Homework, due to 12:00 pm, May 6, 2015

(1) Solve the system of congruences:
  (a) $x^{137} \equiv 428 \mod 541$;
  (b) $x^{73} \equiv 614 \mod 1159$;
  (c) $x^{751} \equiv 677 \mod 8023$.
  (d) $x^{38993} \equiv 328047 \bmod 401227$. (Hint: $401227 = 607 \cdot 661$)

(2) Let p_1 and p_2 be distinct primes and let e and d be integers satisfying $de \equiv 1 \mod (p_1 - 1)(p_2 - 1)$. Suppose further that c is an integer with $\gcd(c, p_1 p_2) > 1$. Prove that $x \equiv c^d \mod p_1 p_2$ is a solution to the congruence $x^e \equiv c \mod p_1 p_2$.

(3) Alice publishes her RSA public key: modulus $N = 2038667$ and exponent $e = 103$.
  (a) Bob wants to send Alice the message $m = 892383$. What ciphertext does Bob send to Alice?
  (b) Alice knows that her modulus factors into a product of two primes, one of which is $p_1 = 1301$. Find a decryption exponent d for Alice.
  (c) Alice receives the ciphertext $c = 317730$ from Bob. Decrypt the message.

(4) Bob's RSA public key has modulus $N = 12191$ and exponent $e = 37$. Alice sends Bob the ciphertext $c = 587$. Unfortunately, Bob has chosen too small a modulus. Help Eve by factoring N and decrypting Alices message. (Hint. N has a factor smaller than 100.)

(5) For each of the given values of $N = p_1 p_2$ and $(p_1 - 1)(p_2 - 1)$ determine p_1 and p_2.
  (a) $N = p_1 p_2 = 352717$ and $(p_1 - 1)(p_2 - 1) = 351520$;
  (b) $N = p_1 p_2 = 109404161$, and $(p_1 - 1)(p_2 - 1) = 109380612$;
  (c) $N = p_1 p_2 = 172205490419$, and $(p_1 - 1)(p_2 - 1) = 172204660344$.