MATC16 Cryptography and Coding Theory
Gábor Pete
University of Toronto Scarborough
gpete at utsc dot utoronto dot ca

Homework Assignment 3 (Due March 22)

Problem 1. Let e, d be encryption and decryption exponents for RSA with modulus $n = pq$.

(a) Show that $m^p \equiv m \pmod{p}$ for any m (not necessarily relatively prime to p). You can assume Fermat's little theorem. **(1 pt)**

(b) Show that $m^{ed} \equiv m \pmod{n}$ for any m. Again, we've seen the case $\gcd(m, n) = 1$, so you may assume that $\gcd \neq 1$. Hint: use the Chinese Remainder Theorem. **(3 pts)**

Problem 2. Take the 4-digit number formed by the end of your student ID. Find a number with difference at most 4 from it that is not divisible by any of 2,3,5, call it n. Choose a random base b (make an attempt to make it really random in $\{2, 3, \ldots, n-2\}$, not just 2 or 3), and test the primality of n with **(a)** the Fermat prime test and **(b)** the Miller-Rabin test, both times using the same base b. **(2+2 pts)**

Problem 3. Suppose you want to factor $n = 2288233$, and you discover that $880525^2 \equiv 2 \pmod{n}$, and $2057202^2 \equiv 3 \pmod{n}$, and $648581^2 \equiv 6 \pmod{n}$, and $668676^2 \equiv 77 \pmod{n}$. Use this information to factor n. **(2 pts)**

Problem 4. $\alpha = 2$ is a primitive root mod $p = 101$. Alice and Bob want to use ElGamal with these parameters.

(a) What are the largest a for Bob and k for Alice that are worth choosing? In other words, these exponents should be random elements of what set? **(1 pt)**

(b) Assume that $a = 24$ and $k = 69$. Choose a message $1 < m < 100$ for Alice to send, and encrypt it. Then check that Bob can decrypt the ciphertext correctly, without knowing k. **(2 pts)**

Problem 5. Suppose you have discovered that $3^6 \equiv 44 \pmod{137}$ and $3^{10} \equiv 2 \pmod{137}$. Find a value of x with $0 \leq x \leq 135$ such that $3^x \equiv 11 \pmod{137}$. (**2 pts**)

Problem 6. Consider the function $h(x) = x^2 \pmod{p}$, where p is a "large" prime, $p = 8848607$. Show that h is not preimage-resistant even for typical values (for 1, 4, 9, 16, etc, it is obviously easy to find preimages), and that it is not weakly collision free, either. **(2 pts)**

Problem 7. What is the probability that, in a family of five, all birthdays are in different months?

(a) First assume that all twelve months have equal lengths. **(1 pt)**

(b) In reality, different months have different lengths. Do you think this increases or decreases or doesn't change the above probability? You don't need to give a proof, but do give some support to your guess. **(2 pt)**

(c) How big does a family have to be to make the above probability zero? **(1 pt)**

(Max possible score: 21 pts)