Att lämnas in måndag den 10 oktober

REGLER : Full points for Q.1 (70 percent) and any one of the other two questions (30 percent each). Hence you get a 30 percent bonus for answering all three questions. Q.3 is probably harder than Q.2 (at least it's longer). In Q.1, half the points are given for each of the two tasks.

1. Before reading further, go to the list of names at the end of this document and get your 'telephone number'. If your name is not there, let me know and I'll give you a 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

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

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.

For your second task you will first need to construct another public key (n_B, e_B) such that satisfy

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

Give this key to me and take the above (n_A, e_A) to be your key instead. So you are now A and I am B. Your task is now to write me a signed message consisting of your word, appropriately encrypted (you, A, are sending a secret message to me, B).

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

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

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

BUT !!!

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

OBS!!! The first task I want you to do by hand, i.e.: you must write out all your calculations, and the algorithms you apply, in full. You may use a calculator, but no mathematical software, in other words.

For the second task, you may use software to do the calculations. Please include with your solution a print-out of your program. You may use built-in programs for algorithms like primality testing, Euclid's algorithm, repeated squaring etc., and don't need to write your own programs to implement these algorithms.

For example, if you use *mathematica*, you may make use of the following in-built programs :

· PrimeQ[n]

Outputs TRUE if n is prime, otherwise FALSE.

·ab

Multiplies a and b.

· EulerPhi[n]

Computes $\phi(n)$.

· GCD[a, b]

Computes the GCD of a and b.

· PowerMod[a, b, c]

Computes $a^b \pmod{c}$. Note that this function can even be used to com-

pute multiplicative inverses, i.e.: if you insert $b = -1$ then it computes $a^{-1} \pmod{c}$ provided $\mathrm{GCD}(a, c) = 1$. If $\mathrm{GCD}(a, c) > 1$ then it replies with an error message.

2. Let n be a positive integer. Let A_n be the subset of $\{1, ..., n\}$ consisting of those integers k for which the equation

$$x^6 + y^6 - z^6 = k$$

has an integer solution. Show that

$$\lim_{n\to\infty} \frac{A_n}{n} \leq \frac{4}{7}.$$

3. Let p be a prime. An integer $x \in \{1, ..., p-1\}$ is said to be a *quadratic residue* modulo p if there exists an integer y such that

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

Let $\mathcal{R}_p$ denote the set of quadratic residues modulo p.

(i) Write out the sets $\mathcal{R}_{13}$ and $\mathcal{R}_{17}$.
(ii) Show that, if p is a prime and x, y are any two integers, then

$$x^2 \equiv y^2 \pmod{p} \Leftrightarrow x \equiv \pm y \pmod{p}.$$

Deduce that $|\mathcal{R}_p| = \frac{p-1}{2}$ for all odd p.
(iii) Prove that, if $p > 3$, then

$$\sum_{x\in\mathcal{R}_p} x \equiv 0 \pmod{p}.$$

List of names and numbers

1. Per Jacobson : 158875
2. Mikael Andersson : 557024
3. Henrik Sangö : 41399
4. Therese Andrésen : 6349
5. Gustav Andersson : 212315
6. Mia Ingmarsdotter : 2948

7. Marcus Oscarsson : 186628
8. Kristoffer Wilhelmsson : 521860
9. Johan Kemme : 548955
10. Alfred Eklöf : 215222
11. Deji Odulate : 428016
12. Navid Razazi : 226064
13. Pontus Hellåker : 515484
14. Valdet Zekaj : 106306
15. Samuel Karlsson : 556019
16. Henrik Påhlsson : 271708
17. Z. Dimitrijevic : 70246
18. Per Düring : 492291
19. Martin Ventin : 277479
20. Sepehr Reyhanian : 606725
21. Farzad Dehmany : 71363
22. Jens Hedin : 180624
23. Fredrik Hedström : 289916
24. Marcus Anemo : 415111
25. Carl Jacobsson : 364521
26. Marie Åhs : 389297
27. Jenny Hilbertsson : 608600
28. Caroline Hermansson : 316398
29. Hanna Levin : 25462
30. Jonas Wignäs : 498513
31. Robin Björnberg : 273065
32. Per Kürcman : 229276
33. Olle Wedin : 142728
34. Gustav Johannesson : 177848
35. Johannes Adler : 445543
36. Ali Mansouri : 362191
37. Erik Jagre : 355374
38. Alireza Arjomand : 261242
39. Samir Dehli : 185936
40. Jesper Frisk : 87494
41. Jonatan Hedin : 295374
42. Tomas Höök : 127395
43. Jack Percival : 600522
44. Peter Schill : 296910
45. David Steen : 116724

46. Mats Wang-Hansen : 242203
47. Emil Edvardsson : 164760
48. Carl Lindström : 184720
49. Martin Hedvall : 307811
50. Malin Aktius : 337696
51. Mats Wiksborg : 518501
52. Ted Bremberg : 664589
53. Erik Karlsson : 399573
54. Lena Berg : 243619
55. Martin Julander : 88257
56. Martin Hadartz : 438626
57. Marie Ström : 237452
58. Jonatan Åkerlind : 560067
59. Henrik Claesson : 607972
60. Irena Draca : 228918
61. Eija Johansson : 78317
62. Jonas Svensson : 498381
63. Martin Larsson : 96026
64. Marcus Birgersson : 503182
65. Carl Hallqvist : 268285
66. Thomas Lewander : 535933
67. Daniel Ohlsson : 580687
68. Anders Eliasson : 305822
69. Martin Gholami : 624875
70. Johanna Majqvist : 239486
71. Andreas Baur : 429325
72. Victor Ström : 311126
73. Jonas Sundström : 536666
74. Alexander Stenberg : 160244
75. William Fall : 658522
76. Nils Wenzelberg : 158056