Assignment: Project 5
Name 1: Jonathan Smoley
Name 2: Samuel Sovi
GitHub Name: JT2M0L3Y

1. **Use the Euclidean algorithm, showing every step, to find the gcd(30030,257).**
   $30030 = 116 * 257 + 218$
   $257 = 1 * 218 + 39$
   $257 = 6 * 39 + 23$
   $39 = 1 * 23 + 16$
   $23 = 1 * 16 + 7$
   $16 = 2 * 7 + 2$
   $7 = 3 * 2 + 1$
   $2 = 2 * 1 + 0$
   Thus, the gcd(30030, 257) = 1.

2. **Here are two factoids, the first we've proved:**
   - **if *n* is composite, it must have a factor, *c*, such that** $c \leq \sqrt{n}$
   - **30030 = 2 * 3 * 5 * 7 * 11 * 13**

   Use the result from problem 1 and the two factoids to argue that 257 is prime.
   $\sqrt{257} \approx 16.031$
   - For 257 to be composite, it must have a factor c, such that $c \leq \sqrt{n}$.
   - Therefore, for 257 to be composite, it must have a prime factor c_1, such that $c_1 \leq \sqrt{n}$.
   - This is because if it had a composite factor, then that factor would be a product of primes (by the Fundamental Theorem of Arithmetic).
   - The prime numbers up to 16.031 are 2,3,5,7,11,13
   - Since we were given that 30030 contains all those prime numbers as factors and that gcd(30030, 257) = 1, we know that none of the prime numbers up to 16.031 are factors of 257.
   - As such, we can conclude that 257 is prime.

3. **Use Fermat's Little Theorem to compute** $2^{58}(mod 11)$**. Show all work.**
   Fermat's Little Theorem:
   Let 'p' be a prime number and 'a' be an integer.
   When p does not divide a, $a^{p-1} \equiv 1\ (mod\ p)$.

   For this problem: $a = 2, p = 11$.
   Plugging in, we get $2^{10} \equiv 1\ (mod\ 11)$

   We can break down 2^{58} into more manageable exponents:
   $2^{58} \equiv (2^{10})^5 * 2^8 \equiv 2^8 \equiv (2^2)^4 \equiv 4^4 \equiv 3\ (mod\ 11)$
   Therefore, $2^{58} \equiv 3\ (mod\ 11)$.

4. **Make an argument for the size of the keyspace for the Vignere cipher. To do so, of course, you have to define the Vignere cipher.**
   The Vignere Cipher uses a keyword to encrypt a message by shifting each letter of the message by its corresponding letter in the keyword. This keyword is repeated until the end of the message is reached, making it applicable even for larger messages.

   The keyspace for the Vignere Cipher is the number of possible keys that can be used to encrypt a message given the keyword's length. Suppose we use the standard 26-letter alphabet. If every letter could be used in each index of the keyword, then the keyspace would be 26^m, where m is the length of the keyword.

   However, there will always be cases in which the key does not encrypt the message. So, a more useful keyspace would be 26^{m-1}, m of course still representing keyword length.

5. **Use Euler and the Phi function to find the last three digits of 7^{803}. Show all work.**
   To do this, we must solve $7^{803} mod(100)$

   $\phi(1000) = \phi(2^3) * \phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 4 * 100 = 400$

   next we must find gcd(1000, 7):

   $1000 = 142 * 7 + 6$
   $7 = 1 * 6 + 1$
   $6 = 6 * 1 + 0$

   gcd(1000, 7) = 1

   $7^{400} \equiv 1 \, mod \, 1000$
   $7^{800} \equiv 1 \, mod \, 1000$
   $7^{803} \equiv 7^3 \, mod \, 1000$
   $7^{803} \equiv 243 \, mod \, 1000$

   Therefore, the last three digits of 7^{803} are 243

6. **Find $2^{43210} \, (mod \, 101)$. Show all work.**
   By Fermat's Little Theorem, $2^{100} \equiv 1 \, (mod \, 101)$
   $2^{43210} \equiv (2^{100})^{432} * 2^{10} \equiv 2^{10} \equiv (2^2)^5 \equiv 4^5 \equiv 14 \, (mod \, 101)$
   Therefore, $2^{43210} \equiv 14 \, (mod \, 101)$.

7. **The three most recent appearances of Haley's comet were in the years 1835, 1910, and 1986. The next occurrence will be in 2061. Use Fermat to prove that:**
$1835^{1910} + 1986^{2061} \equiv 0\,(mod 7)$
(From *Burton, Elementary Number Theory*)

$1835^{1910} \equiv 1^{1910}\, mod(7)$
$1986^{2061} \equiv 5^{2061}\, mod(7)$

By Fermat's Little Theorem
$5^{6} \equiv 1\, mod(7)$

$2061 = 343 * 6 + 3$

$5^{6^{343}} \equiv 1^{343}\, mod(7)$
$5^{6^{343}+3} \equiv 1^{343} * 5^{3}\, mod(7)$
$5^{2061} \equiv 1^{343} * 5^{3}\, mod(7)$
$5^{2061} \equiv 5^{3}\, mod(7)$
$5^{3} \equiv 6\, mod(7)$

Therefore, $1835^{1910} + 1986^{2061} \equiv 1 + 6 \equiv 0\, mod(7)$

8. **Using Euler, evaluate $2^{10000}\,(mod\,77)$. Show all work.**
gcd(2,77):
$77 = 38 * 2 + 1$
$2 = 2 * 1 + 0$
gcd(2,77) = 1

$\phi(77) = \phi(7) * \phi(11) = (7-1)(11-1) = 60$
$Therefore,\ 2^{60} \equiv 1\,(mod\,77)$

10000 = 166 * 60 + 40

$2^{10000} \equiv 2^{60*166} * 2^{40} mod(77)$
$2^{10000} \equiv 1 * 2^{40} mod(77)$
$2^{10000} \equiv 2^{8^{5}} mod(77)$
$2^{10000} \equiv 256^{5}\, mod(77)$

256 = 3 * 77 + 25

$2^{10000} \equiv 25^{5} mod(77)$

$2^{10000} \equiv 23\, mod(77)$

9. A group of people are arranging themselves for a parade. If they line up three to a row, one person is left over. If they line up four to a row, two people are left over, and if they line up five to a row, three people are left over. What is the smallest number of people required to satisfy the conditions? What is the next smallest number? Show all work. (from Trappe & Washington, *Introduction to Cryptography with Coding Theory*)

Using the Chinese Remainder Theorem:

$x \equiv 1\ (mod\ 3)$
$x \equiv 2\ (mod\ 4)$
$x \equiv 3\ (mod\ 5)$

$n = 3 * 4 * 5 = 60$

$N_1 = \frac{60}{3} = 20$
$N_2 = \frac{60}{4} = 15$
$N_3 = \frac{60}{5} = 12$

$20y_1 \equiv 1\, mod\ 3$
$15y_1 \equiv 1\, mod\ 4$
$12y_1 \equiv 1\, mod\ 5$

$\phi(3) = 2, \phi(4) = 2, \phi(5) = 4$

$y_1 \equiv 20^{-1}\, mod\ 3 \equiv 2^{-1}\, mod\ 3 \equiv\ -1\, mod\ 3$
$y_2 \equiv 15^{-1}\, mod\ 4 \equiv 3^{-1}\, mod\ 4 \equiv\ -1\, mod\ 4$
$y_3 \equiv 12^{-1}\, mod\ 5 \equiv 2^{-1}\, mod\ 5 \equiv\ -2\, mod\ 5$

$x \equiv 1 * y_1 * N_1 + 2 * y_2 * N_2 + 3 * y_3 * N_3\ mod\ 60$
$x \equiv 1 * -1 * 20 + 2 * -1 * 15 + 3 * -2 * 12\ \ mod\ 60$

$x \equiv 1 * -1 * 20 + 2 * -1 * 15 + 3 * -2 * 12\ \ mod\ 60$
$x \equiv 58\, mod(60)$

Therefore the smallest number of people that satisfies the condition is 58. The second smallest number would be the next smallest positive number congruent to $58\, mod(60)$ which is 118.

10. **A warm-up RSA problem**

Use Sage whenever possible and, of course, show all of your work

Let *p* = 11, *q* = 13, *e* = 17, *m* = *99*

A. Find d (2 points)

B. Encrypt *m* (2 points)

That is, find c, the ciphertext encryption of plaintext, *m*.

C. Decrypt *c* (2 points)

That is, find m, the plaintext given in the problem definition

A. Find d

$d \equiv e^{-1} (mod(p - 1)(q - 1))$

$d \equiv 17^{-1} (mod(11 - 1)(13 - 1))$

$d \equiv 17^{-1} (mod(10)(12))$

$d \equiv 17^{-1} (mod\ 120)$

SAGE: $inverse\_mod(17, 120) => 113$

ANSWER: $d = 113$

B. Encrypt m

$c \equiv m^{e} mod(n)$

$c \equiv 99^{17} mod(pq)$

$c \equiv 99^{17} mod(11 * 13)$

$c \equiv 99^{17} mod(143)$

SAGE: $power\_mod(99, 17, 143) => 99$

ANSWER: $c = 99$

C. Decrypt C

$m \equiv c^{d}\ mod(n)$

$m \equiv 99^{113}\ mod(143)$

SAGE: $power\_mod(99, 113, 143) => 99$

ANSWER: $m = 99$