Elementary Number Theory and Cryptography, Michaelmas 2014

Problem Sheet 5, (Due: Friday Dec 12, at 12:00 in CM116)

Please hand in Problems 1, 3, 4.
The rest of the Problems will be discussed in the tutorials, (depending on time).

1. Alice and Bob use the Diffie–Hellman key exchange protocol to produce a shared secret key. They have agreed on $p = 101$ and on the primitive element $g = 15$, both of which have been made public.
   You have the role of Eve and have the task to intercept and decode their messages.
   Bob has chosen m and is sending $g^m = 42$ to Alice, while Alice has chosen n and is sending $g^n = 24$ to Bob, 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.

2. 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.]

3. The encrypted message $C = 5859$ was obtained using the RSA algorithm with public key $(n, e) = (11413, 7467)$. Find the original message (here just a number < 11413,usually denote it by X in the lectures) from which it was obtained.

4. You are given $n = 442931$ and $\varphi(n) = 441600$.
   Factor n into a product of two primes using this data.

5. 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 $\varphi(n)$.]

6. (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).]

7. (Factoring with high probability.) [A calculator is probably needed for (a).]

(a) Suppose you are given the public RSA key $(n, e) = (93433, 1071)$, and you obtain the information that the decryption key is $d = 10831$.
Putting $m = d \cdot e - 1$, for which $m = (101100010000000010000000)_2$ is the binary expansion, compute $\rho := 3^{m/16} \pmod{n}$.

(b) Using the ρ from part (a) above, find a factorization of n.