Cryptography 2018 Final Solutions

1. Under the RSA cryptosystem with $N = 55$ and public encryption exponent $e = 7$, Bob encrypts a message m to $c = 9$. What is m? Hint: It shouldn't take too long to find the inverse of 7 just by trying values. And the following may help:

i	0	1	2	3	4	5
$2^i \mod 55$	9	26	16	36	21	36

Solution

As $N = 55$, p and q are 5 and 11, so the decryption exponent is the inverse of 7 modulo $\phi(55) = 40$. Trying multples of 7 near $40, 80, \ldots$ we find that $7 \cdot 23 = 161$ so $7^{-1} \equiv_{40} 23$. So to decrypt 9 we calculate $9^{23} = 9^{16+4+2+1} \equiv_{55} 21 \cdot 16 \cdot 26 \cdot 9 = (16 \cdot 26) \cdot (21 \cdot 9) = 416 \cdot 189 \equiv_{55} 31 \cdot 24 \equiv_{55} 7 \cdot 12 \equiv_{55} \boxed{29}$.

2. Show that a Carmichael number must be the product of distinct primes.

Solution

Assume that $n = p^2 m$ is a Carmicheal number. So $a^n \equiv_n a$ for all a in $\mathbb{Z}_n$. In particular this holds for $a = p$, so $p^n \equiv_n = p$, and so $p^2 \mid n \mid p^n - p$. But then $p \mid p^{n-1} - 1$. This is only possible if $n = 1$, a contradiction.

3. Use the Miller-Rabin Test to decide if 29 is prime. (Use three test numbers. You may choose small numbers to make computation easier.)

Solution

$28 = 2^2 \cdot 7$ so in $\mathbb{Z}_{29}$ we compute

a	a^7	$a^{7 \cdot 2}$	$a^{7 \cdot 2^2}$	witness?
2	12	-1	1	no
3	12	-1	1	no
5	-1	1	1	no

4. Consider the Goldwasser-Micali cryptosystem.

   (a) What properties do the public key elements N and a have? (How do we choose them?)

   (b) Alice chooses $N = 667 (= 23 \cdot 29)$ and $a = 157$ and Bob uses them to encode a message m to $c = 218$. What is m?

Solution

(a) N is the product of two secret primes p and q, and a is a quadratic non-residue modulo p and q.
(b) Computing $\left(\frac{218}{23}\right) = \left(\frac{11}{23}\right) = -\left(\frac{23}{11}\right) = -\left(\frac{1}{11}\right) = -1$, we see that 218 is a non-residue, and so $m = 1$.

5. Show that if a is a quadratic residue modulo $p \equiv_4 3$, then then $a^{\frac{p+1}{4}}$ is its square root.

Solution

Let $a = b^2$. First assume that b is not primitive. Then it has order dividing $\frac{p-1}{2}$, so

$$a^{\frac{p+1}{4}} = b^{2\frac{p+1}{4}} = b^{\frac{p+1}{2}} = b^{\frac{p-1}{2}+1} = b,$$

as needed. Now, as both $b^2 = a$ and $(-b)^2 = a$, it is enough to show that not both of b and $-b$ are primitive. Assume that b is. So $b^{p-1} \equiv_p 1$, and so $b^{\frac{p-1}{2}} \equiv -1$, as 1 and -1 are the only square roots of 1 modulo a prime. But $\frac{p-1}{2}$ is odd, because $p \equiv_4 3$, and so $(-b)^{\frac{p-1}{2}} = (-1)b^{\frac{p-1}{2}} = (-1)(-1) = 1$, showing that $-b$ is not primitive.

6. Let E be $y^2 = x^3 + 2x - 6$. Decide if there is a point (x, y) in $E(\mathbb{F}_{79})$ with $x = 5$, and if there is, find it.

Solution

Where $5^3 + 2(5) - 6 = 129 \equiv_{79} 50$, the Jacobi symbol is

$$\left(\frac{50}{79}\right) = \left(\frac{2}{79}\right) = 1$$

so x is a q.r., and so yes there is a point (x, y) with $x = 5$.
As $79 \equiv_4 3$, one square root of 50 is $50^{\frac{79+1}{4}} = 50^{20} = 50^{16+4}$. Computing, modulo 79: $50^4 \equiv 73 \equiv -6$ and $50^{16} \equiv (-6)^4 \equiv 32$, we get $50^{20} = (-6)32 \equiv 45$. So $(5, 45)$ is a point on our curve.

7. Consider the El Gamal PKC over the elliptic curve $E : Y^2 = X^3 + 5X + 2$ over $\mathbb{F}_{11}$ based on the max-order element $P = (2, 3)$ having order 10.

i	$i \cdot (2,3)$
1	$(2,3)$
2	$(8,2)$
3	$(5,3)$
4	$(4,8)$
5	$(3,0)$
6	$(4,3)$
7	$(5,8)$
8	$(8,9)$
9	$(2,8)$
10	zero

Alice publishes a public encryption key is $Q_A = (5,8)$, decode the message M that encrypts to $C_1 = (5,8)$, $C_2 = (2,3)$.

Solution

As $(5,8) = 7P$, the secret encryption key is $n_A = 7$. We know that $C_1 = kP$ and $C_2 = M \oplus kQ_A = M \oplus n_A kP$ for some k so we decrypt by calculating

$$\begin{aligned} M &= C_2 \ominus n_A C_1 \\ &= (2,3) \ominus 7 \cdot (5,8) \\ &= 1 \cdot P \ominus 49P \\ &= (-48) \cdot P \\ &= 2 \cdot P = (8,2). \end{aligned}$$

8. Let $M = (m_1, \ldots, m_n)$ be a sequence of integers.
   (a) M is *superincreasing* if _____.
   (b) Show that if M is superincreasing, then the map

$$e : \mathbb{F}_2^n \to \mathbb{Z} : v \mapsto v \cdot M$$

   is injective.

Solution

(a) $\ldots m_\alpha > \sum_{i=1}^{\alpha-1} m_i$ for all $\alpha > 1$.
(b) Let $v = (v_1, \ldots v_n)$ and $v' = (v'_1, \ldots, v'_n)$ in $\mathbb{F}_2^*$ be distinct vectors and let $\alpha \in [n]$ be the highest index for which $v_\alpha \neq v'_\alpha$. We may assume that $v_\alpha = 1$ and $v'_\alpha = 0$. We show that $e(v) = v \cdot M > v' \cdot M = e(v')$, proving that e is injective. Indeed using that $v_\alpha = 1$ and $v_{\alpha'} = 0$ for equality (1), and the fact that M is superincreasing for (2), we get

$$v \cdot M \geq \sum_{i=\alpha}^{n} v_i m_i \overset{(1)}{=} m_\alpha + \sum_{i=\alpha}^{n} v'_i m_i \overset{(2)}{>} \sum_{i=1}^{\alpha-1} m_i + \sum_{i=\alpha}^{n} v'_i m_i \geq \sum_{i=1}^{n} v'_i m_i = v' \cdot M.$$