Computer Science CS 4/57221 Introduction to Cryptology
Spring 2014
Final examination
Due on Blackboard on May 7 at 11:00 PM

Please be brief: Irrelevant or incorrect material will cost you points.

1) (25 points) Given positive integers a, b, c and m, with $0 < a, b, c$ what is necessary for and how would you go about finding a numbers x and y such that $ax + by = c$
2) (25 points) Looking at OFB mode from chapter 5, describe how this mode can be attacked if the initial vector (IV) is not changed.
3) (25 points) Choose two four-digit primes and an encryption exponent (3 or 17 may do nicely, or you may have to choose another one).
   a) Use these parameters to define an RSA cryptosystem.
   b) Take the last four digits of your banner ID and encrypt that number with the RSA system defined above.
   c)Find the corresponding decryption exponent and verify that everything worked.
   d)What would be the digital signature (unhashed) corresponding to your message?
4) (25 points) In this problem, we will set up a Diffie-Hellman system; the common prime number is 14983, and the generator we need is 14827; you come up with your own private key; my public key came out to 1357. What is our common secret?
   (To clarify; you take your key and raise the generator to that key; you should now know the rest).