Cryptography Final Solutions

1. What do you calculate to decrypt the message 14 that you intercept under the RSA cryptosystem with $N = 35$ and public encryption exponent $e = 5$.

   Sol: As $N = 35$, p and q are 5 and 7, so the decryption exponent is the inverse of 5 modulo 24. This is 5. So to decrypt 14 we calculate 14^5 modulo 35.

2. Let $p < q$ be odd primes, and assume that for RSA with $N = pq$, e_1 and e_2 are two different encrytion exponents. If the corresponding decryption exponents d_1 and d_2 satisfy $e_1d_1 = 41$ and $e_2d_2 = 57$. Find p.

   Sol: *On the test, I forgot to ask for odd primes, so $p = 2$ was also an answer*

   We know that both $e_1d_1 - 1 = 40$ and $e_2d_2 - 1 = 56$ are multiples of $(p-1)(q-1)$, so $(p-1)(q-1)$ divides $\gcd(40, 56) = 8$. As $p < q$ are odd primes, this gives us that $p = 3$ (and $q = 5$).

3. (a) Show that 2 is a Miller-Rabin witness to the fact that 21 is composite.

   Sol: Modulo 21 we have that $2^5 = 11 \neq \pm 1$, and $2^{10} \neq -1$ so 2 is a Miller-Rabin witness that 21 is not prime.

   (b) Is it an Euler witness?

   Sol: Yes, $2^{20} \equiv 4 \neq 1 \bmod 21$.

4. Use Pollard's $p - 1$ method to find a factor of the product $n = 55$ of two primes. (Hint: A base of 2 will work. You might need that $9^4 = 6581 \equiv 16 \bmod 55$.)

   Sol: Computing the exponents modulo n, we get

   - $\gcd(55, 2^{2!} - 1) = \gcd(55, 3) = 1$,
   - $\gcd(55, 2^{3!} - 1) = \gcd(55, 8) = 1$
   - $\gcd(55, 2^{4!} - 1) = \gcd(55, 15) = 5$

   So 5 is a factor of 55. Dividing, the other factor is 11.

5. Show that if $n > 2$ is even, then $2^n - 1$ is not prime.

   Sol: Indeed, if $n = 2m$ then $2^n - 1 = 2^{2m} - 1 = (2^m - 1) \cdot (2^m + 1)$, and as $m > 1$ both of these factors are greater than 1.

6. (a) Decide if 24 is a quadratic residue modulo 155.

   Sol: As $155 = 5 \cdot 31$, we determine if 24 it is a quadratic residue modulo 5 and 31. We have

   $$\left(\frac{24}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = 1,$$

   so it is a residue modulo 5. On the other hand,

   $$\left(\frac{24}{31}\right) = \left(\frac{2}{31}^3 \frac{3}{31}\right) = 1^3 \cdot - \left(\frac{31}{3}\right) = - \left(\frac{1}{3}\right) = -1,$$

   so 24 is a non-residue modulo 31, which implies that it is a non-residue modulo 155. Alternately, you could have just computed $\left(\frac{24}{155}\right)$, but this would not have helped if it had turned out to be 1.

(b) Decide if 1000000 is a quadratic residue modulo 23908100. (Hint: This shouldn't take long.)

Sol: As the modulus is even, you can't use symbols here. And even when you can use symbols, you can't cancel, as many of you tried to do. But as I was trying to say in the hint, there is an easy solution. As $1000000 = (1000)^2$ is a square, it is a square modulo any base, so yes, it is a quadratic residue.

7. (a) Show that $P = (4, 5)$ is a point on the elliptic curve $E : Y^2 = X^3 + 4X + 1$ over $\mathbb{F}_7$.

Sol: Modulo 7 we have $5^2 \equiv 4 \equiv (4)^3 + 4(4) + 1$.

$Q = (0, 1)$ is another point. Compute $Q \ominus P$ on this curve.

Sol: This is the same as computing $Q \oplus (-P) = (0, 1) \oplus (4, 2)$; we do this. The slope of the line through the points Q and $-P$ is

$$\lambda = \frac{2-1}{4-0} = \frac{1}{4} \equiv 2(\mod 7).$$

The x-value of the third point on this line is $\lambda^2 - 0 - 4 \equiv 0 \mod 7$, and the y-value is $\lambda(0 - 0) + 1 \equiv 1$. So $Q \ominus P = (0, -1) = (0, 6)$

8. Using (the symmetric variation on) fast powering for elliptic curves, how many operations ($\oplus$ or $\ominus$) would it take you to compute $22P$ for some point P (of order greater than 22) on an elliptic curve.

Sol: $22 = 16 + 8 - 2$ so we could do it with four operations to compute $2P, 4P, 8P$ and $16P$, and then two more to compute $22P = 16P \oplus 8P \ominus 2P$. So we could do it in 6 operations. (Using $22 = 16 + 4 + 2$ also uses 6 operations.)

9. 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

Where the public key is $A = (4, 3)$, decode the message m that encrypts to $c_1 = (5, 3)$, $c_2 = (2, 3)$.

Sol: As $(4, 3) = 6P$, the secret encryption key is $k_a = 6$. We know that $c_1 = k_b P$ and $c_2 = m \oplus k_a k_b P$ so we decrypt by

calculating

$$\begin{aligned} m &= c_2 \ominus k_a c_1 \\ &= (2,3) \ominus 6 \cdot (5,3) \\ &= 1 \cdot P \ominus 6 \cdot 3 \cdot P \\ &= (1-18) \cdot P \\ &= 3 \cdot P = (5,3). \end{aligned}$$

Note that P has order 10 so $-17P = -7P = 3P$. Several people treated these integers as though there were in $\mathbb{F}_{11}$.