Elementary Number Theory and Cryptography,
Michaelmas 2011, Problem Sheet 7. (kth roots mod n, RSA attacks)

1. (a) Find 88^{-1}, the (multiplicative) inverse of 88, in the ring $\mathbb{Z}/703\mathbb{Z}$.
   (b) Find an $x \in \mathbb{Z}$ such that
   $$x^{647} \equiv 64 \pmod{703}.$$
   [Hint: Part (a) and Euler-Fermat may come in handy here, and presumably you will need another idea.]

2. The encoded message ("ciphertext") 5859 was obtained using the RSA algorithm with public key $(n, e) = (11413, 7467)$. Find the original message ("plaintext", here a number < 11413) from which it was obtained.
   [Hint: Factorize 11413 and then produce a decryption exponent.]

3. Let $n = pq$, where p and q are distinct odd primes. Suppose $a \in \mathbb{Z}$ is coprime to n.
   (a) Show that $a^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{p}$ and $a^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{q}$, and deduce that $a^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n}$.
   (b) Using the above (or otherwise), show that if $ed \equiv 1 \pmod{\frac{1}{2}\varphi(n)}$ then
   $$a^{de} \equiv a \pmod{n}.$$
   [Note that this implies that for the RSA algorithm we could also work with $\frac{1}{2}\varphi(n)$ rather than with $\varphi(n)$.]

4. (a) You are given $n = 442931$ and $\varphi(n) = 441600$.
   Factor n into a product of two primes using this data.
   (b) (*) Suppose you are given $n = pqr$ as a product of 3 primes, together with $\varphi(n)$ and the sum of the primes dividing n, i.e. $\psi(n) := p + q + r$. Devise an algorithm to retrieve the three primes from this data.
   Try your algorithm on the following data:
   $$n = 7935412033, \qquad \varphi(n) = 7923420000, \quad \text{and} \quad \psi(n) = 6015.$$
   [Hint: You can assume Cardano's formula for the solutions of a cubic equation: the equation $x^3 + bx + c = 0$ (†) has a solution of the form
   $$x = \sqrt[3]{-\frac{c}{2} + \sqrt[2]{\left(\frac{c}{2}\right)^2 + \left(\frac{b}{3}\right)^3}} + \sqrt[3]{-\frac{c}{2} - \sqrt[2]{\left(\frac{c}{2}\right)^2 + \left(\frac{b}{3}\right)^3}}.$$
   Note that, by a change of variable $x \mapsto x - a_2/3$, you can transform any cubic of the form $x^3 + a_2x^2 + a_1x + a_0 = 0$ into the form (†).
   And don't be afraid to use complex numbers on the way...]

5. (a) Use the Fermat factorization method to write $n = 3525283$ as a product of two primes.
   (b) Show that if $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y \pmod{n}$, then $\gcd(x+y, n)$ is a non-trivial factor of n.
   (c) (*) For the composite number $n = 642401$, you are given the information that
   $$516107^2 \equiv 7 \pmod{n}$$
   and
   $$187722^2 \equiv 2^2 \cdot 7 \pmod{n}.$$
   Try to factor n by hand using this information.
   [Hint: Ideas from Fermat factorization may be useful, as well as part (b).]