MTH6115 Cryptography

Solutions 11

---

1 Since $163-1 = 162 = 2\cdot 3^4$, in order to show that 2 is a primitive element modulo 163 we must show that $2^{162} \equiv 1 \pmod{163}$, while $2^{162/2} = 2^{81} \not\equiv 1 \pmod{163}$ and $2^{162/3} = 2^{54} \not\equiv 1 \pmod{163}$. The calculations to do this are given below.

$$2^3 = 8, \quad 2^9 = 512 \equiv 23, \quad 2^{27} = (2^9)^3 \equiv 23^3 = 12167 \equiv 105 \equiv -58,$$
$$2^{54} = (2^{27})^2 \equiv (-58)^2 = 3364 \equiv 104 \equiv -59,$$
$$2^{81} = 2^{27} \cdot 2^{54} \equiv (-58) \cdot (-59) = 3422 \equiv 162 \equiv -1, \quad 2^{162} = (2^{81})^2 \equiv (-1)^2 = 1.$$

For the rest of this question, the (not-so-)subtle hint is to search for an integer n such that $n \equiv a \pmod{163}$ and n has the form $n = (-1)^{\varepsilon} \cdot 2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma} \cdot 7^{\delta}$. Then $\log_2(n) = 81\varepsilon + \alpha + 101\beta + 15\gamma + 73\delta$, which we may reduce modulo 162. Therefore we have:

(a) We have $20 = 2^2 \cdot 5$, and so $\log_2(20) = 2 + 15 = 17$.

(b) We have $90 = 2 \cdot 3^2 \cdot 5$, and so $\log_2(90) = 1 + 2 \cdot 101 + 15 = 218 \equiv 56$.

(c) We have $11 + 3 \cdot 163 = 500 = 2^2 \cdot 5^3$, and so $\log_2(11) = 2 + 3 \cdot 15 = 47$. (Alternatively, $11 - 2 \cdot 163 = -315 = (-1) \cdot 3^2 \cdot 5 \cdot 7$, and so $\log_2(11) = 81 + 2 \cdot 101 + 15 + 73 = 371 \equiv 47$.)

(d) We have $161 - 163 = -2 = (-1) \cdot 2$, and so $\log_2(161) = 81 + 1 = 82$. (Alternatively, $161 + 163 = 324 = 2^2 \cdot 3^4$, and so $\log_2(161) = 2 + 4 \cdot 101 = 406 \equiv 82$.)

(e) We have $26 + 163 = 189 = 3^3 \cdot 7$, and so $\log_2(26) = 3 \cdot 101 + 73 = 376 \equiv 52$. (Alternatively, $26 - 2 \cdot 163 = -300 = (-1) \cdot 2^2 \cdot 3 \cdot 5^2$, and so $\log_2(26) = 81 + 2 + 101 + 2 \cdot 15 = 214 \equiv 52$.)

(f) We have $67 - 163 = -96 = (-1) \cdot 2^5 \cdot 3$, and so $\log_2(67) = 81 + 5 + 101 = 187 \equiv 25$.

In all cases, congruences at the end are modulo 162.

2 Let us take the arbitrary value of k to be 37. Then the message $x = 164$ gets encrypted to (g^k, xh^k), where both parts are taken modulo $p = 619$. So here I get encryption $(402, 484)$. Other answers are possible.

The decryption of $(581, 201)$ is $201 \cdot 581^{-110} \equiv 297 \pmod{619}$. (The value of k used to encrypt this was 75, but you do not need to find this, and I used the discrete logarithm to do so.)

3 The rest of Alice's and Bob's public keys are

$$h_A \equiv 2^{43} \equiv 7 \bmod 107,$$

$$h_B \equiv 2^{23} \equiv 22 \bmod 107.$$

To encrypt $x = 35$, pick a random number k prime to 106 and encrypts x as $(2^k, x \cdot 22^k)$ modulo 107. For example, if you pick $k = 11$, then $2^{11} \equiv 15 \bmod 107$, $22^{11} \equiv 82 \bmod 107$ and the encrypted message is $(2^{11}, 35 \cdot 22^{11}) = (15, 88) \bmod 107$.

To sign $y = 27$ Alice picks a random number m (coprime to 106), and calculates $l = m^{-1} \bmod 106$. Then she calculates $z_1 \equiv 2^m \bmod 107$ and $z_2 = (y - az_1)l \bmod 106$ and sends (y, z_1, z_2). For example, if she picks $m = 21$, then $l = -5$ is the inverse of m modulo 106. Then, $z_1 \equiv 2^{21} \equiv 59 \bmod 107$ and $z_2 \equiv (27 - 43 \cdot 59)(-5) \equiv 42 \bmod 106$. The signed message is $(27, 59, 42)$.

4 (a) We have $5^{251} \equiv -1 \pmod{503}$, and $7^{251} \equiv 1 \pmod{503}$. (We use the 'squaring table' for the fast computation of these numbers.) So, 5 is a primitive root, but 7 is not.

(b) We have $2^{659} \equiv 1 \pmod{1319}$, $7^{659} \equiv 1 \pmod{1319}$, and $13^{659} \equiv -1 \pmod{1319}$. So, 13 is a primitive root, but 2 and 7 are not.