Cryptography I, homework sheet 12

Due: 19 December 2013, 10:45

Please submit your homework electronically; the TAs do not want to receive homework on paper. Please bundle your scans into one pdf file. Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually. To submit your homework, email it to `crypto13@tue.nl`.
In general, you may use computer algebra systems such as mathematica and sage; please submit your code as part of your homework if you end up using a system. Accepted systems/languages: Sage, mathematica, matlab, Pari-GP, Java.

Before the exam please train yourself in doing moduluar arithmetic. Better calculators are programmabge and is useful for you to teach it to do arithmetic modulo numbers; also XGCD is a useful program to implement. Do this before the exam. Of course you can also print and bring huge multiplication tables and hope that I use those numbers. My exercises will not assume that you have polynomial arithmetic.

1. Compute $\varphi(37800)$.
2. Compute $\varphi(193920134995885916749824 0)$.
3. Execute the RSA key generation where $p = 239, q = 433$, and $e = 23441$.
4. RSA-encrypt the message 23 to a user with public key $(e, n) = (17, 11584115749)$. Document how you compute the exponentiation if you only have a pocket calculator.
5. Find the smallest positive integer x satisfying the following system of congruences, should such a solution exist.

$$\begin{aligned} x &\equiv 0 \bmod 3 \\ x &\equiv 1 \bmod 5 \\ x &\equiv 2 \bmod 8 \end{aligned}$$

6. Show how to retrieve the message m in RSA-OAEP from $m'||r'$.

Some more fun with elliptic curves of different shapes: `http://cr.yp.to/talks/2008.05.12/zoo.html`.