Math 437: Cryptography

Exam 1

February 23 2017

NAME:

To receive full credit you must clearly show all work and justify your answers. No books, notes, or calculators are allowed during this exam. This is a 100 minute exam.

Question:	1	2	3	4	5	6	7	8	Total
Points:	10	15	10	10	10	10	10	0	75
Score:									

1. (a) (5 points) Describe what it means for g to be a **primitive root** of $\mathbb{F}_p$ for some prime p.

   (b) (5 points) If g is a primitive root of $\mathbb{F}_p$ for some prime p, what is the order of g modulo p?

2. (a) (5 points) Use the Euclidean algorithm to show that that the $\gcd(251, 180) = 1$.

   (b) (5 points) Use the extended Euclidean algorithm to determine values for u, v such that

   $$1 = 251u + 180v.$$

   (c) (5 points) Determine $180^{-1} (\mathrm{mod}\, 251)$. Give your answer as an integer between 0 and 251.

3. Recall the Affine cipher has a key $k = (k_1, k_2)$ and a prime p such that

$$e_k(m) \equiv k_1 m + k_2 (\mathrm{mod}\, p)$$
$$d_k(c) \equiv k_1^{-1}(c - k_2)(\mathrm{mod}\, p)$$

Let $p = 251$ and $k = (180, 9)$.

(a) (5 points) Encrypt the message $m = 56$.

(b) (5 points) Decrypt the ciphertext $c = 15$.

4. (10 points) Let $a \in \mathbb{Z}$ be nonzero and p be a prime integer. Show how Fermat's little theorem can be used to find a^{-1} in $\mathbb{Z}/p\mathbb{Z}$.

5. (10 points) Use Fermat's little theorem to determine $12^{-1} (\mathrm{mod}\, 37)$. Give your answer as an integer between 0 and 37.

6. (a) (5 points) Verify that 2 is a primitive root of $\mathbb{F}_{13}$.

   (b) (5 points) Without finding all primitive roots of $\mathbb{F}_{13}$, determine how many primitive roots of $\mathbb{F}_{13}$ there are.

7. (10 points) Let m be a positive integer and let $a \in \mathbb{Z}$. Prove that there exists a $b \in \mathbb{Z}$ such that $ab \equiv 1 (\mathrm{mod}\, m)$ if and only if $\gcd(a, m) = 1$.

8. (10 points (bonus)) Recall the Affine cipher has a key $k = (k_1, k_2)$ and a prime p such that

$$e_k(m) \equiv k_1 m + k_2 (\mathrm{mod}\, p)$$
$$d_k(c) \equiv k_1^{-1}(c - k_2) (\mathrm{mod}\, p)$$

It can be shown that the Affine cipher is vulnerable to known plaintext attacks with 3 pairs (m_1, c_1), (m_2, c_2), and (m_3, c_3). If you obtain the pairs $(8, 9)$, $(6, 32)$, and $(11, 45)$, break the cipher and decrypt the ciphertext $c = 31$.