Cryptography I, homework sheet 2

Due: 18 September 2014, 10:45

Please hand in your homework in groups of two or three. To submit your homework, email it to `crypto14@tue.nl`.

Please write the names and student numbers on the homework sheet. Please indicate your home university and study direction.
You can use a calculator or some computer algebra system for these exercises, but make sure to document all intermediate computations.

1. Compute $\varphi(37800)$.

2. Execute the RSA key generation where $p = 239, q = 433$, and $e = 23441$.

3. 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.

4. Find the smallest positive integer x satisfying the following system of congruences, should such a solution exist.

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

5. Users A, B, C, D, and E are friends of S. They have public keys $(e_A, n_A) = (5, 62857), (e_B, n_B) = (5, 64541), (e_C, n_C) = (5, 69799), (e_D, n_D) = (5, 89179)$, and $(e_E, n_E) = (5, 82583)$. You know that S sends the same message to all of them and you observe the ciphertexts $c_A = 11529, c_B = 60248, c_C = 27504, c_D = 43997$, and $c_E = 44926$. What was the message?