T-79.5501 Cryptology
Homework 10
April 3, 2007

1. Suppose that $n = 355044523$ is the modulus and $b = 311711321$ is the public exponent in the *RSA Cryptosystem.* Using Wiener's Algorithm, attempt to factor n. If you succeed, determine also the secret exponent a and $\phi(n)$.

2. Bob and Bart are using the Rabin Cryptosystem. Bob's modulus is 2183 and Bart's modulus is 2279. Alice wants to send an integer x, $0 < x < 2183$, encrypted to both of them. She sends ciphertext 1479 to Bob and the ciphertext 418 to Bart. Carol sees the ciphertexts and she knows Bob's and Bart's moduli. Show how Carol can compute x without factoring of moduli. Hint: Use Chinese Remainder Theorem.

3. Bob is using the *Rabin Cryptosystem.* Bob's modulus is $40741 = 131 \cdot 311$. Alice knows Bob's modulus but not its factors. Alice wants to remind Bob of an important date and sends it to Bob encrypted. The ciphertext is 589.

   (a) Show how Bob decrypts the ciphertext. One of the possible plaintexts is a date, which Bob accepts and discards the other decryptions.

   (b) Alice happens to see one of the decryptions discarded by Bob. It is 28020. Show how Alice can now factor Bob's modulus.

4. It is given that

$$12^{2004} \equiv 4815 \pmod{50101},$$

   where 50101 is a prime. Show that the element $\alpha = 4815$ is of order 25 in the multiplicative group $\mathbb{Z}_{50101}^*$.

5. Consider $p = 1231$, which is a prime. Find an element of order $q = 41$ in the multiplicative group $\mathbb{Z}_{1231}^*$.

6. Consider ElGamal Public-key Cryptosystem in Galois field $\mathrm{GF}(2^4)$ with polynomial $x^4 + x + 1$ and with the primitive element $\alpha = 0010 = x$. Your private key is $a = 7$.

   a) Compute your public key β.

   b) Decrypt ciphertext (0100,1110) using your secret key.