1. **Theorem:**

Suppose $p$ and $q$ are large distinct odd primes and $n = pq$. Let $A$ satisfy $\gcd(A, n) = 1$. Observe $\gcd(A, p) = \gcd(A, q) = 1$ too.

Then if $x^2 \equiv A \mod n$ has any solutions at all then it has exactly four distinct solutions.

**Proof:**

First note that if $x^2 \equiv A \mod n$ has solutions then so do $x^2 \equiv A \mod p$ and $x^2 \equiv A \mod q$ and in fact they have two each. We know this from studying quadratic residues.

Next note that by the Chinese Remainder Theorem solutions of $x^2 \equiv A \mod n = pq$ correspond exactly to pairs of solutions to $x^2 \equiv A \mod p$ and $x^2 \equiv A \mod q$. Thus in total we have four solutions.

Suppose $x \equiv a \mod n$ is one solution, so $a^2 \equiv A \mod n$.

(a) Consider the system of congruences:

\[
\begin{align*}
    x &\equiv a \mod p \\
    x &\equiv a \mod q
\end{align*}
\]

By the CRT this has a unique solution mod $n = pq$. Since the first equation implies $x^2 \equiv a^2 \equiv A \mod p$ and the second equation implies $x^2 \equiv a^2 \equiv A \mod q$ and since $\gcd(p, q) = 1$ we get $x^2 \equiv a^2 \equiv A \mod n = pq$. Call this solution $X$.

(b) Observe that $x = -X$ is also a solution because $(-X)^2 \equiv X^2 \equiv A \mod n = pq$.

Moreover note that this $-X$ satisfies the system:

\[
\begin{align*}
    x &\equiv -a \mod p \\
    x &\equiv -a \mod q
\end{align*}
\]

(c) Consider the system of equations:

\[
\begin{align*}
    x &\equiv a \mod p \\
    x &\equiv -a \mod q
\end{align*}
\]

By the CRT this has a unique solution mod $n = pq$. Since the first equation implies $x^2 \equiv A \mod p$ and the second equation implies $x^2 \equiv A \mod q$ and since $\gcd(p, q) = 1$ we get $x^2 \equiv A \mod n = pq$. Call this solution $Y$.

(d) Observe that $x = -Y$ is also a solution because $(−Y)^2 \equiv Y^2 \equiv A \mod n = pq$.

Moreover note that this $-Y$ satisfies the system:

\[
\begin{align*}
    x &\equiv -a \mod p \\
    x &\equiv a \mod q
\end{align*}
\]

(e) Note that these are all distinct mod $n$ because all satisfy different pairs of congruences mod $p$ and $q$. 

2. **Theorem:**
If \( p \equiv 3 \mod 4 \) and if \( x^2 \equiv A \mod p \) has solutions then we can find them easily.

**Proof:**
There must be two and then since \( A \) is a quadratic residue we know \( A^{(p-1)/2} = \left( \frac{A}{p} \right) = 1 \) by Euler’s Criterion and then:

\[
\left( \pm A^{(p+1)/4} \right)^2 \equiv A^{(p+1)/2} \equiv A \cdot A^{(p-1)/2} \equiv A \cdot 1 \equiv A \mod p
\]

3. **Theorem:**
Consider the equation \( x^2 \equiv A \mod n \). If we know \( p, q \) with \( n = pq \) and if there are solutions then there are four and we can easily find them.

**Proof:**
Since \( x^2 \equiv A \mod n \) has solutions so do \( x^2 \equiv A \mod p \) and \( x^2 \equiv A \mod q \).
By the above calculation the equation \( x^2 \equiv A \mod p \) has solutions \( x \equiv \pm A^{(p+1)/4} \mod p \) and the equation \( x^2 \equiv A \mod q \) has solutions \( x \equiv \pm A^{(q+1)/4} \mod q \).
This gives us the four systems which arise in the first Theorem. More specifically we solve the following to get \( X \) and from then we get \(-X\):

\[
x \equiv A^{(p+1)/4} \mod p
\]
\[
x \equiv A^{(q+1)/4} \mod q
\]
And we solve the following to get \( Y \) and from then we get \(-Y\):

\[
x \equiv A^{(p+1)/4} \mod p
\]
\[
x \equiv -A^{(q+1)/4} \mod q
\]

**Example:**
Suppose \( p = 31 \) and \( q = 43 \). Let \( n = pq = 1333 \). Suppose we know \( x^2 \equiv 669 \mod 1333 \). We solve the first system:

\[
x \equiv 669^{(31+1)/4} \equiv 7 \mod 31
\]
\[
x \equiv 669^{(43+1)/4} \equiv 14 \mod 43
\]
The CRT gives \( x \equiv 100 \mod 1333 \). This is our \( X \). We know that \(-X \equiv 1233 \mod 1333 \) would solve the system with \(-7, -14\).
We solve the second system:

\[
x \equiv 669^{(31+1)/4} \equiv 7 \mod 31
\]
\[
x \equiv -669^{(43+1)/4} \equiv -14 \mod 43
\]
The CRT gives \( x \equiv 1061 \mod 1333 \). This is our \( Y \). We know that \(-Y \equiv 272 \mod 1333 \) would solve the system with \(-7, 14\).
All together we have: \( X = 100, -X = 1233, Y = 1061, -Y = 272 \).
4. **Theorem:**

Consider the equation \( x^2 \equiv A \mod n = pq \). Suppose there is a solution \( x \equiv a \mod n \). Then if \( \pm X, \pm Y \) are the four solutions as constructed earlier then knowing one of \( \pm X \) and one of \( \pm Y \) is equivalent to factoring \( n \).

**Proof:**

\( \implies : \)

Suppose we know \( X, Y \). Observe that \( X + Y \equiv 2a \not\equiv 0 \mod p \) and \( X + Y \equiv 0 \mod q \). Note that \( 2a \not\equiv 0 \mod p \) because \( p \nmid 2 \) and \( p \nmid a \).

Thus \( p \mid (X+Y) \) and \( q \mid (X+Y) \) and so \( \gcd (X+Y, n) = q \) which we can find using the Euclidean Algorithm. Then we can find \( p = n/q \).

A similar argument works for \( X, -Y, -X, Y \) and \( -X, -Y \). With details omitted:

\( \gcd (-X - Y, n) = q \) too.

\( \gcd (X + (-Y), n) = p \) (see homework).

\( \gcd (-X + Y, n) = p \) too.

\( \Leftarrow : \)

If we can factor \( n \) then we can solve the systems.

5. **Process:**

We then proceed as follows:

(a) Alice picks two large odd primes \( p \) and \( q \) both congruent to 3 mod 4 and calculates \( n = pq \). She sends \( n \) to Bob.

(b) Bob then picks some \( b \) with \( \gcd (b, n) = 1 \) and sends \( S \equiv b^2 \mod n \) back to Alice. Keep in mind that Bob knows one solution to \( x^2 \equiv S \mod n \) (that’s his \( b \)) but doesn’t know which of the systems’ \( x, -X, Y, -Y \) this is because he doesn’t know \( p, q \) and hence can’t solve the systems.

(c) Since Alice knows \( p \) and \( q \) she can find \( X, -X, Y, -Y \). She knows that one of these is Bob’s \( b \) but doesn’t know which.

(d) Alice picks one, call it \( R \). She has an equal chance of choosing one that will help Bob factor \( n \) and one that will not.

(e) She sends that one back to Bob.

(f) If Bob can factor \( n \) with what he has then he wins the coin flip. Otherwise Alice wins. Really he just tests \( \gcd (\pm S \pm R, n) \) and sees if he gets something other than 1 or \( n \).

6. **Example:**

Alice chooses \( p = 31 \) and \( q = 43 \) and calculate \( n = pq = 1333 \). She sends this to Bob. Bob picks \( b = 100 \) and calculates \( b^2 \equiv 669 \mod 1333 \) and sends 669 back to Alice. Alice solves \( x^2 \equiv 898 \mod 1333 \) and gets solutions 100, 272, 1061, 1233. She knows Bob used one of these but doesn’t know which. She chooses one of them and sends it back. If she sends back 100 or 1233 then Bob cannot factor \( n \). However if she sends back 272 or 1061 then he can. Observe:

- If she sends 100 then Bob tests \( \gcd (\pm 100 \pm 100, 1333) \) and they all equal 1 or 1333.
- If she sends 1233 then Bob tests \( \gcd (\pm 100 \pm 1233, 1333) \) and they all equal 1 or 1333.
- If she sends 272 then Bob tests \( \gcd (\pm 100 \pm 272, 1333) \) and notes that the results are 31 or 43.
- If she sends 1061 then Bob tests \( \gcd (\pm 100 \pm 1061, 1333) \) and notes that the results are 31 or 43.