RSA.

Bob would like to receive encrypted messages from Alice via RSA.

1. Bob chooses $p = 7$ and $q = 11$. His public key is (N, e).

   (a) $N =$

   What is N a function of p and q?

   $N = pq = 77$

   (b) e is relatively prime to the number:

   The answer is not N. It is derived from Fermat's little theorem.

   e is relatively prime to $(p-1)(q-1) = 60$. This is because when the message x^e is raised to the power of $d = e^{-1} \bmod 60$, we get $x^{ed} \bmod N = x^{k(p-1)(q-1)+1} \bmod N = x(x^{k(p-1)(q-1)}) \bmod N = x \bmod N$ according to Fermat's little theorem.

   (c) e need not be prime itself, but what is the smallest prime number e can be? Use this value for e in all subsequent computations.

   $e =$

   The smallest prime number that is coprime with 60 is 7, so $e = 7$

   (d) What is $gcd(e, (p-1)(q-1))$?

   Related to part (b)

   e is required to be coprime to $(p-1)(q-1)$, which means their gcd is 1 by definition

   (e) What is the decryption exponent d?

   $d =$

   Recall that $d = e^{-1} \mod (p-1)(q-1)$.

   To find d, we need to compute $e^{-1} \bmod 60$. Recall that $e = 7$ from part c). We can find the multiplicative inverse of $7 \bmod 60$ using the egcd algorithm, which gives us 43.

   (f) Now imagine that Alice wants to send Bob the message 30. She applies her encryption function E to 30. What is her encrypted message?

   $E(x) =$

   Recall that $E(x) \equiv x^e \mod N$.

   Alice uses the public key $(77,\ 7)$ to encode her message as $30^7 \bmod 77$. We can compute this value using a combination of the Chinese Remainder Theorem and Fermat's Little Theorem.

   Let $y = 30^7 \bmod 77$. We first use Chinese remainder theorem to express $y \bmod 7$ and $y \bmod 11$:

$$\begin{aligned} y &\equiv a \bmod 7 \\ y &\equiv b \bmod 11 \end{aligned}$$

   We can solve for a and b using Fermat's Little Theorem:

$$\begin{aligned} a &= 30^7 \bmod 7 \\ &= 30 \times (30^6) \bmod 7 \\ &= 30 \bmod 7, \text{ because } x^6 \bmod 7 = 1 \text{ by FLT} \\ &= 2 \end{aligned}$$

$$\begin{aligned} b &= 30^7 \bmod 11 \\ &= (30 \bmod 11)^7 \bmod 11 \\ &= 8^7 \bmod 11 \\ &= 2 \times 2^{10} \times 2^{10} \bmod 11 \\ &= 2, \text{ because } x^{10} \bmod 11 = 1 \text{ by FLT} \end{aligned}$$

   Now that we have $y \bmod 7$ and $y \bmod 11$, we can write a system of equations and solve algebraically for y. Because $y \equiv 2 \bmod 7$, we can express y as $7s + 2,\ s \in \mathbb{Z}$. Using the fact that $y \equiv 2 \bmod 11$, we have

$$7s + 2 \equiv 2 \bmod 11 \implies s \equiv 0 \bmod 11$$

   From this we know that $s = 11t,\ t \in \mathbb{Z}$. Substituting into the original equation, we have that

$$y = 7(11t) + 2 = 77t + 2,\ t \in \mathbb{Z}$$

   meaning $30^7 \bmod 77 = 2$, so the message Alice sends is $\hat{x} = 2$.

   (g) Bob receives the encrypted message, and applies his decryption function D to it.

   $D(x) =$

   Recall that $D(x) \equiv x^d \mod N$.

   Bob applies his private key $d = 43$ to decode Alice's message. He has to compute

$$2^{43} \bmod 77$$

   From the previous part, we know that $2 = 30^7 \bmod 77$, giving

$$(30^7)^{43} \bmod 77 = 30^{1 \bmod 60} \bmod 77 = 30$$

   Here we applied Fermat's Little Theorem and the fact that $ed \equiv 1 \bmod (p-1)(q-1)$ to verify the answer.

2. Decide whether each of the following statements are true or false.

   (a) Bob has to publish his key (N, e) to receive encrypted messages from Alice.

   - True
   - False

   This is the unique feature of asymmetric or public key cryptography: the key (N, e) is open information to everyone.

   (b) Eve needs to know Bob's key d in order to send him encrypted messages.

   - True
   - False

   No, she only needs to know (N, e) to encode the message.

   (c) The security of RSA relies on the computational intractability of determining x from $y = x^e \mod N$, even when y, e, and N are all known.

   - True
   - False

   True, the most efficient algorithms we know of to solve this problem are far too slow to crack RSA for extremely large primes.

   (d) $E(x) = x^e \mod N$ is a bijection on numbers $\mod N$.

   - True
   - False

   We say a function M is a bijection from set A to set B iff every element of A maps to a unique element of B.

   This is true. If $0 \le x \le N-1$, then each value of x will map to a unique value x^e in that same set.

Polynomial Interpolation.

3. Three points uniquely determine a degree 2 polynomial. Given the three points $\{(x_1, y_1) = (-1, 2), (x_2, y_2) = (1, -2), (x_3, y_3) = (2, 5)\}$ we wish to find the unique polynomial $p(x) = a_2x^2 + a_1x + a_0$ such that $p(x_i) = y_i$. In this question we will find $p(x)$ by solving a system of linear equations:

   (a) Compute a, b, c, d such that: $p(-1) = a_2 \cdot a + a_1 \cdot b + a_0 \cdot c = d$

   $a =$

   $a = 1$. See solution to d for explanation.

   $b =$

   $b = -1$. See solution to d for explanation.

   $c =$

   $c = 1$. See solution to d for explanation.

   $d =$

   From the point $(-1, 2)$, we know that

$$p(-1) = a_2 \times (-1)^2 + a_1 \times (-1) + a_0 = 2$$

   giving us $a = 1,\ b = -1,\ c = 1,\ d = 2$

   (b) Compute a, b, c, d such that: $p(1) = a \cdot a_2 + b \cdot a_1 + c \cdot a_0 = d$

   $a =$

   $a = 1$. See solution to d for explanation.

   $b =$

   $b = 1$. See solution to d for explanation.

   $c =$

   $c = 1$. See solution to d for explanation.

   $d =$

   From the point $(1, -2)$, we know that

$$a_2 \times 1^2 + a_1 \times 1 + a_0 = -2$$

   giving us $a = 1,\ b = 1,\ c = 1,\ d = -2$

   (c) Compute a, b, c, d such that: $p(2) = a \cdot a_2 + b \cdot a_1 + c \cdot a_0 = d$

   $a =$

   $a = 4$. See solution to d for explanation.

   $b =$

   $b = 2$. See solution to d for explanation.

   $c =$

   $c = 1$. See solution to d for explanation.

   $d =$

   From the point $(2, 5)$, we know that

$$a_2 \times 2^2 + a_1 \times 2 + a_0 = 5$$

   giving us $a = 4,\ b = 2,\ c = 1,\ d = 5$

   (d) Subtract polynomials $p(x_1)$ and $p(x_2)$ to determine the value for a_1:

   $a_1 =$

   We first compute $p(-1) - p(1)$:

$$\begin{aligned} a_2 - a_1 + a_0 &= 2 \\ -(a_2 + a_1 + a_0 &= -2) \end{aligned}$$

   Giving us $-2a_1 = 4 \implies a_1 = -2$

   (e) Solve the remaining system of two equations and two variables to determine a_2 and a_0:

   $a_2 =$

   $a_2 = 3$. See solution to a_0 for explanation.

   $a_0 =$

   We first substitute $a_1 = -2$ into two of the equations in the original system, giving

$$\begin{aligned} a_2 + (-2) \times 1 + a_0 &= -2 \implies a_2 + a_0 = 0 \\ 4a_2 + (-2) \times 2 + a_0 &= 5 \implies 4a_2 + a_0 = 9 \end{aligned}$$

   We can substitute $a_0 = -a_2$ into the second equation to get

$$4a_2 + a_0 = 4a_2 - a_2 = 9 \implies a_2 = 3$$

   Because $a_0 = -a_2$,

$$a_0 = -3$$

4. In this question we will find $p(x)$ using the Lagrange interpolation method. Recall from question 3 that we are given the three points $\{(x_1, y_1) = (-1, 2), (x_2, y_2) = (1, -2), (x_3, y_3) = (2, 5)\}$ we wish to find the unique polynomial $p(x) = a_2x^2 + a_1x + a_0$ such that $p(x_i) = y_i$.

   (a) Compute a, b, c such that $\Delta_1(x) = a(x-b)(x-c)$. Note b, c are integers such that $b < c$:

   $a =$

   Recall that $\Delta_j(x)$ is 1 for $x = x_j$ and 0 for $x = x_i,\ i \neq j$

   $a = \frac{1}{6}$. See solution to c for explanation.

   $b =$

   $b = 1$. See solution to c for explanation.

   $c =$

   We know that $\Delta_1(x)$ should be 1 for $x = x_1 = -1$ and 0 for $x = x_2 = 1$ and $x = x_3 = 2$. Let's take care of the second condition first.

   One polynomial that is 0 for $x = 1$ and $x = 2$ is

$$(x-1)(x-2)$$

   This gives us

$$\begin{aligned} b &= 1 \\ c &= 2 \end{aligned}$$

   Now we simply need to find the right scaling factor a to make sure that $a(x-1)(x-2) = 1$ when $x = -1$. Plugging in -1, we see we need to satisfy

$$a \times (-2) \times (-3) = 1 \implies a = \frac{1}{6}$$

   (b) Compute a, b, c such that $\Delta_2(x) = ax^2 + bx + c$:

   $a =$

   Recall that $\Delta_j(x)$ is 1 for $x = x_j$ and 0 for $x = x_i,\ i \neq j$

   $a = -\frac{1}{2}$. See solution to c for explanation.

   $b =$

   $b = \frac{1}{2}$. See solution to c for explanation.

   $c =$

   Following the same procedure as above, let us first find a polynomial that is 0 when $x = x_1 = -1$ and $x = x_3 = 2$. This gives us

$$(x+1)(x-2)$$

   To ensure that it will be 1 when $x = x_2 = 1$, we scale by $\frac{1}{(1+1)(1-2)} = -\frac{1}{2}$, giving

$$-\frac{1}{2}(x+1)(x-2)$$

   Expanding, we get

$$-\frac{1}{2}x^2 + \frac{1}{2}x + 1$$

   meaning $a = -\frac{1}{2}$, $b = \frac{1}{2}$, and $c = 1$

   (c) Compute a, b, c such that $\Delta_3(x) = a(x-b)(x-c)$. Note b, c are integers such that $b < c$.

   $a =$

   Recall that $\Delta_j(x)$ is 1 for $x = x_j$ and 0 for $x = x_i,\ i \neq j$. This should be a fraction.

   $a = \frac{1}{3}$. See solution to c for explanation.

   $b =$

   $b = -1$. See solution to c for explanation.

   $c =$

   Following the same procedure as above, let us first find a polynomial that is 0 when $x = x_1 = -1$ and $x = x_2 = 1$. This gives us

$$(x+1)(x-1)$$

   To ensure that it will be 1 when $x = x_2 = 2$, we scale by $\frac{1}{(2+1)(2-1)} = \frac{1}{3}$, giving

$$\frac{1}{3}(x+1)(x-1)$$

   meaning $a = \frac{1}{3}$, $b = -1$, and $c = 1$

   (d) Compute a, b, c such that $y_1\Delta_1(x) + y_3\Delta_3(x) = ax^2 + bx + c$.

   $a =$

   $a = 2$. See solution to c for explanation.

   $b =$

   $b = -1$. See solution to c for explanation.

   $c =$

   Recall $y_1 = 2$ and $y_3 = 5$. Plugging those into the equation given, we have

$$y_1\Delta_1(x) + y_3\Delta_3(x) = 2\left(\frac{1}{6}(x-1)(x-2)\right) + 5\left(\frac{1}{3}(x+1)(x-1)\right)$$

   Simplifying, we get

$$\frac{1}{3}x^2 - x + \frac{2}{3} + \frac{5}{3}x^2 - \frac{5}{3} = 2x^2 - x - 1$$

   Meaning $a = 2$, $b = -1$, and $c = -1$

   (e) Compute a, b, c such that $y_2\Delta_2(x) = ax^2 + bx + c$.

   $a =$

   $a = 1$. See solution to c for explanation.

   $b =$

   $b = -1$. See solution to c for explanation.

   $c =$

   Recall $y_2 = -2$. Plugging this into the expression given,

$$y_2\Delta_2(x) = -2\left(-\frac{1}{2}x^2 - \frac{1}{2}x - 1\right) = x^2 - x - 2$$

   meaning $a = 1$, $b = -1$, and $c = -2$

   (f) Finally, compute a_2, a_1, a_0 such that $p(x) = a_2x^2 + a_1x + a_0 = \sum_{i=1}^{3} y_i\Delta_i(x)$.

   $a_2 =$

   $a_2 = 3$. See solution to a_0 for explanation.

   $a_1 =$

   $a_1 = -2$. See solution to a_0 for explanation.

   $a_0 =$

   We simply have to combine the two expressions we found for $y_1\Delta_1(x) + y_3\Delta_3(x)$ and $y_2\Delta_2(x)$:

$$\sum_{i=1}^{3} y_i\Delta_i(x) = 2x^2 - x - 1 + x^2 - x - 2 = 3x^2 - 2x - 3$$

   This gives us $a_3 = 3$, $a_2 = -2$, and $a_1 = -3$

Secret Sharing.

5. Suppose you are in charge of setting up a secret sharing scheme where you want to distribute $n = 5$ shares to 5 people such that any $k = 3$ or more people can figure out the secret, but two or fewer cannot. Suppose we are working over $GF(7)$.

   (a) What is the degree of the polynomial you will use to distribute the shares?

   How many points uniquely determine a degree n polynomial?

   We want 3 points to uniquely determine this polynomial, so it should be of degree 2.

   (b) You randomly choose the polynomial: $P(x) = 5x^2 + 3x + 3$. What is the secret?

   $P(0) =$

   Remember we're working in $GF(7)$.

   The y-intercept, 3, is our secret.

   (c) What is the share given to the first official?

   $P(1) =$

$$P(1) = (5 + 3 + 3) \bmod 7 = 11 \bmod 7 = 4$$

   (d) What is the share given to the second official?

   $P(2) =$

$$P(2) = (20 + 6 + 3) \bmod 7 = (6 + 6 + 3) \bmod 7 = 15 \bmod 7 = 1$$

   (e) What is the share given to the third official?

   $P(3) =$

$$P(3) = (45 + 9 + 3) \bmod 7 = (3 + 2 + 3) \bmod 7 = 8 \bmod 7 = 1$$

   (f) What is the share given to the fourth official?

   $P(4) =$

$$P(4) = (5 \times 16 + 12 + 3) \bmod 7 = (3 + 5 + 3) \bmod 7 = 11 \bmod 7 = 4$$

   (g) What is the share given to the fifth official?

   $P(5) =$

$$P(5) = (5 \times 25 + 15 + 3) \bmod 7 = (6 + 1 + 3) \bmod 7 = 10 \bmod 7 = 3$$

   (h) Suppose officials 1, 2, and 5 get together, and try to recover the secret. Using Lagrange interpolation, they compute their delta functions $\Delta_1(x), \Delta_2(x), \Delta_5(x)$. What are a, b, c when $\Delta_1(x) = a(x-b)(x-c)$? Again note that $b < c$ and b, c are integers.

   $a =$

   This should not be a fraction. Recall that we are in GF(7).

   $a = 2$. See solution to c for explanation.

   $b =$

   $b = 2$. See solution to c for explanation.

   $c =$

   First, we know we want $\Delta_1(x)$ to be 0 when $x = 2$ and $x = 5$. This gives us

$$\Delta_1(x) = a(x-2)(x-5) \mod 7$$

   Second, we want $\Delta_1(x)$ to be 1 when $x = 1$. This will determine the value of a.

$$\Delta_1(1) = a(1-2)(1-5) \mod 7 = 4a \bmod 7 = 1$$

   Now we know $a = 4^{-1} \bmod 7 = 2$. This gives us $a = 2$, $b = 2$, $c = 5$

   (i) What are a, b, c when $\Delta_2(x) = a(x-b)(x-c)$? Again note that $b < c$ and b, c are integers.

   $a =$

   This should not be a fraction. Recall that we are in GF(7).

   $a = 2$. See solution to c for explanation.

   $b =$

   $b = 1$. See solution to c for explanation.

   $c =$

   First, we know we want $\Delta_2(x)$ to be 0 when $x = 1$ and $x = 5$. This gives us

$$\Delta_2(x) = a(x-1)(x-5) \mod 7$$

   Second, we want $\Delta_2(x)$ to be 1 when $x = 2$:

$$\Delta_2(2) = a(2-1)(2-5) \mod 7 = 4a \bmod 7 = 1$$

   Now we know $a = 4^{-1} \bmod 7 = 2$. This gives $a = 2$, $b = 1$, $c = 5$

   (j) What are a, b, c when $\Delta_5(x) = a(x-b)(x-c)$? Again note that $b < c$ and b, c are integers.

   $a =$

   This should not be a fraction. Recall that we are in GF(7).

   $a = 3$. See solution to c for explanation.

   $b =$

   $b = 1$. See solution to c for explanation.

   $c =$

   First, we know we want $\Delta_5(x)$ to be 0 when $x = 1$ and $x = 2$. This gives us

$$\Delta_5(x) = a(x-1)(x-2) \mod 7$$

   Second, we want $\Delta_5(x)$ to be 1 when $x = 5$:

$$\Delta_5(5) = a(5-1)(5-2) \mod 7 = 5a \bmod 7 = 1$$

   Now we know $a = 5^{-1} \bmod 7 = 3$. This gives us $a = 3$, $b = 1$, $c = 2$

   (k) Their final polynomial $p(x) = a_2x^2 + a_1x + a_0 = P(1) \cdot \Delta_1(x) + P(2) \cdot \Delta_2(x) + P(5) \cdot \Delta_5(x)$ has coefficients:

   $a_2 =$

   Recall that we are in GF(7). This should be between 0 and 6.

   $a_2 = 5$. See solution to a_0 for explanation.

   $a_1 =$

   $a_1 = 3$. See solution to a_0 for explanation.

   $a_0 =$

   Let's write out the expression for $P(1)\Delta_1(x) + P(2)\Delta_2(x) + P(5)\Delta_5(x)$:

$$4 \times 2(x-2)(x-5) + 1 \times 2(x-1)(x-5) + 3 \times 3(x-1)(x-2) \mod 7$$

   Simplifying, we have

$$\begin{aligned} P(x) &= (x-2)(x-5) + 2(x-1)(x-5) + 2(x-1)(x-2) && \bmod 7 \\ &= x^2 - 7x + 10 + 2x^2 - 12x + 10 + 2x^2 - 6x + 4 && \bmod 7 \\ &= 5x^2 - 11x + 10 && \bmod 7 \\ &= 5x^2 + 3x + 3 && \bmod 7 \end{aligned}$$

   This gives $a = 5$, $b = 3$, and $c = 3$. We have successfully recovered the original polynomial $P(x)$.

   (l) Could officials 1 and 2 recover the secret with official 4 instead of collaborating with official 5?

   - Yes
   - No

   Yes, any three points is enough to recover the polynomial.

   (m) Could officials 1 and 2 recover the secret by only collaborating with each other?

   - Yes
   - No

   No, there are 7 possible polynomials of degree 2 with $P(1)$ and $P(2)$ fixed. Note that there were only seven possibilities for the original secret in the first place, so the last point contains just as much information as the secret itself.