Discussion 3C

CS 70, Summer 2024

1 RSA Warm-Up

(a) We must have that $\gcd(e,(p-1)(q-1)) = 1$ for there to exist a private key. Since p and q are both prime numbers greater than 3, they must be odd. Then $p-1$ and $q-1$ are both even, so $(p-1)(q-1)$ is also even. Thus, $gcd(2,(p-1)(q-1)) = 2 \neq 1$, which violates the gcd constraint for e.

(b) We must have that $\gcd(3,(p-1)(q-1)) = 1$. So $(p-1)$ and $(q-1)$ cannot be multiples of 3, that is, $(p-1) \neq 3k$ and $(q-1) \neq 3j$ for any integers $k, j \in \mathbb{Z}$.

This means that $p \neq 3k+1$ and $q \neq 3j+1$, so p and q can only be of the form of $3k$ or $3k+2$. However, p and q cannot be of the form of $3k$ because they must be prime.

Our condition is that p and q are prime numbers of the form $3k+2$.

(c) The public key is defined to be (N,e), where $N = pq$. Plugging in our values, $N = 5 \cdot 17$ and $e = 3$, so our public key will be $(85,3)$.

(d) For the RSA scheme, we must have $ed \equiv 1 \pmod{(p-1)(q-1)}$. Plugging in our values, we want to find a d such that $3d \equiv 1 \pmod{64}$. That is, $d \equiv 3^{-1} \pmod{64}$.

We can find the inverse using the extended Euclidean algorithm.

$$\begin{aligned} \mathbf{64} &= 1 \times \mathbf{64} + 0 \times \mathbf{3} && (E_1) \\ \mathbf{3} &= 0 \times \mathbf{64} + 1 \times \mathbf{3} && (E_2) \\ \mathbf{1} &= 1 \times \mathbf{64} + (-21) \times \mathbf{3} && (E_3 = E_1 - 21E_2). \end{aligned}$$

Therefore $3^{-1} \equiv -21 \pmod{64}$. We will use $d = 3^{-1} \bmod 64 = 43$ (since $-21 \equiv 43 \pmod{64}$).

(e) To encrypt a message, we use $E(x) = x^e \bmod N$. Plugging in our values, $E(10) = 10^3 \bmod 85 = 65 \bmod 85 = 65$. Our encrypted message is 65.

(f) To decrypt a message, we use $D(y) = y^d \bmod N$. Plugging in our values, we want to find $D(19) = 19^{43} \bmod 85$.

Since these numbers are quite large, repeat squaring is difficult. We will use the Chinese remainder theorem. From the Chinese remainder theorem, we know that we know that for coprime values p and q, all solutions to the system

$$\begin{aligned} x &= a \pmod{p} \\ x &= b \pmod{q} \end{aligned}$$

are unique modulo pq. In our case, $p = 5$ and $q = 17$ so let's start by finding $19^{43} \bmod 5$ and $19^{43} \bmod 17$.

$$\begin{aligned} 19^{43} &\equiv (-1)^{43} && \pmod{5} \\ &\equiv -1 && \pmod{5} \\ &\equiv 4 && \pmod{5} \\ 19^{43} &\equiv 2^{43} && \pmod{17} \\ &\equiv (2^4)^{10} \cdot 2^3 && \pmod{17} \\ &\equiv 16^{10} \cdot 8 && \pmod{17} \\ &\equiv (-1)^{10} \cdot 8 && \pmod{17} \\ &\equiv 8 \pmod{17}. \end{aligned}$$

Therefore we consider the following system of linear congruences.

$$\begin{aligned} x &\equiv 4 \pmod{5} \\ x &\equiv 8 \pmod{17}, \end{aligned}$$

created specifically because 19^{43} satisfies them. Then any other solution we find is equivalent to 19^{43} modulo 85.

The standard Chinese remainder theorem solution is

$$\begin{aligned} x &= 4 \cdot (17 \cdot (17^{-1} \bmod 5)) + 8 \cdot (5 \cdot 5^{-1} \bmod 17) \\ &= 4 \cdot (17 \cdot 3) + 8 \cdot (5 \cdot 7) \\ &= 484. \end{aligned}$$

We know that all solutions are congruent modulo 85, so we have that $19^{43} \equiv 484 \equiv 59 \pmod{85}$.

That is, $D(19) = 19^{43} \bmod 85 = 59$.

2 RSA with Multiple Keys

(a) Because all public keys are generated from the same prime, they share a common factor. In particular, since $p \mid N_1$ and $p \mid N_2$ is the only common divisor of N_1 and N_2,

$$\gcd(N_1, N_2) = \gcd(pq_1, pq_2) = p.$$

Therefore Ewen can quickly compute p using the Euclidean algorithm. Then Ewen can find $q_1 = N_1/p$ and $q_2 = N_2/p$.

Then, using the extended Euclidean algorithm, Ewen can compute $d_1 = e^{-1} \bmod N_1$ and $d_2 = e^{-1} \bmod N_2$. Finally, she can recover

$$x_1 = y_1^{d_1} \bmod N_1 \qquad x_2 = y_2^{d_2} \bmod N_2.$$

(b) Ewen can no longer use idea from part **(a)** since the moduli are now all pairwise coprime. However, in this scheme, the value e is the same for all public keys. Ewen sees

$$\begin{aligned} y_1 &\equiv x^3 \pmod{N_1} \\ y_2 &\equiv x^3 \pmod{N_2} \\ y_3 &\equiv x^3 \pmod{N_3}. \end{aligned}$$

Using the Chinese Remainder Theorem, Ewen can find a solution y to these equations. By the uniqueness of the Chinese remainder theorem, $y \equiv x^3 \pmod{N_1 N_2 N_3}$.

Moreover, since $x < N_1$, $x < N_2$, and $x < N_3$, this means that $x^3 < N_1 N_2 N_3$. In particular, $x^3 \bmod N_1 N_2 N_3 = x^3$. So $y \bmod N_1 N_2 N_3 = x^3$ and therefore Ewen can get the original message by computing

$$x = \sqrt[3]{x^3} = \sqrt[3]{y \bmod N_1 N_2 N_3}.$$

3 Concert Tickets

(a) There are only 101 possible values for Akemi's ticket number. For each $v \in \{0, \ldots, 100\}$, Eileen can compute $E(v) = v^e \bmod N$ and see which matches with the encrypted message y.

To confirm that this works, we must show that if $E(v) = y$, then $v = x$. Suppose that $E(v) = y$. Then, by the definition of the decryption function, $x = D(y) = D(E(v))$. But we proved that for the RSA scheme, $D(E(v)) = v$. So $x = v$, as desired.

(b) Eileen sees $y_1 \equiv r^e \bmod N$ and $y_2 \equiv (rx)^e \bmod N$. If Eileen can find $x^e \bmod N$, she can apply her method from **(a)**.

Note that the second message is

$$y_2 = (rx)^e \bmod N = (r^e \cdot x^e) \bmod N.$$

If Eileen can find $(r^e)^{-1} \bmod N$, then Eileen can find $x^e \bmod N$ as $(r^e)^{-1} y_2 \bmod N$. Eileen sees $y_1 = r^e \pmod{N}$. She can use the extended Euclidean algorithm to find $y_1^{-1} \bmod N = (r^e)^{-1} \bmod N$.

We must prove that this inverse exists. Since r is coprime to N, we know that r^{-1} exists modulo N. Then, by Discussion 2B Question 2**(a)**,

$$(r^e)^{-1} \equiv (r^{-1})^e \pmod{N},$$

so if r^{-1} exists modulo N, then so does $(r^e)^{-1}$ modulo N.

Once Eileen has found $(r^e)^{-1}$, she can find x^e:

$$\begin{aligned} y_2 &\equiv r^e \cdot x^e && \pmod{N} \\ (r^e)^{-1} \cdot y_2 &\equiv (r^e)^{-1} \cdot r^e \cdot x^e && \pmod{N} \\ (r^e)^{-1} \cdot y_2 &\equiv x^e && \pmod{N} \end{aligned}$$

Finally, Eileen can use her approach from **(a)** to find x.