Name and UNI:

Making, Breaking Codes, Midterm 1

This examination booklet contains 6 problems. Do all of your work on the pages of this exam booklet. Show all your computations and justify/explain your answers. Cross out anything you do not want graded.

If there is a mistake in the question or if you are not sure what something means, just make a guess, explain what is going on in your answer, and continue.

You have about 75 minutes to complete the midterm. Do not begin until instructed to do so. When time is up, stop working and close your test booklet. Books, notes, calculators, cell phones, headphones, laptops, and other electronic devices are not allowed.

1. Using the correspondence $A = 0$, $B = 1$, ..., $Z = 25$ use the affine cipher $x \mapsto -x + 5$ (mod26) to encrypt the plaintext "ax" into a ciphertext (written in terms of capital letters). Explain your work.

Solution:
Note that $a = 0$ and $x = 23$. Then

$$\begin{aligned} 0 &\mapsto -0 + 5 \equiv 5 \pmod{26}, \\ 23 &\mapsto -23 + 5 = -18 \equiv 8 \pmod{26}. \end{aligned}$$

Since $F = 5$ and $I = 8$, the plaintext 'ax' is encrypted as 'FI'.

2. Compute the multiplicative inverse of 7 modulo 705. Use either the Euclidean algorithm or the extended Euclidean algortihm and show your work.

Solution:
The Euclidean algorithm that computes $\gcd(7, 705)$ is done as follows:

$$\begin{aligned} 705 &= 7(100) + 5 \\ 7 &= 5(1) + 2 \\ 5 &= 2(2) + 1 \\ 2 &= 1(2). \end{aligned}$$

We then back-substitute:

$$\begin{aligned} 1 &= 5 - 2(2) \\ &= 5 - (7 - 5)(2) \;=\; 7(-2) + 5(3) \\ &= 7(-2) + (705 - 7(100))(3) \;=\; 7(-302) + 705(3). \end{aligned}$$

Thus,

$$7(-302) \;\equiv\; 1 \pmod{705},$$

or

$$7(403) \;\equiv\; 1 \pmod{705}.$$

The inverse of 7 $(\text{mod}\, 705)$ is 403.

3. Explain why $a^{36} \equiv 1 \pmod{481}$ for any integer a with $\gcd(a, 481) = 1$ using that $481 = 13 \cdot 37$ and using the Chinese remainder theorem.

Solution:

Since $\gcd(a, 481) = 1$, we have $\gcd(a, 13) = \gcd(a, 37) = 1$. Note that $13, 37$ are prime numbers. It follows from Fermat's Little Theorem that

$$\begin{aligned} a^{36} &= (a^{12})^3 \equiv 1 \pmod{13}, \\ a^{36} &\equiv 1 \pmod{37}. \end{aligned}$$

By the fact that $\gcd(13, 37) = 1$ and the Chinese Remainder Theorem,

$$a^{36} \equiv 1 \pmod{481}.$$

4. Answer the following questions about RSA.
(a) Briefly describe the RSA public key cryptosystem. You must state the public information, the secret decryption key, and how to encrypt and decrypt messages.

Solution:

(1) Bob chooses two large distinct prime numbers p and q.
(2) Bob chooses an integer e such that $\gcd(e, (p-1)(q-1)) = 1$.
(3) Bob computes d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$.
(4) Bob computes $n = pq$.
(5) Bob makes (n, e) **public** and keeps (p, q, d) **secret**. d is the **secret decryption key** for Bob.

Now, suppose Alice wants to send Bob a message m. We may assume $m < n$. Otherwise, Alice breaks m into blocks in which each of them is smaller than n.

Encryption (for Alice): She computes $c \equiv m^e \pmod{n}$ and sends c to Bob.

Decryption (for Bob): He computes $c^d \pmod{n}$ to recover the message m.

(b) What (supposedly) hard number theory problem does the security of RSA rely on?

Solution:

Existence of efficient (polynomial-time) algorithm for prime factorizations of large integers.

5. You are given that 5 is a primitive root modulo 97 and you are given that

$$2^{32} \equiv 35 \pmod{97},\ 3^{32} \equiv 35 \pmod{97},\ 4^{32} \equiv 61 \pmod{97},\ 5^{32} \equiv 35 \pmod{97}.$$

Let x be the smallest positive integer such that $5^x \equiv 2 \pmod{97}$. Explain how to use the Pohlig-Hellman algorithm to determine $x \pmod 3$.

Solution:

Note that

$$97 - 1 \ = \ 96 \ = \ 2^5 \cdot 3.$$

It is given that

$$2^{\frac{97-1}{3}} \ = \ 2^{32} \ \equiv \ 35 \pmod{97}.$$

For $k = 0, 1, 2$, we consider

$$5^{\frac{97-1}{3}k} \ = \ 5^{32k} \pmod{97}.$$

Since

$$5^{32(0)} \ \equiv \ 1 \ \not\equiv \ 35 \ \equiv \ 2^{32} \pmod{97},$$
$$5^{32(1)} \ \equiv \ 35 \ \equiv \ 2^{32} \pmod{97},$$

we have $x \equiv 1 \pmod 3$ by the Pohlig-Hellman algorithm.

6. Let p be a prime number.
(a) Precisely define what is a primitive root modulo p.

Solution:

There are a couple of possible definitions: we say α is a primitive root $(\mathrm{mod}\, p)$ if

(1) α is a generator of the group $(\mathbb{Z}/p\mathbb{Z})^\times$, **or**
(2) α satisfies the property that:

$$\{\alpha^x : 1 \leqslant x \leqslant p-1\} \;=\; \{1, \ldots, p-1\},$$

or
(3) The smallest $x \in \{1, \ldots, p-1\}$ for which $\alpha^x \equiv 1 \pmod p$ is $p-1$.

(b) How many primitive roots modulo p are there?

Solution: There are $\phi(p-1)$ primitive roots $(\mathrm{mod}\, p)$.

(c) Find all the primitive roots modulo 7.

Solution:

There are $\phi(7-1) = \phi(6) = 2$ primitive roots $(\mathrm{mod}\, 7)$.

(1) Since $2^3 \equiv 1 \pmod 7$, 2 is not a primitive root $(\mathrm{mod}\, 7)$.
(2) Since $3^1 \equiv 3 \not\equiv 1 \pmod 7$, $3^2 \equiv 2 \not\equiv 1 \pmod 7$ and $3^3 \equiv 6 \not\equiv 1 \pmod 7$, 3 is a primitive root $(\mathrm{mod}\, 7)$.
(3) Since $4^3 \equiv 1 \pmod 7$, 4 is not a primitive root $(\mathrm{mod}\, 7)$.
(4) Since $5^1 \equiv 5 \not\equiv 1 \pmod 7$, $5^2 \equiv 4 \not\equiv 1 \pmod 7$ and $5^3 \equiv 6 \not\equiv 1 \pmod 7$, 5 is a primitive root $(\mathrm{mod}\, 7)$.
(5) Since $6^2 \equiv 1 \pmod 7$, 6 is not a primitive root $(\mathrm{mod}\, 7)$.

Therefore, the primitive roots $(\mathrm{mod}\, 7)$ are 3 and 5.