PMAT 329 — Quiz 3 — Fall 2003

December 3, 2003

Name:____

Please DO NOT write your ID number on this page.

- **Duration:** 50 minutes.
- **Total points:** 50.
- Show **all** your work.
- **No aids allowed. This includes calculators.**

1. (a) [2 points] Define the term *stream cipher*.

   (b) [2 points] Define the term *primitive root modulo* p (p a prime).

   (c) [2 points] Let p be a prime. State the *discrete logarithm problem* modulo p.

   (d) [2 points] Define what it means for a public key cryptosystem to provide *signature capability*.

   (e) [2 points] Define the *Euler phi function* $\phi(n)$ for any positive integer n.

2. (a) [3 points] State all the properties of an *authentication function* A_K (K a secret key).

   (b) [3 points] State all the properties of a *one-way function* f.

3. [6 points] Describe the Diffie-Hellman key exchange protocol. Give a definition/explanation of each symbol you use, including whether it is secret or public, and describe in detail the steps that each communicant has to perform.

4. (a) [3 points] Let p be a prime. Suppose you guess that an integer $g \pmod{p}$ is a primitive root modulo p. Describe a fast procedure to verify your guess.

   (b) [4 points] Use your procedure of part (a) to find a primitive root modulo 29. Show all your work.

5. The *Pohlig-Hellman* cryptosystem is a conventional (private key) cryptosystem with the following specifications:

   - All users agree on a large public prime p.
   - Keys are pairs of integers (e, d) with $1 < e, d < p$, $\gcd(e, p-1) = \gcd(d, p-1) = 1$, and $ed \equiv 1 \pmod{p-1}$.
   - Messages and ciphertexts are integers modulo p, i.e. integers between 1 and $p - 1$.
   - *Encryption*: For a message M with $1 \le M \le p-1$, define the ciphertext to be

     $$C \equiv M^e \pmod{p}, \qquad (1 \le C \le p-1).$$

   - *Decryption*: Decrypt a ciphertext C with $1 \le C \le p-1$ to

     $$M \equiv C^d \pmod{p}, \qquad (1 \le M \le p-1).$$

   Note that unlike RSA, e is *not* public. Remember that this is a conventional cryptosystem, so we only have secret keys; that is, we assume that both encrypter and decrypter know the key (e, d) which is secret to everyone else.

   (a) [4 points] Prove that this works, i.e. that encryption followed by decryption yields the original message. That is, if M is any message and $C \equiv M^e \pmod{p}$, then $M \equiv C^d \pmod{p}$.

(b) [2 points] Which (presumably hard) number theoretic problem is the security of the Pohlig-Hellman scheme based on?

(c) [5 points] Suppose a cryptanalist has an algorithm for solving any instance of the (presumably hard) hard number theoretic problem identified in part (b). Explain how the cryptanalyst could use this algorithm to mount a known ciphertext attack on the Pohlig-Hellman scheme and find the secret key (e, d).

(d) [5 points] Suppose $p = 19$ and $e = 13$. Find the corresponding value for d. Show all your work.

(e) [5 points] Using $p = 19$ and $e = 13$, encrypt the message $M = 5$. Use the power algorithm and show all your work.