \cdot (-2) + 3917 \cdot 5 \Rightarrow d = 5 \rightarrow$ cheia privată

Scanned with CamScanner

b) Decriptați mesajul BMHA_X primit de Iulia, știind că lungimea blocurilor în clar este 2 și a celor criptate este 3.

$$\underbrace{BMH}\underbrace{A\_X}$$

$BMH = 30^2 + 12\cdot30+7 = 900+360+7 = 1267$

$1267^5 \pmod{9991} = 404 = (13)(14) = NO$

$A\_X = 0\cdot30^2 + 26\cdot30+23 = 803$

$803^5 \pmod{9991} = 570 = (19)(0) = TA$

```
570 : 30 = 19        19 : 30 = 0
30                   0
270                  19
270
= 0
```

$$BMHA\_X \xrightarrow{decriptare} NOTA$$

6) Alice folosește RSA. Blocurile mesajelor în clar au 1 caracter, iar blocurile mesajelor criptate au 2 caractere. Pentru a determina cheile de criptare/decriptare, ea alege numerele prime $p=23$, $q=17$ și face publică cheia de criptare $(n, e=3)$.

a) Bob dorește să-i trimită lui Alice mesajul HELP_ME! Criptați acest mesaj.

Scanned with CamScanner

$y = 1, \ell = 2$

$p = 23, q = 17$

$(n, e = 3)$

$n = 23 \cdot 17 = 391$

a) $m_1 = \text{HELP\_ME!}$

$H = 7$

$7^3 \pmod{391} = 343 = (11)(13) = LN$

$343 : 30 = 11$ $\quad$ $11 : 30 = 0$

$\underline{30}$ $\quad$ $\underline{0}$

$= 43$ $\quad$ 11

$\underline{30}$

13

$E = 4$

$4^3 = 64 = (2)(4) = CE$

$64 : 30 = 2$ $\quad$ $2 : 30 = 0$

$\underline{60}$ $\quad$ $\underline{0}$

$= 4$ $\quad$ 2

$L = 11$

$11^3 = 158 = (5)(8) = Fİ$

$158 : 30 = 5$ $\quad$ $5 : 30 = 0$

$\underline{150}$ $\quad$ $\underline{0}$

$= 8$ $\quad$ 5

$P = 15$

$15^3 = 247 = (8)(7) = İH$

$247 : 30 = 8$ $\quad$ $8 : 30 = 0$

$\underline{240}$ $\quad$ $\underline{0}$

$= 7$ $\quad$ 8

Scanned with CamScanner

$\_ = 26$

$26^3 = 372 \pmod{391} = (12)(12) = MM$

$372 : 30 = 12$
30
$= 72$
60
12

$12 : 30 = 0$
0
12

$M = 12$

$12^3 = 164 = (5)(14) = FO$

$164 : 30 = 5$
150
$= 14$

$5 : 30 = 0$
0
5

$\text{HELP\_ME!} \xrightarrow{\text{criptare}} \text{LNCEFiiHMMFOCE}$

b) Determinați cheia de decriptare a lui Alice și decriptați mesajul primit de aceasta EBMMAAFOMML!EBAiHi

I _ A M _ S

$d \cdot e \equiv 1 \pmod{\varphi(n)}$

$\varphi(391) = 22 \cdot 16 = 352$

$3 \cdot d \equiv 1 \pmod{352}$; $X_{352} = (1, 0)$, $X_3 (0, 1)$

$352 = 3 \cdot 117 + 1$ | $X_1 = (1,0) - 117(0,1) = (1, -117)$

$\Rightarrow 3^{-1} \pmod{352} = -117$

$d = -117 = 235$

$EB = 4 \cdot 30 + 1 = 121$

$121^{235} \pmod{391} = 121 \cdot (121^2)^{117} = 121 \cdot (174)^{117} = 121 \cdot 174 \cdot (174^2)^{58}$

$= 331 \cdot (169^2)^{29} = 331 \cdot 18 (18^2)^{14} = 93 \cdot (324^2)^7 = 93 \cdot ((-67)^2)^7$

$= 93 \cdot 188 \cdot (188^2)^3 = 280 \cdot 154 \cdot 154^2 = 110 \cdot 256 = 8 = i$

Scanned with CamScanner

$AA = 0 \cdot 30 + 0 = 0$

$0^{235} = 0 \,(\text{mod } 391) = 0 = A$

$L! = 11 \cdot 30 + 28 = 330 + 28 = 358$

$358^{235} \,(\text{mod } 391) = 18 \,(\text{mod } 391) \Rightarrow S$

$EB = 4 \cdot 30 + 1 = 121$

$121^{235} \,(\text{mod } 391) = 8 \Rightarrow \dot{I}$

$A\dot{I} = 0 \cdot 30^1 + 8 \cdot 30^0 = 8$

$8^{235} \,(\text{mod } 391) = 2 \Rightarrow C$

$Hi = 7 \cdot 30 + 8 \cdot 30^0 = 210 + 8 = 218$

$218^{235} \,(\text{mod } 391) = 10 \rightarrow K$

EBMMAAFOMML!EBAiHi $\xrightarrow{\text{decriptare}}$ i_AM_SiCK

Scanned with
CamScanner