TMA 055 : Diskret Matematik

Inlämningsuppgift 3

Följande allmäna regler gäller för alla inlämningsuppgifterna (se också Kurs PM:et) :

1. Motivera (bevisa) alla svar.
2. Uppge vilka du samarbetet med.
3. Spara uppgifterna (med kommentarer) när du får tillbaka dem.

Att lämna in torsdag den 26 september

OBS !! Du får full poäng (60p.) för lösningar till huvuduppgiften (45p.) plus en av de första två uppgifterna (15p. var). Den återstående uppgiften kan då betraktas som ett bonusproblem.

1. Let p be a prime. An integer a among $1, 2, ..., p-1$ is said to be a *quadratic residue* modulo p if there exists an integer x such that

$$x^2 \equiv a \pmod{p}.$$

Otherwise, a is said to be a *quadratic non-residue.*

(i) How many quadratic residues and non-residues are there modulo p ?
(ii) Let a, b, c be integers such that neither a nor b is a multiple of p. Show that there exist integres x and y such that

$$ax^2 + by^2 \equiv c \pmod{p}.$$

(Hint : pigeonhole principle).

2. Let n be an integer which is a product of two distinct primes p and

q.

(i) Suppose you know both n and $\phi(n)$. Explain how you can quickly derive the factorisation of n.
(ii) Show that if a is any integer (not necessarily relatively prime to n), and k any integer such that $k \equiv 1 \pmod{\phi(n)}$, then

$$a^k \equiv a \pmod{n}.$$

3 (huvuduppgiften). Before reading further, go to the list of names at the end of this document and get your 'telephone number'. Each number represents an RSA-encrypted 4-letter English word. Your first task is to decrypt the word. For this you'll need to know how the encryption was done.

First, I converted each word W to a non-negative integer M less than 26^4 using the method described in the lectures, but this time using base 26 instead of 32 (since I have no need for punctuation symbols). Each M was then encrypted using my (public) RSA encryption function f_A obtained from my public key

$$(n_A, e_A) = (667763, 123679),$$

where

$$n_A = p_A q_A \quad \text{and} \quad p_A = 911, \;\; q_A = 733.$$

Since I'm telling you the factorisation of my n_A, you have enough information to be able to be able to decode your word.

Your second task is to reencrypt your word, but this time using an encryption function f_B which you will construct yourself ; that is, you must construct your own public key (n_B, e_B). Your n_B should satisfy

$$26^4 < n_B < 26^5.$$

Your final task is to write me a signed message consisting of your word, appropriately encrypted (you, B, are sending a secret message to me, A).

NOTE : For digital signatures, there is a small subtlety with RSA which

I did not mention in class, namely : if B is sending to A, then

if $n_B < n_A$, the signing function is $f_A \circ f_B^{-1}$,

BUT !!!

if $n_B > n_A$, you must sign with the function $f_B^{-1} \circ f_A$.

List of names and numbers

1. Fredrik Pettersson : 158875
2. Ivana Trogulic : 557024
3. Roland Muskovic : 41399
4. Marcus Hellqvist : 6349
5. Henrik Andersson : 212315
6. Jonas Oresten : 2948
7. Tommy Boström : 186628
8. Benny Nilsson : 521860
9. Björn Mattsson : 548955
10. Louis Chu : 215222
11. Sebastian Carlsson : 428016
12. Erik Gullstrand : 226064
13. Anders Hickenström : 515484
14. Jakob Stille : 106306
15. Simon Magnusson : 556019
16. Daniel Öhman : 271708
17. Henrik Ekman : 70246
18. Ivar Schmidt : 492291
19. Albert Ottosson : 277479
20. Kristofer Jalve : 606725
21. Henrik Linger : 71363
22. Gustav Ahn : 180624
23. P.O. Bengtsson : 289916
24. Roger Jönsson : 415111
25. David Angerwall : 277811
26. Christian Ekholm : 389297
27. Jonas Lundin : 608600
28. Henrik Pettersson : 377697
29. Karl Gustav Johansson : 25462

30. Henrik Holst : 498513
31. Fredrik Carlsson : 273065
32. Fredrik Sandedal : 229276
33. Matilda Enlund : 142728
34. Jonas Williamsson : 177848
35. Markus Kutti : 445543
36. Oskar Sämfors : 362191
37. Fredrik Bengtsson : 355374
38. Martin Nilsson : 261242
39. Anna Svanberg : 185936
40. Daniel Lind : 87494
41. David Djurbäck : 295374
42. Lena Hård : 127395
43. Joakim Holt : 600522
44. Tobias Ågren : 296910
45. Carl Wanngård : 116724
46. Johan Dufberg : 104424
47. Ola Sandgren : 164760
48. Jakob Ursby : 184720
49. Martin Frid : 307811
50. Anna Gund : 337696
51. Mikael Gustavsson : 518501
52. Fredrik Nordlander : 664589
53. Mattias Söderlundh : 399573
54. Daniel Sterner : 243619
55. Jonas Andersson : 88257
56. Martin Ekenbäck : 438626
57. Henrik Elofsson : 237452
58. Anneli Olsen : 560067
59. Anton Berzelius : 607972
60. Frida Larsson : 228918
61. Önder Tumayer : 78317
62. Oscar Eriksson : 498381
63. Mattias Hermansson : 96026
64. Joachim Mårtensson : 503182
65. Daniel Carlsson : 268285
66. Marja Blom : 535933
67. Iman Shahram : 580687
68. Henrik Jonsson : 305822

69. Erik Nordborg : 624875
70. Mikael Johansson : 239486
71. Katja Shunevich : 429325
72. Karl Nilsson : 311126
73. David Lennström : 536666
74. Christian Adolfsson : 160244
75. Maris Åhs : 658522
76. Susanne Eira : 158056
77. Niklas Einvall : 202168
78. Robert Kihl : 369081
79. Rolando Aguilar : 581300
80. Micke Pedersen : 234191
81. Jonas Lakhall : 480772
82. Mattias Ågren : 605053
83. Henrik Ahlstrand : 617258
84. Gustav Friberg : 91516
85. Jan Hendén : 625270
86. Andreas Lindberg : 460861
87. Tobias Jansson : 20440
88. Dag Hanarp : 589766
89. Erik Larsson : 548614
90. Daniel Ode : 207054
91. Mattias Falkehag : 172352
92. Johan Johansson : 115785
93. Linus Andersson : 247959
94. Rikard Persson : 406419
95. Ola Davidsson : 534169
96. Carl Stranne : 571204
97. Markus Ahlstrand : 324453
98. Per P. Sollin : 537132
99. Nils J. Wessman : 478031
100. Mattias Gustafsson : 200586
101. Fredrik Marthinsson : 260200
102. Karina Svensson : 91117
103. Carl Lamberg : 419683
104. Ana Magazinovic : 550527
105. Marko Isomäki : 337075
106. Johan Haldén : 137048
107. Peter Sjöstrand : 186141

108. Kalle Ohlsson : 310907
109. Anton Persson : 48578
110. Kenneth Nygren : 492488
111. Kristoffer Carlsson : 140470
112. Fredrik Engström : 69104
113. Olle Nyström : 495882
114. Imren Arda : 98951
115. Niclas Elfvenstam : 642122
116. Emilia Bjehlestam : 194283
117. Andreas Sigurdsson : 149577
118. Rasmus Hedin : 243330
119. Faraja Tammo : 607391
120. Christofer Edvardsen : 17021
121. Joakim Möller : 89987
122. Haris Mehmedovic : 12851
123. Fredrik de Groot : 638552
124. Lukas Elinder : 143590
125. Henrik Matsum : 145299
126. Anders Erestam : 115690
127. Robert Dinäss : 596368
128. Calle Håkansson : 348635
129. Kristoffer Sohtell : 193079
130. Annika Ermander : 386602
131. NiklasLarsson : 293707
132. Johan Myhr : 648438
133. Erik Häggström : 391321
134. Anders Johansson : 623833
135. Roger Eriksson : 293755
136. Anna Josefsson : 141792
137. Ola Bjurermo : 559397
138. Hans Grufman : 418631
139. Johan Lundahl : 384108
140. Nina Tahmasebi : 9161
141. Markus Wandt : 110651
142. Olle Sundström : 555435
143. Sebastian Tafuri : 36738
144. Daniel Hellström : 227260
145. Joakim Ström : 361233
146. Andreas Andersson : 505944

147. Thomas Serkitjes : 462823
148. Göran Nilsson : 95448
149. Alexander Ehrensvärd : 648393
150. Peiman Khorramshahi : 470656
151. Jesper Olsson : 343289
152. Eva Israelsson : 182108
153. Jonas Nordström : 354973
154. Lukas Lundblad : 637193
155. Anna Sjöberg : 434200
156. Johan Rastén : 46519