UNIVERSITY OF THE WITWATERSRAND
SCHOOL OF MATHEMATICS

MATH 3003: Coding and Cryptography Tutorial Questions
Suggested Answers and Hints

Tutorial 6

1. $r = 48$. Note: (i) $231 = 128 + 64 + 32 + 4 + 2 + 1$; (ii) $\phi(49) = 42$.

2. (a) Residue is 3 (mod 13). Euler's Theorem is quicker than modular exponentiation.

   (b) Number of decimal digits is 30103. The number of decimal digits in a positive integer N is $\log_{10}\lceil N \rceil$, where $\lceil N \rceil$ is the ceiling function, i.e., the least integer $\geq N$.

3. $p = \frac{(n-\phi(n)+1)+\sqrt{(n-\phi(n)+1)^2-4n}}{2}$ and $q = \frac{(n-\phi(n)+1)-\sqrt{(n-\phi(n)+1)^2-4n}}{2}$.
   Obtain the simultaneous solutions of $pq = n$ and $(p-1)(q-1) = \phi(n)$.

4. $(p, q) = (97, 151)$ or $(p, q) = (151, 97)$. Use Question 3.

5. Hint: n has only two divisors > 1 namely p and q.

6. This is equivalent to the probability that if x is a randomly selected integer between 1 and n, then x is a multiple of p or q.

   But there are $\lfloor \frac{n}{p} \rfloor = q$ multiples of p, and $\lfloor \frac{n}{q} \rfloor = p$ multiples of q. Now apply elementary inclusion-exclusion reasoning to obtain the first part.

   The estimate is $< \frac{1}{10^{99}}$. Substitute $p = q = 10^{100}$ into the given expression and obtain an upper bound.

7. The ciphertext is 1215 1224 1471 0023 0116.

8. The plaintext message is "GREETINGSX".

9. (a) $(e, n) = (5, 16781)$.

   (b) $d \equiv 6605 \pmod{16512}$.

   (c) Plaintext $P \equiv 5374^{6605} \equiv 6925 \pmod{16781}$ (needs a computer algebra system!)

10. The signed ciphertext is 0250 1560 0326.