Tutorial 11: Public Key Cryptography

1. Using the prime numbers 5 and 13 as a starting point, generate public and private keys for the RSA algorithm (the number 29 can be inverted by trial and error in a couple of minutes). Hence write down the encryption and decryption functions corresponding to your key choice. Use these functions to encrypt and decrypt a suitably small message, say M = 2. Note using the above keys this can be done with an ordinary calculator in about 10 minutes.

2. Rufus has published his public key, it is *(n,e) = (143,103)*. From this determine his private key.

3. Rufus is having trouble with the RSA data listed below. Determine, in each case what the problem is. (all the symbols have the usual meaning in the context of RSA)
   a. p = 9; q = 13; e = 17; M = 8
   b. p = 13; q = 17; e = 9; M = 2
   c. p = 19; q = 13; e = 11; M = 311
   d. p = 7; q = 13; e = 11; M = 11

4. Rufus agrees that RSA may be useful for encrypting integers but cannot be applied to binary files, which contain bytes. How do you answer him?

5. In the proof that the RSA deciphering function is the inverse its enciphering function, the following use is mad of Euler's theorem,:
   $M_j^{\varphi(n)} \bmod n = 1$
   Where φ(n) is the Euler totient function and the other symbols have their usual meanings. Euler's theorem requires that both M_j and n are relatively prime and that $M_j < n$. Explain why these assumptions are valid in the context of RSA.

6. Given the product of two prime numbers 11*7 = 77 and the choice of RSA private key (77,43) determine and write down the public key for this cryptosystem. Table 1 provides the data you need to do this. Hence write down the encryption and decryption functions for the cryptosystem.

```
43 * 1  = 0 * 60 + 43
43 * 2  = 1 * 60 + 26
43 * 3  = 2 * 60 +  9
43 * 4  = 2 * 60 + 52
43 * 5  = 3 * 60 + 35
43 * 6  = 4 * 60 + 18
43 * 7  = 5 * 60 +  1
43 * 8  = 5 * 60 + 44
43 * 9  = 6 * 60 + 27
43 * 10 = 7 * 60 + 10
```

7. Explain how one would attempt to derive the private part of an RSA key from its public key and why this is a computationally difficult task.

8. 1024 bit RSA refers to an implementation of RSA in which each part *(e,n)* of the public key and the private key *(d,n)* is 1024 bits long. What should the size in bits, of a message and ciphertext blocks be in this implementation.

9. Explain why in the above question, the keyspace is not 2^{1024}. Imagine that the computationally challenged race of Zorks has invented an 8 bit version of RSA. For $n = 33$, find the keyspace of their cipher by determining every possible set of keys. Note: do not count cases where the public and private keys are swapped as additional keys. Also be aware not to count degenerate keys such as $e = d$ and such as produced by $p = 1$.

[8marks, Exam 2004]