T-79.5501 Cryptology
Homework 8
November 17 & 18, 2005

1. (a) Find all square roots of 1 modulo 4453.
   (b) 2777 is a square root of 3586 modulo 4453. Find all square roots of 3586 modulo 4453.

2. The integers 26945 and 459312 are square roots of the integer 80833 modulo 540143. Based on this information find some nontrivial integer divisors of 540143.

3. It is given that

   $$2^{4!} \equiv 1655213 \,(\mathrm{mod}\, 15122003).$$

   Use the Pollard $p-1$ algorithm to find a nontrivial divisor of 15122003.

4. The integer $n = 89855713$ is known to be a product of two primes. Further, it is given that $\phi(n) = 89836740$. Determine the factors of n.

5. (Stinson 5.30) Suppose that Bob has carelessly revealed his decryption exponent to be $a = 14039$ in an *RSA Cryptosystem* with public key $n = 36581$ and $b = 4679$. Implement the randomized algorithm to factor n given this information. Test your algorithm with the "random choices $w = 9983$ and $w = 13461$.

6. 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.