Elementary Number Theory and Cryptography,
Michaelmas 2011, Problem Sheet 6. (Roots mod p, RSA)

1. (a) Solve the congruence
$$x^{11} \equiv 2 \pmod{17},$$
in other words, compute the eleventh root of 2 modulo 17.
Check your result using the method of successive squaring.

   (b) Solve the following congruence
$$x^3 \equiv 7 \pmod{19}.$$
How many different solutions can you find (modulo 19)?

2. (a) Note that $2^3 \equiv 8 \pmod{23}$. By finding an inverse of 3 in $\mathbb{Z}/22\mathbb{Z}$, or otherwise, find an integer x such that
$$8^x \equiv 2 \pmod{23}.$$

   (b) Try to find a square root of 23 modulo 19. Why does the method given in the lectures not apply here?

3. Michael and Nikita use the Diffie–Hellman key exchange protocol to produce a secret shared key. They have agreed on $p = 101$ and an element $g = 15$ of order $p - 1$, both of which have been made public.
You are the infamous Eve Stroppa and have the task to intercept and decode their messages.
Michael has chosen m and is sending $g^m = 42$ to Nikita, while Nikita has chosen n and is sending $g^n = 24$ to Michael, which establishes a shared secret key for them.
You intercept both messages (i.e. 42 and 24).

   (a) Try your luck: by checking the first few powers of g mod 101, try to find m or n and hence produce their shared key.

   (b) Double check by producing the shared key in two possible ways from the data that they sent.

4. (a) Solve $7d \equiv 1 \pmod{30}$.

   (b) Suppose you write a message as a number $m \pmod{31}$.
Encrypt m as $m^7 \pmod{31}$. How would you decrypt a message, i.e. given $s \pmod{31}$, how do you find m with $s \equiv m^7 \pmod{31}$?
[Hint: Establish an inverse map by raising to an appropriate power.]

5. We use the notation as in the description of the RSA algorithm.

   (a) Your RSA modulus is $n = 91$ and your encoding exponent is $e = 19$. Find the decryption exponent d. Why would $e = 9$ be a bad choice?

   (b) You receive public keys $(n, e) = (55, 7)$ and $(n', e') = (100160063, 17)$. Using the standard bijection of the alphabet and the set of numbers $\{1, \dots, 26\}$, encode your own name (letterwise) using the public key above; then "fatten" each ensuing single digit number into a block of *two* digits, i.e., 1 as 01, …, 9 as 09 (to ensure injectivity of the encoding); finally concatenate all these blocks to a single number N.
Find a decryption exponent for the key (n', e') and decode N. Do you recognise yourself after identifying numbers with letters?

6. (a) (Computer problem:) Try to write a program that takes a string and produces a number for it (i.e. encodes it) using the public key (n', e') in 5(b); write a second program to decode the number into a string.

   (b) Challenge a friend/your marker/your lecturer by producing a public key and a (polite) encoded message in this key that s/he should decode.