1. Let’s first prove the statement by induction. Clearly $1^2 \equiv 1 \mod 4$. Suppose now that for an odd positive integer $m$ we have that $m^2 \equiv 1 \mod 4$. We want to show that $(m+2)^2 \equiv 1 \mod 4$. Indeed,

$$(m+2)^2 \equiv m^2 + 4m + 4 \equiv m^2 \equiv 1 \mod 4$$

which verifies the induction step.

Let’s now prove the statement by contradiction. Clearly $1^2 \equiv 1 \mod 4$. Suppose there exists $m$ an odd positive integer such that $m^2 \neq 1 \mod 4$. We can choose $m$ to be the smallest integer with this property. Then clearly $m \geq 3$, and $m - 2 \geq 1$ would need to satisfy

$$(m-2)^2 \equiv 1 \mod 4.$$ 

But that would imply that $(m-2)^2 = m^2 - 4m + 4 \equiv m^2 \mod 4 \neq 1 \mod 4$, which gives a contradiction.

2. (a) We want to compute $\varphi(p^s)$. We have that $\{1, 2, \ldots, p^s\}$ has $p^s$ elements, and among them $\{p \cdot 1, p \cdot 2, \ldots, p \cdot p^{s-1}\}$ have gcd greater than 1. Thus, we get that $\varphi(p^s) = p^s - p^{s-1}$.

(b) Suppose $m$ is an even number. Let $\{d_1 = 2, d_2, \ldots, d_{m-\varphi(m)}\} \subset \{1, \ldots, m\}$ be the integers with $\gcd(\cdot, m) > 1$ and $\{e_1 = 1, \ldots, e_{\varphi(m)}\}$ be the integers with $\gcd(\cdot, m) = 1$ (all of them are odd). Since $m$ is even, we have $\gcd(d_i, 2m) > 1$ and $\gcd(e_j, 2m) = 1$.

Clearly $\{d_1 + m, d_2 + m, \ldots, d_{m-\varphi(m)} + m\}$ all have $\gcd(\cdot, m) > 1$ hence also $\gcd(\cdot, 2m) > 1$, while $\{e_1 + m, \ldots, e_{\varphi(m)} + m\}$ have $\gcd(\cdot, m) = 1$, but also $\gcd(\cdot, 2m) = 1$ since they are all odd numbers.

Thus, putting this information together we get that since the $e_i$’s, $e_i + m$’s, $d_j$’s, $d_j + m$’s are just the set $\{1, \ldots, 2m\}$ in some order, we have

$$\varphi(2m) = 2\varphi(m).$$

3. Let’s show that $10q + r$ is divisible by 7 iff $q - 2r$ is divisible by 7. We have

$$7|10q + r \iff 7|3q + r \iff 7|3(q - 2r) + 7r \iff 7|3(q - 2r) \iff 7|q - 2r.$$ 

4. Using Wolfram Alpha, we get $p = 8971, q = 8243$. So this gives us $n = 73,947,953$. We have that

$$\varphi(pq) = (p-1)(q-1) = 73,930,740 = 2^2 \cdot 3 \cdot 5 \cdot 13^2 \cdot 23 \cdot 317.$$ 

After a few tries, we can find $e = 4679$, which is relatively prime to $\varphi(n)$. So the public key is $(n, e)$. To compute the private key $d$, we need to solve

$$ed \equiv 1 \mod \varphi(n).$$

A solution is given by $d = 553,019$. To encrypt the message, we compute

$$c(m) = m^e \mod n = 73,030,096.$$
Now, to recover the original message from the ciphertext, we compute

\[ c(m)^d \mod n = 2015. \]

5. We can get two random odd 4-digit composite numbers: \( n_1 = 2037 \) and \( n_2 = 3027 \). We have \( n_1 \equiv 1 \mod 4 \) and \( n_2 \equiv 3 \mod 4 \). We have \( n_1 - 1 = 2^2 \cdot 509 \) and \( n_2 - 1 = 2 \cdot 1513 \). So \( d_1 = 509 \) and \( d_2 = 1513 \).

We have that 57 is a composite witness for both \( n_1 \) and \( n_2 \). Indeed, \( 57^{d_1} \not\equiv \pm 1 \mod n_1 \) and \( 57^{2d_1} \not\equiv -1 \mod n_1 \), so 57 is a composite witness for \( n_1 \). Similarly, we have \( 57^{d_2} \not\equiv \pm \mod n_2 \), which shows that 57 is a composite witness for \( n_2 \).

6. The public key is a pair of numbers \((n, e)\) where \( n \) is a product of two large primes \( p, q \) and \( e \) is relatively prime to \( \varphi(n) \). The secret key is \( d \) such that \( ed \equiv 1 \mod \varphi(n) \).

Adam can send Nets a message \( m \), and Nets can send back \( \sigma(m) = m^d \mod n \). Adam can then verify, using the public key, that

\[ \sigma(m)^e \equiv m^{de} \mod n \equiv m \mod n \]

recovers the initial message. Since only Nets knows the private key \( d \), this will constitute proof that Adam is indeed in contact with Nets.