Long question A

State carefully the Fermat-Euler theorem, defining any terms that you use. [4 marks]

Explain how calculating $a^{n-1} \pmod n$ for various values of a can be used to show that n is composite without actually finding its factors. By considering $561 = 11 \times 51$ or otherwise, show that the test is not perfect and suggest an improvement to it more selective. [6 marks]

Derive the RSA system for public key cryptography and explain how this can be used both to send messages that are kept secret from an interceptor and to prove the identity of a sender. [6 marks]

Show that knowledge of the secret key as well as the public key allows an interceptor to factor the modular base being used. [4 marks]

Answer

Given $m \geq 2$ and a with $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod m$ where $\varphi(m)$ is Euler's totient function. $(3-1)|(561-1)$,

If there is a value $a \leq p$ for which $a^{p-1} \not\equiv 1 \pmod p$, then p is not prime. (11-1)|(561-1) and (51-1)|(561-1) so $a^{(561-1)} \equiv 1 \pmod p$ for all p by the CRT. Consider $a^{(p-1)/2} \not\equiv \pm 1 \pmod p$ instead.

Pick primes p and q with product m so $\varphi(m) = (p-1)(q-1)$. Pick e and d with $ed \equiv 1 \pmod{\varphi(m)}$. Then $(a^e)^d \equiv a \pmod m$. Publish m and e while keeping d secret.

Suppose $de - 1 = n\,\varphi(m)$. n can be found by rounding up $(de - 1)/m$. Hence calculate $\varphi(m)$. p and q are the roots of $x^2 - (m + 1 - \varphi(m))x + m = 0$.