T-79.503 Foundations of Cryptology
Homework 11
December 2, 2004

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 $n_1 = 2183$ and Bart's modulus is $n_2 = 2279$. Alice wants to encrypt an integer x, $0 < x < 2183$, to both of them. She sends ciphertext $y_1 = 1479$ to Bob and the ciphertext $y_2 = 418$ to Bart. Determine x. You can find the solution without factorisation of the moduli.

3. Consider ElGamal Public-key Cryptosystem in Galois field 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.

4. It is given that
$$2^{48} \equiv 443 \pmod{1201},$$
where 1201 is a prime. Show that the element $\alpha = 443$ is of order 25 in the multiplicative group $\mathbb{Z}_{1201}^*$.

5. Using Shanks' algorithm attempt to determine x such that
$$443^x \equiv 489 \pmod{1201}.$$
Hint: Determine first the order n of the cyclic group G generated by α.

6. (Stinson 6.4 (a)) Suppose that p is an odd prime and k is a positive integer. The multiplicative group $\mathbb{Z}_{p^k}^*$ has order $\phi(p^k) = p^{k-1}(p-1)$, and is known to be cyclic. A generator of this group is called a *primitive element modulo* p^k. Suppose that α is a primitive element modulo p. Prove that at least one of α or $\alpha + p$ is a primitive element modulo p^2.