Att lämnas in måndag den 11 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. However, I think personally that Q.2 is the harder one. 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 (mod c). Note that this function can even be used to compute multiplicative inverses, i.e.: if you insert $b = -1$ then it computes $a^{-1} \pmod{c}$ provided $\text{GCD}(a, c) = 1$. If $\text{GCD}(a, c) > 1$ then it replies with an error message.

2. Let p be a prime and let a, b, c be any three elements of $\mathbf{Z}_p$ with $a, b \neq 0$. Prove that the congruence

$$ax^2 + by^2 + c \equiv 0 \pmod{p}$$

has at least one solution in $\mathbf{Z}_p$.

(Hint : Pigeonhole principle).

3 (i) Let G be a plane graph. By counting in two different ways the pairs (r, e), where r is a region (possible the exterior) and e is an edge on the boundary of r, prove that

$$R \leq \frac{2}{3}E.$$

(ii) Hence, or otherwise, prove that every plane graph has at least one node whose degree is at most 5.

(Hint : Use Euler's formula to prove that the average degree of a node is strictly less than 6).

List of names and numbers

1.	Gunnar Olsen :	158875
2.	Niklas Sigfusson :	557024
3.	Martin Å kesson :	41399
4.	Jonas Andersson :	6349
5.	Yudi Bravo :	212315
6.	Rickard Friberg :	2948
7.	Lovisa Lander :	186628
8.	Magnus Bågenholm :	521860
9.	Erik Skårbratt :	548955
10.	Marcus Linder :	215222
11.	Tobias Lernvall :	428016
12.	Johan Engström :	226064
13.	Fredrik Lundberg :	515484
14.	Marie Å hs :	106306

15. Thomas Lundberg : 556019
16. Linus Lundin : 271708
17. Simon Housernäs : 70246
18. Carl Bergfeldt : 492291
19. Vilhelm Geijer : 277479
20. Per Rondqvist : 606725
21. Simon Ahlström : 71363
22. Emma Moore : 180624
23. Martin Arvidsson : 289916
24. Gustav Lövgren : 415111
25. Fredrik Sikén : 277811
26. Erik Ryman : 389297
27. Erik Å kesson : 608600
28. Erik Pettersson : 377697
29. Dan Härdfeldt : 25462
30. Johan Thuresson : 498513
31. Fabian Ahlström : 273065
32. Tobias Harrysson : 229276
33. Gustav Andersson : 142728
34. Anders Sandberg : 177848
35. Erik Lindgren : 445543
36. Ingemar Jansson : 362191
37. Peter Hygren : 355374
38. Robert Kniström : 261242
39. Karolina Ljungberg : 185936
40. Johan Norberg : 87494
41. Johan Bengtsson : 295374
42. Michaela Sundin : 127395
43. Christoffer Bengtsson : 600522
44. Daniel Lundberg : 296910
45. Peter Johansson : 116724
46. Anders Å slund : 104424
47. Arton Haziraj : 164760
48. Andreas Fallström : 184720
49. Gustav Minnhagen : 307811
50. Viktor Claesson : 337696
51. Joakim Gunnarsson : 518501
52. Jonas Lindqvist : 664589
53. Per Sarrander : 399573

54. Martin Andersson : 243619
55. Andreas Karlsson : 88257
56. Emil Edvardsson : 438626
57. Jonas Eira : 237452
58. Jonas Holgersson : 560067
59. Georgiana Gruia : 607972
60. Marcus Gustavsson : 228918
61. Mikael Brunnhede : 78317
62. Fredrik Brunnhede : 498381
63. Shahin Ghazinouri : 96026
64. Mattias Winsten : 503182
65. Marcus Ahlstrand : 268285
66. Johan Rudholm : 535933
67. Christofer Edvardsen : 580687
68. Jonas Klittmark : 305822
69. Rikard Larsson : 624875
70. Robert Bergfors : 239486
71. Paul Jonsson : 429325
72. Krister Hao : 311126