CSE 20: Week 4 Howework Solutions

Douglas Turnbull
Department of Computer Science, UC San Diego
`dturnbul@cs.ucsd.edu`

October 20, 2005

This week we introduced many number theory concepts and showed how they relate to cryptography. You need to know how to factor a natural number n, and how to find the gcd(m,n) (and lcm(m,n)) of two natural numbers n and m using the Euclidean algorithm.

Additional cryptography concepts include: plaintext vs. ciphertext, public and private keys, the discrete log problem, the factorization problem, Euler's ϕ function, the Diffie-Hellman (symmetric key-exchange) protocol, and the RSA protocol. You need not memorize the intricate details of these concepts, but you should have a high level understanding of why they are important, how they are used in practice, and why they work.

NT: Solutions to 1.21, 1.27, 2.2, 2.4, 2.10, and 2.13 are found in the back of your textbook.

NT 2.2: The solution key has a typo. Where it reads 'multiplying one of $\{1, 2, 2^{\}}$', it should read 'multiplying one of $\{1, 2, 2^2\}$.'

NT 2.13: The solution key is wrong. The final statement should read: $2^{37} \equiv 2 \times (13) \equiv 51$.