Instructor: Leo Goldmakher

University of Toronto Mississauga
Department of Mathematical and Computational Sciences

MAT 302: CRYPTOGRAPHY

Final Exam (held on April 21st in the Faculty Club, South Building 3140)

INSTRUCTIONS:

The final exam will consist of two questions, to be answered orally (you will have access to a whiteboard). The duration of the exam will be roughly 20 minutes. 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.

The first question, Question A below, will be asked of each student. The second question will be selected from List B below, as follows: each student will draw two numbers out of a hat, and then will have a choice as to which of the two corresponding problems to discuss.

Best of luck!

QUESTIONS

Question A:
Describe the RSA algorithm: how it works, why it is secure, and any pertinent mathematics. Your discussion should include the square-and-multiply algorithm.

List B

1. **Classical ciphers and random number generators**

   Scytale, Caesar, Affine, and Substitution ciphers: how they work, what their weaknesses are.
   The idea of the stream cipher; the one time pad; the linear congruential generator.

2. **Stirling's formula**

   State Stirling's formula, and sketch proof that $N! \asymp \sqrt{N}\left(\frac{N}{e}\right)^N$.

3. **Group theory**

   Definitions of $\mathbb{Z}_n$ and $\mathbb{Z}_n^\times$.
   Proof that $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \ : \ (a, n) = 1\}$.
   Proof that $a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}$.

4. **Euler φ-function**

   Definition; formula for $\varphi(p^n)$ and proof; proof that φ is multiplicative; Euler's theorem that $a^{\varphi(n)} = 1$ for all $a \in \mathbb{Z}_n^\times$.

5. **Prime number theory**

   Statement of Fundamental Theorem of Arithmetic.
   Statement of Prime Number Theorem, and interpretation.
   Sketch of proof that $\mathbb{Z}_p^\times$ is cyclic.

6. **Primality testing**

   Describe the Fermat and Miller-Rabin tests, including all relevant mathematics.
   Prove that for any $a \in \mathbb{Z}_n^\times$, we have $(x + a)^n \equiv x^n + a \pmod{n}$ if and only if n is prime.

7. **Diffie-Hellman and related ideas**

   Describe the Diffie-Hellman Key Exchange, and all relevant mathematics.
   The Diffie-Hellman problem, the discrete log problem, and their relationship to each other.
   The Elgamal cipher.
   Safe primes: what they are, why they're useful.

8. **Elliptic curves**

   Explain how to determine all integer solutions to $x^2 + y^2 = z^2$.
   Describe the group law on elliptic curves.
   Describe the Elliptic Curve Diffie-Hellman Key Exchange.