Introduction to Cryptography: Assignment 12

Group number 57

Elwin Tamminga s1013846

Lucas van der Laan s1047485

1

(a) 19 and 23 are (co-)prime, thus
$\varphi(437) = \varphi(19 \cdot 23) = \varphi(19) \cdot \varphi(23) = (19 - 1) \cdot (23 - 1) = 18 \cdot 22 = 396$

(b) $\#(\mathbb{Z}/437\mathbb{Z})^*$ contains all integers smaller than 437 and coprime to 437, thus
$\#(\mathbb{Z}/437\mathbb{Z})^* = \varphi(437) = 396$.

(c) $c = m^e \mod n = 104^7 \mod 437 = 384$

(d) $A = (n, e) = (437, 7)$
$\varphi(n) = \varphi(437) = 396$
$ed \equiv 1 \pmod{\varphi(n)}$
$7 \cdot d \equiv 1 \pmod{\varphi(437)}$
$d \equiv 7^{-1} \pmod{396}$

Extended Euclidean Algorithm:

$$\begin{aligned} 396 &= 7 \cdot 56 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \end{aligned}$$

$$\begin{aligned} 4 &= 396 - 7 \cdot 56 \\ 3 &= 7 - 4 \cdot 1 \\ 1 &= 4 - 3 \cdot 1 \end{aligned}$$

$$\begin{aligned} 4 - 3 &= 1 \\ 4 - (7 - 4) &= 1 \\ 4 - 7 + 4 &= 1 \\ 2 \cdot 4 - 7 &= 1 \\ 2 \cdot (396 - 7 \cdot 56) - 7 &= 1 \\ 2 \cdot 396 - 112 \cdot 7 - 7 &= 1 \\ 2 \cdot 396 - 113 \cdot 7 &= 1 \end{aligned}$$

$d = -113 \mod 396 = 283$

(e) $m' = C'^d \mod n = 384^{283} \mod 437 = 104$.

2

$p = 19, q = 23$

(a) $d_p = 7^{-1} \mod 18$
$d_q = 7^{-1} \mod 22$

$\varphi(18) = \varphi(2 \cdot 3^2) = \varphi(2) \cdot \varphi(3^2) = 1 \cdot (3-1) \cdot 3^{2-1} = 6$
$\varphi(22) = \varphi(2) \cdot \varphi(11) = 1 \cdot 10 = 10$

$d_p = 7^{-1} \mod 18 = 7^{\varphi(18)-1} \mod 18 = 7^{6-1} \mod 18 = 13$
$d_q = 7^{-1} \mod 22 = 7^{\varphi(22)-1} \mod 22 = 7^{10-1} \mod 22 = 19$

Using CRT, we can verify this by using Alice's private key from 1.d (283):
$d_p = d \mod (p-1) = 283 \mod 18 = 13$
$d_q = d \mod (q-1) = 283 \mod 22 = 19$

(b) $c_p = C \mod p = 384 \mod 19 = 4$
$c_q = C \mod q = 384 \mod 23 = 16$

$m_p = c_p^{d_p} \mod p = 4^{13} \mod 19 = 9$
$m_q = c_q^{d_q} \mod q = 16^{19} \mod 23 = 12$

(c)

$$\begin{aligned} m &\longleftarrow m_q + q \cdot (t \cdot i_q \mod p) \\ t &\longleftarrow (m_p - m_q) \mod p \\ i_q &\longleftarrow q^{-1} \mod p \end{aligned}$$

$i_q = 23 = 23^{\varphi(19)-1} = 23^{17} \equiv 5 \pmod{19}$
$t = 9 - 12 \mod 19 = 16$
$m = 12 + 23 \cdot (16 \cdot 5 \mod 19) = 12 + 23 \cdot 4 = 12 + 92 = 104$

3

(a) Not it is not IND-CPA secure, because the deterministic nature of textbook RSA results in that a plaintext will always return the same ciphertext. This means that when we send m_1 and m_2, the challenger chooses a message and sends back the ciphertext c. We then just have to encrypt m_1 and m_2 and compare the ciphertexts of the messages with c. This reveals which message was encrypted, and thus textbook RSA is not IND-CPA secure.

(b) Eve can create a forgery by doing m_1^i and s_1^i with $i > 1$, which can be used to create any forgeries she wants in that scope.
$m_1^i = s_1^{i \cdot e} \mod n$
If we intercept one message, e.g. using the values from the last assignments:
$m = 104, d = 283, n = 437, e = 7$
$s = 104^{283} \mod 437 = 215$
We can then verify the signature using $m = 215^7 \mod 437 = 104$

If we then forge a new message using $i = 4$, we get:
$m^4 = 104^4 \mod 437 = 82$
$s^4 = 215^4 \mod 437 = 232$

This is valid, because:
$232^7 \mod 437 = 82 = m^4$