Homework 6

Due: Friday, March 25

All homeworks are due at 11:59 PM on Gradescope.

Please do not include any identifying information about yourself in the handin, including your Banner ID.

Be sure to fully explain your reasoning and show all work for full credit.

Problem 1

For each of the following, find a multiplicative inverse for the given element in two ways: first by using the extended Euclidean algorithm, and second by using Euler’s Theorem. If no inverse exists, state so and explain why.

a. 4 (mod 17)
b. 25 (mod 21)
c. 38 (mod 19)
d. 42 (mod 33)
e. 31 (mod 23)
Problem 2

Professor Lewis wants to establish a secure communication channel between his office at Brown University and a local coffee shop. He wants to use a cryptosystem that is both simple and effective, and has decided to use the RSA cryptosystem as a result. He publishes the public key:

\[ pq = N = 12712871 \]

with encryption exponent

\[ e = 4567 \]

a. The coffee shop’s fierce opposition group, Anti-coffee, wants to send nonsense along the communication channel to disrupt the mission.

Encrypt his favorite number, 840 using public keys \( N \) and \( e \).

b. In a moment of weakness, Professor Lewis has revealed his decryption exponent, \( d = 86239 \), to Anti-coffee! Decrypt the most recent message, 7685566.

c. Show how you can factor \( N = pq \) given the quantity \((p - 1)(q - 1)\).

**Hint**: Distribute and expand, then try to use Vieta’s formula.

d. In a *second* moment of weakness, Professor Lewis has revealed to Anti-coffee:

\[ (p - 1)(q - 1) = 12704952 \]

Factor \( N = pq \) using this information and your methodology from part (c).
Problem 3

a. Compute the remainder when $11^{1111} + 33^{3333} + 55^{5555} + 77^{7777}$ is divided by 13.

**Hint:** Can anything be simplified with Fermat’s Little Theorem?

b. Prove that $\frac{21n+4}{14n+3}$ is in lowest terms for any positive integer $n$. This means that the numerator and the denominator have no common factors.

**Hint:** Consider the greatest common divisor of the numerator and denominator. You can use Euclid’s algorithm to compute it.

c. Prove that if $d = \text{gcd}(a, b)$, then $\text{gcd}(a/d, b/d) = 1$.

**Hint:** Prove that any prime number $p$ which is a common factor of $a$ and $b$ has multiplicity 0 in $\text{gcd}(a/d, b/d)$. That is, it doesn’t divide $\text{gcd}(a/d, b/d)$. 
Problem 4 (Mind Bender — Extra Credit)

For those looking for a more traditional Mind Bender on mathematical topics related to the course, we encourage you look into the Diffie-Hellman Key Exchange and the Elgamal Public Key Cryptosystem.

However, this week, the Mind Bender will emphasize on the social implications of cryptography. This will be a short writing/reflection assignment. A short paragraph or two for each part is sufficient.

a. You have implemented RSA encryption and are hoping to sell your program to fund your daily hot-drink intake. What companies or organizations might approach you for this technology? What should you keep in mind when making this decision. Can your technology be used maliciously?

Give three examples of companies or organizations who might want to acquire this technology, and pros/cons for why you should or shouldn’t provide your technology to them.

b. Right before signing your multi-million-dollar deal with said company, the government approaches you claiming that the sale and export of cryptography is regulated.

Learn about the restrictions on the export of cryptography from the US. Do you think these regulations are reasonable? How have the policies changed over the years?

c. After you finally sign your deal with said company (and can now fund your copius daily hot-drink intake), the government approaches you again with a warrant asking for you to divulge the company’s private keys.

Learn about key disclosure laws and key escrow. Do you think the government should be allowed to do this? How might you protect the company you’re working for? Will you hold the company’s private keys in escrow? Give arguments for and against.