Math 1350 **The Art of Secret Writing** **Fall 2012**

Review for Final Exam

This review sheet gives an over view of the material we have covered since Exam 2. The final exam **will be** cumulative so please also revisit the first two review sheets. You will be allowed the use of graphing (or lesser featured) calculators but not of any technology that has an internet or phone connection.

The exam will take place on Tuesday 11 December 2012 from 7pm until 9:30pm in Malott 253. Any requests for an alternate time due to exam conflict must be made before as early as possible to ensure that you will be able to sit the exam.

The practice problems below are often hitting several of the skills at once and time should be budgeted accordingly.

Skills to practice:

- Be comfortable enciphering and deciphering using the binary Vigenere cipher.
- Computing the output of a linear feedback shift register.
- Computing the output of a Feistal function
- Sieve of Erasthones
- Fermat's Factoring Method
- Extended Euclidean Algorithm
- Computing very large powers modulo p or pq
- Setting up an RSA public and private key pair.
- Enciphering and deciphering using RSA.
- Digitally signing a message.

Concepts to be applied:

- Feistel functions performed in several rounds.
- Feedback registers to be used to create cipher keys.
- The notation for computer based block ciphers, concatenation, XOR.
- Prime Number theorem and counting of primes.
- Computational Expense of factoring methods.
- Fermat's Little Theorem and Corollary
- Relative Security of RSA

Vocabulary:

- Feedback shift register
- Block cipher
- Feistel Functions
- Symmetric / Asymmetric ciphers
- Public-key Encryption
- RSA
- Digital Signature for a message (as opposed to the linguistic signature of Chapter 2).

Practice problems:

Task 1. (1) *Let a linear feedback shit register with five registers be seeded with the values:* $b_1 = b_2 = b_3 = b_4 = b_5 = 1$ *and with update functions* $b_5' = (b_1 + b_2 + b_3 \oplus b_4) \mod 2$. *Calculate the as many digits of the key stream that this feedback register produces as are necessary for the following parts of this task.*

(2) *Using this key stream using the binary Vigenere cipher encipher your birthdate.*

(3) *Using a Feistel function from the textbook (page 224 is a good example) again encipher your birthdate. Use the second, third, and seventh digits from the key stream as the key when doing this.*

(4) *The following message was encipher using the binary Vigenere cipher, 8-bit ANSII codings for letters into binary strings and the first 16 digits of the feedback register above as a repeating key. Decipher the message:*[1]

10110111 10111011 10010110 10110001 10010101 10101101

Task 2. *Set up a public and private key pair using the RSA method. Determine how many base-26 digits it can encipher in a single block. Then encipher and decipher your last name.*

Using the same keys create another message and sign it.

Task 3. *Why is it that of all the ciphers we learned that only RSA makes it possible to sign a message?*

Task 4. *Make some explanation of why RSA is computationally more complex than using Feistel function block ciphers?*

[1] This portion of the task is too time intensive for the exam, however a much smaller message would be plausible.

Task 5. *Using the theorems of Chapter 4 (state which one you are using) to calculate*

$$62^{80} \mod 79 \qquad 43^{303} \mod 303$$

Task 6. *Bob has published an RSA modulus of* 3127 *and public key* 35*. Someone claiming to be Bob has sent you the signed message* $190, 2602$*. How much do you trust that the sender is Bob?*

Task 7. *Bob has published the RSA modulus of* 35 *and* $e = 3$ *send him the message HELLO.*

Task 8. *You have chosen* $p = 7$ $q = 11$*,* $m = 77$*,* $n = 60$*,* $e = 17$ $d = 53$ *and published the relevant items. Determine how many letters can be enciphered in each block. You then receive from me the following message:*

62 42 19 41 16

What does it say? Does it make sense?

Task 9. *Suppose you find yourself in a country where communications are not secure and that you knew you would be going there and could prepare. You are allowed to exchange a short hand written note with your business partner before you leave. While you are in this country you take several videos that you want to securely transmit home. What encryption scheme do you choose and why?*