## 0: Message Size

**(a)** The message was 'hello'. Please see separate file for python code.

**(b)** The message ($m$) has to be short for this attack to work for the inequality $m^e < N$ to be true. When this is true, we can say that $m^e \mod N = m^e$ by the division theorem. From RSA, we are given that $m^e \mod N = c$. It follows that $m^e = c$ by transitive property. Thus, we can take the $e^{th}$ root from each side to obtain $m$.

## 1: Wiener's Attack

**(a)** We will prove this in three parts: **i.** $gcd(k,d) = 1$; **ii.** $\frac{1}{d\phi(N)} < \frac{2}{dN}$; **iii.** $\frac{2}{dN} < \frac{1}{2d^2}$.

**i.** We know that $gcd(k,d) = kx_{(k,d)} + dy_{(k,d)}$ by Bezout's Theorem. If we let $x_{(k,d)} = -\phi(N)$ and $y_{(k,d)} = e$, then the above equation becomes $gcd(k,d) = -k\phi(N) + de$. Rearranging the equation, $gcd(k,d) = ed - k\phi(N)$. Since we are given that $ed - k\phi(N) = 1$, it follows that $gcd(k,d) = 1$.

**ii.** By the definition of RSA, we know that

$$\phi(N) = (p-1)(q-1).$$

From this definition, we can multiply both sides by 2 such that

$$\begin{aligned}
2\phi(N) &= 2(p-1)(q-1) && \text{Multiplication}\\
&= 2(pq - p - q + 1) && \text{Expansion}\\
&= 2pq - 2p - 2q + 2 && \text{Simplification}
\end{aligned}$$

Since it is given that $q < p$, we know that $2q < 2p$ by Multiplication. Multiplying both sides by -1, we know that $-2q > -2p$. Thus, the above equation becomes

$$\begin{aligned}
2\phi(N) &= 2pq - 2p - 2q + 2 && \\
&> 2pq - 2p - 2p + 2 && \text{-2q > -2p}\\
&> pq + pq - 4p + 2 && \text{Simplification}\\
&> pq + p(q-4) + 2 && \text{Factor out p}
\end{aligned}$$

Since we know that $q \geq 11$ and $pq = N$, we know that $pq + p(q-4) + 2 > N$. Thus, by transitivity, $2\phi(N) > N$. Dividing both sides by 2, we have $\phi(N) > \frac{N}{2}$. It follows that $\frac{2}{N} > \frac{1}{\phi(N)}$. Dividing both sides by d, we have $\frac{2}{dN} > \frac{1}{d\phi(N)}$

**iii.**

$$\begin{aligned}
d &< \frac{N^{1/4}}{3} && \text{Given}\\
3d &< N^{1/4} && \text{Multiply both sides by 3}\\
81d^4 &< N && \text{Take both sides to } 4^{th} \text{ power}
\end{aligned}$$

From the problem, it is given that $d \geq 1$ and therefore $4d < 81d^4 < N$. By transitivity, $4d < N$. Multiplying both sides by $d/2$ and taking their reciprocals, we have $\frac{2}{dN} < \frac{1}{2d^2}$.

Thus, since $|\frac{e}{\phi(N)} = \frac{k}{d}| = \frac{1}{d\phi(N)}$, it follows that $|\frac{e}{\phi(N)} = \frac{k}{d}| = \frac{1}{d\phi(N)} < \frac{2}{dN} < \frac{1}{2d^2}$

**(b)**

$$
\begin{aligned}
|N - \phi(N)| &= |pq - (p-1)(q-1)| && \text{Definitions of N and } \phi(N) \\
&= |pq - pq + p + q - 1| && \text{Expansion} \\
&= |p + q - 1| && \text{Simplification} \\
&< p + q && \text{Algebra} \\
&< 2q + q && \text{p < 2q} \\
&= 3q && \text{Algebra} \\
&= 3\sqrt{q^2} && \text{Algebra} \\
&< 3\sqrt{pq} && \text{q < p} \\
&< 3\sqrt{N} && \text{Definition of N}
\end{aligned}
$$

Thus, by transitive property, $|N - \phi(N)| < 3\sqrt{N}$.

**(c)**

$$
\begin{aligned}
|\frac{e}{N} - \frac{k}{d}| &= |\frac{ed - kN}{dN}| && \text{Expansion} \\
&= |\frac{ed - k\phi(N) + k\phi(N) - kN}{dN}| && \text{Add and Subtract } k\phi(N) \text{ term} \\
&= |\frac{1 + k\phi(N) - kN}{dN}| && ed - k\phi(N) = 1 \\
&= |\frac{1 - k(N - \phi(N)}{dN}| && \text{Factor out k} \\
&< |\frac{-k(N - \phi(N)}{dN}| && |\frac{1}{dN}| > 0 \\
&< |\frac{-k(3\sqrt{N})}{dN}| && \text{Lemma 1} \\
&= 3\sqrt{N}|\frac{-k}{dN}| && \text{Expansion} \\
&= \frac{3k\sqrt{N}}{dN} && \text{Absolute Value} \\
&= \frac{3k}{d\sqrt{N}} && \text{Simplification}
\end{aligned}
$$

Thus, by transitive property, $|\frac{e}{N} - \frac{k}{d}| < \frac{3k}{d\sqrt{N}}$.

**(d)** From the RSA definition, we know that $ed - k\phi(N) = 1$ and that $e < \phi(N)$. Rearranging, we get

$$
\begin{aligned}
k\phi(N) &= ed - 1 && \text{Definition of RSA} \\
&< d\phi(N) - 1 && \text{Definition of RSA} \\
&< d\phi(N) && \text{Algebra (1 > 0)}
\end{aligned}
$$

Therfore, after dividing both sides by $\phi(N)$, we have $k < d$.

**(e)**

$$
\begin{aligned}
\left|\frac{e}{N} - \frac{k}{d}\right| &< \frac{3k}{d\sqrt{N}} && \text{Lemma 2} \\
&< \frac{3d}{d\sqrt{N}} && \text{Lemma 3} \\
&= \frac{3}{\sqrt{N}} && \text{Algebra}
\end{aligned}
$$

Recall from the proof in part (a) that from the given equation, $d < \frac{N^{1/4}}{3}$, it follows that $81d^4 < N$. Taking the square root of both sides, we have $9d^2 < \sqrt{N}$. Plugging this back into the previous equation, we have

$$
\begin{aligned}
\left|\frac{e}{N} - \frac{k}{d}\right| &= \frac{3}{\sqrt{N}} \\
&< \frac{3}{9d^2} && 9d^2 < \sqrt{N} \\
&= \frac{1}{3d^2} && \text{Algebra} \\
&< \frac{1}{2d^2} && \text{Algebra } (3 > 2)
\end{aligned}
$$

Thus, by transitive property, $|\frac{e}{N} - \frac{k}{d}| < \frac{1}{2d^2}$.

**(f)** Please see separate file for python code.

**K1:**
p: 379
q: 239

**K2:**
p: 12539632253212038182708715136208112909218665186857529270323913088513184321026 8
623694759272951477309175651580107479888246643943799780581053055976259674107877 9183
334313465285784641547337946209862560728244362727045181039585188931575421849733 7824
97314739268462870758534554043371669139994715280886867412249276814 79

q: 10587227430092432880125156352261513126400243087944617662585663424891839528786738244
81028003070098698049752891315178404448265930063107699979384196844771392339402243933 1363
45379577053381014906645248362974872430884715070536239763523790043459252091749863986 4991
794037302557392451359630138288311306233093747249 4359

**K3:**
p: 10918952865582252098239079408125557864742626689493456084272621932157218930343513888
27086239742020020665125949434778606170986745399223421875615530475367304422261477116 10
748684672421097690778657965915142725249457595134788101121498884165931345086318046756 6
6929043284062069738665413932884219986587885816264358239 73
q: 807041082259868466890888946236319428223940129656797901348229603537636962877452866108 8

976916143284318371720727548960763190767670787185459307551595502845206784155186969907564026998321223111640877514909003853795143290403172782711553127971775016783408443036335771182794064164898443477185450145798901154037659083 9