Cryptography I, homework sheet 3

Due: 01 October 2010, 10:45

Attention: one-line answers using a computer algebra system do *not* count. But it is a good moment to familiarize yourself with some system(s) so that you know how to solve similar problems for real life examples and to verify your answers. You may use a computer algebra system to compute subresults, such as factorizations, modular reduction, multiplication, squaring.

1. Show that $M_3(\mathbb{Z}/2)$ forms a ring, where $M_3(\mathbb{Z}/2)$ denotes the set of all 3×3 matrices with entries in $\mathbb{Z}/2$. Is this ring commutative?
2. Compute $\varphi(37800)$.
3. Compute $\varphi(193920134995885916749824 0)$.
4. Give all elements in $(\mathbb{Z}/12)^\times$.
5. Give all elements in $(\mathbb{Z}/21)^\times$.
6. Execute the RSA key generation where $p = 239, q = 433$, and $e = 23441$.
7. RSA-encrypt the message 23 to a user with public key $(e, n) = (17, 11584115749)$. Document how you compute the exponentiation.