MAT 302: ALGEBRAIC CRYPTOGRAPHY

Department of Mathematical and Computational Sciences
University of Toronto, Mississauga

February 27, 2013

Practice Mid-term Exam

INSTRUCTIONS:

- The duration of the exam is 100 minutes.
- The exam is worth a total of 100 marks.
- Please use the workspace at the end of this booklet for calculations.
- You are allowed to bring one 3" $\times$ 5" cue ('index') card to the exam with writing on both sides. No other written notes are permitted.
- No Calculators, Cellphones, Laptops or other electronic devices.

Good luck!

QUESTIONS

Problem 1: True or False (10 Marks)

Please circle the correct answer.

(a) Let p be prime, g be a generator, $h_1, h_2 \in \mathbb{Z}_p^*$, and let $\mathsf{dlog}_g(h)$ denote the discrete logarithm of h to the base g. Then, $\mathsf{dlog}_g(h_1 + h_2) = \mathsf{dlog}_g(h_1) + \mathsf{dlog}_g(h_2)$. TRUE FALSE

(b) Let e and N be integers such that $\mathsf{gcd}(e, \phi(N)) \neq 1$. Let $a \in \mathbb{Z}_N^*$. Then, there are no solutions x for the equation $x^e = a \pmod N$. TRUE FALSE

(c) There is a positive integer N such that $\phi(N) = 17$. TRUE FALSE

Problem 2: Do you know your algorithms? (15 Marks)

1. **(5 Marks)** Find all solutions x of the equation $x^{1999} = 10 \pmod{17}$.

2. **(10 Marks)** Compute $19^{20^{21}} \pmod{30}$.

Problem 3: Cryptography (10 Marks)

1. The RSA encryption system turns out to be insecure if you choose the RSA primes P and Q to be very close to each other. In particular, show that if the difference between P and Q is at most 100 (namely, $|P - Q| \leq 100$), you can quickly find P and Q, given only $N = PQ$ in about 100 operations.

Problem 4: More on Primality Tests (25 Marks)

Assume that you have a number N and $a \in \mathbb{Z}_N^*$ such that

(a) $a^{N-1} = 1 \pmod{N}$, and

(b) for every prime factor F of $N-1$, $a^{(N-1)/F} \neq 1 \pmod{N}$.

1. **(10 Marks)** What is the order of a in the group $\mathbb{Z}_N^*$? Prove your assertion.

2. **(15 Marks)** Prove that in this case, N is prime.

Problem 5: Another Primality Criterion (10 Marks)

Prove that a natural number $n > 1$ is prime if and only if $(n-1) = -1 \pmod{n}$.

Problem 5: A Twist on Finding Roots (20 Marks)

You are given a natural number N, numbers $f, g \in \mathbb{Z}_N^*$ and relatively prime integers a and b such that

$$f^a = g^b \pmod{N}$$

That is, f is the a^{th} root of g^b mod N. How will you use this information to find the a^{th} root of g, namely a number $h \in \mathbb{Z}_N^*$ such that

$$h^a = g \pmod{N}$$

Your algorithm has to be fast, and in particular, should not use the knowledge of the prime factorization of N.

WORK SHEET

WORK SHEET

WORK SHEET