TMA 055 : Diskret Matematik

Inlämningsuppgift 3

(Att lämna in måndag den 13 oktober)

1 (15p) (i) Draw a planar graph G whose vertices are all the countries of Europe and in which two countries are joined by an edge if they share a common border[1]. Then

(a) order the vertices in alphabetical order, first in English and then in Swedish. Apply the greedy algorithm with each ordering to color G.
What is $\chi(G)$?

(b) take the largest connected piece of your graph and compute $V =$ no. of vertices, $E =$ no. of edges and $R =$ no. of enclosed regions in G. Then compute $V - E + R$.

(ii) This time, take a graph based on the countries of South America instead[2]. Repeat part **(b)** above. Notice anything ?

(iii) Repeat part **(b)** again, this time for the graph of a football (I mean a REAL football, that is, one that's sown together to form pentagons and hexagons). Notice anything ?

(iv) Explain everything you've noticed.

2 (35p). Before reading further, go to the list of names at the end of

[1] An up-to-date map of Europe, in case you don't have one, can be found for example at http://www.wunderground.com/global/Region/EU/Temperature.html. Do not count sea borders (for example, Britain is not connected to France). Do not include Turkey, Israel or former Soviet republics. In order to make sure your graph is planar, give Gibraltar to Spain !! If you wish to avoid arousing my nationalistic fury, avoid connecting Britain to Ireland !!

[2] http://www.wunderground.com/global/Region/SA/Temperture.html.

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 35 (since it's english and 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 decode your word.

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

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

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 math software to do the calculations. Please include with your solution a print out of your program. You may use in-built 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.

· a*b

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 compute 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 'Fuck you, asshole !' (ok, not exactly).

List of names and numbers

1. Tobias Abrahamsson : 158875
2. Karl Ahlstedt : 557024
3. Niklas Algården : 41399
4. Mohammad Ali : 6349
5. Andreas Almer : 212315
6. Marie Andersson : 2948

7. Oscar Andersson : 186628
8. Peter Andersson : 521860
9. Ulrika Andersson : 548955
10. Christer Andreasson : 215222
11. Emil Arnell : 428016
12. André Aydin : 226064
13. Robert Bagge : 515484
14. Camilla Berglund : 106306
15. Viktor Berglund : 556019
16. Andreas Bergqvist : 271708
17. Samuel Bergqvist : 70246
18. Anna Bexander : 492291
19. Björn Bexander : 277479
20. David Elebring : 606725
21. Jonas H.D. Eriksson : 71363
22. Jonas M. Eriksson : 180624
23. Karl Erlandsson : 289916
24. Linda Erlenhov : 415111
25. Henrik Ernholm : 364521
26. Joakim Evers : 389297
27. Josef Falk : 608600
28. Per Finnstam : 316398
29. Daniel Fjällholm : 25462
30. Peter Fransson : 498513
31. Björn Franzon : 273065
32. Niklas Gustafsson : 229276
33. Oskar Hagberg : 142728
34. Christian Hansson : 177848
35. Mikael Havel : 445543
36. Martin Hedström : 362191
37. Anders Hermansson : 355374
38. Andreas Hermansson : 261242
39. Henrik Hjelte : 185936
40. Johan Hoff : 87494
41. Erik Holm : 295374
42. Daniel Holmqvist : 127395
43. Christina Håkansson : 600522
44. David Håkman : 296910
45. Johan Isaksson : 116724

46. Mats Åke Isaksson : 242203
47. Anders Jahnberg : 164760
48. Anders Jernberg : 184720
49. Daniel Johansson : 307811
50. Kim Johansson : 337696
51. Sofia Johansson : 518501
52. Tomas Johansson : 664589
53. Anders Järnstedt : 399573
54. Ola Karlsson : 243619
55. Roland Karlsson : 88257
56. Terese Karlsson : 438626
57. Håkan Karolusson : 237452
58. Peter Kellerman : 560067
59. Mikael Kjellgren : 607972
60. Magnus Källvik : 228918
61. Alex Lam : 78317
62. Markus Larsson : 498381
63. David Lindh : 96026
64. Carl Lindström : 503182
65. Cecilia Ljunggren : 268285
66. Mattias Lundin : 535933
67. Christoffer Malm : 580687
68. Björn Mathiasson : 305822
69. Conny Moberg : 624875
70. Jimmy Myhrman : 239486
71. Anders Mökander : 429325
72. Erik Nilsson : 311126
73. Carl Magnus Nordin : 536666
74. Ingrid Norling : 160244
75. Gunnar Olsson : 658522
76. Fredrik Olsson : 158056
77. Johanna Olsson : 202168
78. Karin Paulette : 369081
79. Joakim Persson : 581300
80. Marcus Persson : 234191
81. Dejan Popovski : 480772
82. Milad Pouyanmehr : 605053
83. Anna-Lena Rinaldo : 617258
84. Anders Runeson : 91516

85. Daniel Runstedt : 625270
86. David Rylander : 460861
87. Mikael Samuelsson : 20440
88. Henrik Sandgren : 589766
89. Torbjörn Sandsgård : 548614
90. Per Sandström : 207054
91. Peter Schill : 172352
92. Martin Schölin : 115785
93. Martin Sigby : 247959
94. Stefan Simonsson : 406419
95. Maria Stegberg : 534169
96. Johan Stenfeldt : 571204
97. Michael Swedberg : 324453
98. Anders Thid : 537132
99. Mattias Thorsell : 478031
100. Nikola Vorkapic : 200586
101. Peter Windeman : 260200
102. Johan Zhang : 91117
103. Fredrik Ögren : 419683
104. Björn Öhnell : 550527
105. Fredrik Sinkkonen : 337075
106. Petros Tedla : 137048
107. Daniel Kaczmarek : 186141
108. Justus Magnusson : 310907
109. Katorina Martinsson : 48578
110. Helena Gerebo : 492488
111. Christofer Edvardsson : 140470
112. Mirela Puskar : 69104
113. Alma Ciric : 495882
114. Edin Catovic : 98951
115. Izudin Gore (???) : 642122
116. Henrik Andersson : 194283
117. Sara Wallgren : 149577
118. Jonas Lindvall : 243330
119. Per Eklund : 607391
120. Nils-Erik Nyberg : 17021
121. Marie Åhs : 89987
122. Helena Ottosson : 12851
123. Kent Hansson : 638552

124. Amar Omarovic Egmer (???) : 143590
125. Linus Gustafsson : 145299
126. Radenko Ristic : 115690
127. Anna von Zweigbergk : 596368
128. Mikael Johansson : 348635
129. Nils Wenzelberg : 193079
130. Viktor Claesson : 386602
131. Mikael Fredriksson : 293707
132. Jonas Yngvesson : 648438
133. Avenir Kobstski: 391321
134. Goran X (the grad student !) : 623833
135. Sparat : 293755
136. Sparat : 141792
137. Sparat : 559397
138. Sparat : 418631
139. Sparat : 384108
140. Sparat : 9161
141. Sparat : 110651
142. Sparat : 555435
143. Sparat : 36738
144. Sparat : 227260