Section 7 Lecture 44 – Digital Signatures - Solution

Setting up the keys

Alice has public key $n = pq = 7 \times 13 = 91$. She calculates $\varphi(n) = 6 \times 12 = 72$, and then needs to find her private key d such that $de = 1 \pmod{72}$ – calculate in any way you like to get that $d = 29$ is a suitable solution since $5 \times 29 = 145 = 1 \pmod{72}$.

Bob has public key $n = pq = 11 \times 17 = 187$. He calculates $\varphi(n) = 10 \times 16 = 160$, and then needs to find his private key d such that $de = 1 \pmod{160}$ – calculate in any way you like to get that $d = 23$ is a suitable solution since $7 \times 23 = 161 = 1 \pmod{160}$

Encrypting and decrypting

Alice calculates $c = m^e \pmod{n}$ where n and e are Bob's public keys which gives $19^7 \pmod{187} = 145$ and sends this encrypted message to Bob. Bob calculates $m = c^d \pmod{n} = 145^{23} \pmod{187} = 19$ which recovers the original message, and so encryption and decryption works.

Signature

19 (mod 16) = 3 which is 0011 in binary, so reversing gives 1100 which is 12 as a decimal number, so $h = 12$. Alice encrypts this using $s = h^d \pmod{n}$ where d is her private key and n her public key, and so her signature is $12^{29} \pmod{91} = 38$, which she then encrypts using Bob's public keys e and n to get the encrypted signature $s^e \pmod{n} = 38^7 \pmod{187} = 47$ which she sends to Bob.

Bob decrypts the signature using his private key d to get $47^{23} \pmod{187}$ to get Alice's signature $s = 38$.

He then calculates $s^e \pmod{n}$ where e and n are Alice's public keys, which gives $38^5 \pmod{91} = 12$ which matches the hash he obtains from the message (in exactly the same way as Alice) and so has verified the signature.