0: Message Size

(a) Code submission in separate file. The message is "b'hello'".

(b) The encrypted message is m^e, and since m is small, we can say that $m^e < N$ which means that $m^e \mod N = m^e$. Since m^e is not affected by the $\mod N$ operation, the encryption step of the RSA just returns m^e. We can just take the e-th root of this to get m back. If m were large, then $m^e \mod N$ (the encryption step of RSA) would return something not equal to m^e, so this attack wouldn't work if m is large.

1: Wiener's Attack

(a) To prove that our definition of a and b satisifies the pre-conditions of Legendre's Theorem, we will prove several separate results and put them together at the end.

We first prove that $gcd(k, d) = 1$. To prove this, we note that $gcd(k, d)|k$ and $gcd(k, d)|d$, so $gcd(k, d)$ divides any linear combination of k and d i.e. for any $m, n \in \mathbb{N}$, $gcd(k, d)|mk + nd$. By the definition of RSA, $ed \equiv_{\phi(N)} 1$. So, there is a $k \in \mathbb{Z}$ such that $ed - k\phi(N) = 1$. By letting $m = e$ and $n = -\phi(N)$, we see that $mk + nd = 1$ for any choice of m, n since the choice of e, p, and q is arbitrary during RSA. As such, we can now say that $gcd(k, d)|mk + nd = gcd(k, d)|1$, and the only number that divides 1 is 1, $gcd(k, d) = 1$.

We next show the following two inequalities separately after making a few statements about d:

- $d \neq 0$: This is true because of the RSA condition that $ed \equiv_{\phi(N)} 1$
- $d > 0$: Due to the RSA condition that $ed \equiv_{\phi(N)} 1$, d is the multplicative inverse of e and therefore must be non-negative.

$$
\begin{aligned}
(p-2)(q-2) &> 2 && \text{[trivial based off given assumption that } p, q > 11\text{]} \\
pq - 2q - 2p + 4 &> 2 \\
2pq - 2q - 2p + 2 &> pq \\
2(p-1)(q-1) &> pq \\
2\phi(N) &> N && \text{[by definition of } N \text{ and } \phi(N)\text{]} \\
\frac{2}{dN} &> \frac{1}{d\phi(N)} && [d \neq 0] \\
\frac{N^{\frac{1}{4}}}{3} &> d && \text{[given]} \\
N^{\frac{1}{4}} &> 3d \\
N &> 81d^4 > 4d \\
N &> 4d && \text{[transititivity of inequality for real numbers]} \\
N &> \frac{2 * 2d^2}{d} && [d > 0] \\
\frac{1}{2d^2} &> \frac{2}{dN}
\end{aligned}
$$

We now know that $\frac{1}{d\phi(N)} < \frac{2}{dN}$ and $\frac{2}{dN} < \frac{1}{2d^2}$. By the transititivity of inequality for real numbers, we can say that

$$\frac{1}{d\phi(N)} < \frac{2}{dN} < \frac{1}{2d^2}$$

,

We have proven that our definition of a and b satisfies the pre-conditions of Legendre's theorem.

(b) Lemma 1: $|N - \phi(N)| < 3\sqrt{N}$

Proof. Lemma 1a: $N - \phi(N) > 0$

Because $p, q > 11$, we can say the following:

$$\begin{aligned}
p + q - 1 > 11 + 11 - 1 &> 0 && \text{[given that } p, q > 11\text{]} \\
pq - pq + p + q - 1 &> 0 \\
pq - (p-1)(q-1) &> 0 \\
N - \phi(N) &> 0 && \text{[definition of } N \text{ and } \phi(N)\text{]}
\end{aligned}$$

Thus Lemma 1a is true. □

We break up our given of $q < p < 2q$ into $q < p$ and $p < 2q$ to prove the lemma.

$$\begin{aligned}
q &< p && \text{[given]} \\
\sqrt{q} &< \sqrt{p} \\
q &< \sqrt{pq} \\
q &< \sqrt{N} && \text{[definition of N]} \\
3q &< 3\sqrt{N} \\
q + p < q + 2q &< 3\sqrt{N} && \text{[given that } p < 2q\text{]} \\
q + p - 1 < q + p &< 3\sqrt{N} && \text{[transititivity of inequality for real numbers]} \\
q + p - 1 &< 3\sqrt{N} && \text{[transititivity of inequality for real numbers]} \\
pq - (pq - q - p + 1) &< 3\sqrt{N} \\
N - \phi(N) &< 3\sqrt{N} \\
|N - \phi(N)| &< 3\sqrt{N} && [N - \phi(N) > 0 \text{ by Lemma 1a, so definition of absolute value applies}]
\end{aligned}$$

Therefore we have proven **Lemma 1**.

(c) Lemma 2: To prove this lemma, we will employ **Lemma 1**.

$$\begin{aligned}
\left|\frac{e}{N}-\frac{k}{d}\right| &= \left|\frac{ed-kN}{Nd}\right| \\
&= \left|\frac{ed-k\phi(N)-kN+k\phi(N)}{Nd}\right| \\
&= \left|\frac{1-k(N-\phi(N))}{Nd}\right| && \text{[by RSA condition that } ed \equiv_{\phi(N)} 1\text{]} \\
&< \left|\frac{-k(N-\phi(N))}{Nd}\right| && [N-\phi(N)>0 \text{ from part b}] \\
&< \left|\frac{-3k\sqrt{N}}{Nd}\right| && \text{[by } \textbf{Lemma 1}\text{]} \\
&< \left|\frac{3k\sqrt{N}}{Nd}\right| && \text{[by definition of absolute value]} \\
&\leq \frac{3k}{d\sqrt{N}}
\end{aligned}$$

The last statement of the simplification can be made because $d > 0$ from previous part, $k > 0$ by RSA property $ed \equiv_{\phi(N)} 1$, and $N > 0$ because $p, q > 0$. Thus we have proven **Lemma 2**.

(d) Lemma 3: $k < d$

We prove this lemma by simplifying the RSA condition that $ed \equiv_{\phi(N)} 1$

$$
\begin{aligned}
ed &\equiv_{\phi(N)} 1 && \text{[condition of RSA]} \\
ed - k\phi(N) &= 1 && \text{[true for some } k \in \mathbb{Z} \text{ by definition } \equiv_n] \\
1 + k\phi(N) &= ed \\
k\phi(N) &< ed \\
k &< \frac{ed}{\phi(N)} < \frac{\phi(N)d}{\phi(N)} && \text{[by definition of RSA]} \\
k &< d
\end{aligned}
$$

Thus we have proven **Lemma 3**.

(e) Prove that $\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$

Proof. Lemma 1b: $\frac{3}{\sqrt{N}} < \frac{1}{2d^2}$

$$\begin{aligned} d &< \frac{N^{\frac{1}{4}}}{3} && \text{[given]} \\ 36d^4 < 81d^4 &< N \\ 36d^4 &< N && \text{[transitivity of inequality for real numbers]} \\ 6d^2 &< \sqrt{N} \\ 3 * 2d^2 &< \sqrt{N} \\ \frac{3}{\sqrt{N}} &< \frac{1}{2d^2} \end{aligned}$$

Thus we have proven Lemma 1b. □

We prove the original statement by employing **Lemma 2** and **Lemma 3**

$$\begin{aligned} \left|\frac{e}{N} - \frac{k}{d}\right| &< \frac{3k}{d\sqrt{N}} && \text{[by \textbf{Lemma 2}]} \\ &< \frac{3d}{d\sqrt{N}} && \text{[by \textbf{Lemma 3}]} \\ &= \frac{3}{\sqrt{N}} \\ &< \frac{1}{2d^2} && \text{[by Lemma 1b]} \\ \left|\frac{e}{N} - \frac{k}{d}\right| &< \frac{1}{2d^2} \end{aligned}$$

Thus we have proven the original statement.

(f) Code submission in separate file on gradescope.

- K1:

  p = 379
  q = 239

- K2:

  p = 12539632253212038182708715136208112909218665186857529270323913
  088513184321026862369475927295147730917565158010747988824664394379
  978058105305597625967410787791833343134652857846415473379462098625
  607282443627270451810395851889315754218497337824973147392684628707
  5853455404337166913999471528088686741224927681479

  q = 10587227430092432880125156352261513126400243087944617662585663
  424891839528786738244810280030700986980497528913151784044482659300
  631076999793841968447713923394022439331363453795770533810149066452
  483629748724308847150705362397635237900434592520917498639864991794
  0373025573924513596301382883113062330937472494359

- K3:

  p = 10918952865582252098239079408125578647426266894934560842726219
  321572189303435138882708623974202002066512594943477860617098674539
  922342187561553047536730442226147711610748684672421097690778657965
  915142725249457595134788101121498884165931345086318046756669290432
  8406206973866541393288421998658788581626435823973

  q = 80704108225986846689088894623631942822394012965679790134822960
  353763696287745286610889769161432843183717207275489607631907676707
  871854593075515955028452067841551869699075640269983212231116408775
  149090038537951432904031727827115531279717750167834084430363357711
  827940641648984434771854501457989011540376590839