Section 7 Lecture 44 – Digital Signatures - Exercise

Follow these steps to show how a digital signature can be created and checked using RSA, where Alice has private keys $p = 7$ and $q = 13$, and public exponent $e = 5$ and Bob has private keys $p = 11$ and $q = 17$ and public exponent $e = 7$

- Set up all the keys for both Alice and Bob, and then perform the usual RSA encryption of Alice's message $m = 19$ using RSA (exactly as we did when we discussed RSA earlier in the course) and check that Bob can decrypt it at the other end
- Hash the message $m = 19$ by converting it (mod 16), writing this in binary, reversing the binary string and then writing as a number again to obtain h
- Create Alice's signature by finding $s = h^d \pmod{n}$ where d is Alice's private key d and n is her public key, and then encrypt this signature using Bob's public key in the usual way
- Show that if Bob decrypts the signature in the usual way, and then performs $s^e \pmod{n}$ (where e is Alice's public exponent) then he recovers the hash h (which he can check by hashing the decrypted message $m = 19$ exactly as Alice did)