Solution of Problem 1

a) \( p = 13 \) is a prime number, \( a = 5 \) is a quadratic residue mod \( p \).

1) \[ v = b^2 - 4a = b^2 - 4 \cdot 5 = b^2 - 20. \]

   Choose: \( b = 5 \implies v = 25 - 20 = 5 \).
   With Euler’s criterion, compute:
   \[
   (v)_{11} = (5)_{11} = 5^{10/2} = 1. \]
   \( \implies v = 5 \) is a quadratic residue mod 11.

   Choose: \( b = 6 \implies v = 36 - 20 = 16 \equiv 5 \mod 11. \)
   \( \implies v = 5 \) is a quadratic residue mod 11.

   Choose: \( b = 7 \implies v = 49 - 20 = 29 \equiv 7 \mod 11. \)
   With Euler’s criterion, compute:
   \[
   (\frac{7}{11}) = 7^{10/2} \equiv 7^{5} \equiv 49 \cdot 49 \cdot 7 \equiv 5 \cdot 5 \cdot 7 \equiv -1 \mod 11. \]
   \( \implies v \) is a quadratic non-residue modulo 11.

2) Insert the values for \( a \) and \( b \) into the polynomial \( f(x) = x^2 - 7x + 5 \).

3) Compute \( r = x^{\frac{\phi(p)}{2}} \mod f(x) \):

   \[
   x^6 : (x^2 - 7x + 5) = x^4 + 7x^3 + 2x - 3
   - (x^6 - 7x^5 + 5x^4)
   + 7x^5 - 5x^4
   - (7x^5 - 5x^4 + 2x^3)
   - 2x^3
   - (-2x^3 + 3x^2 - 10x)
   - 3x^2 + 10x
   - (-3x^2 + 10x - 4)
   \]
   
   Hence, \( r = 4 \). Furthermore, and \(-r = -4 \equiv 7 \mod 11 \implies (r, -r) = (4, 7)\).
   // Validation \( r^2 = a \mod 11 \) is correct in both cases.

b) Both \( p, q \) satisfy the requirement for a Rabin cryptosystem: \( p, q \equiv 3 \mod 4 \).
   For \( c \mod p \equiv 225 \mod 11 \equiv 5 \), we already know the square roots \( x_{p,1} = 4, x_{p,2} = 7 \).
For $c \mod q \equiv 225 \mod 23 \equiv 18$, compute the square roots $x_{q,1}, x_{q,2}$ with the auxiliary parameter $k_q = \frac{q+1}{4} = 6$:

$$x_{q,1} = c^{k_q} = 18^6 = 18^3 \cdot 18^3 \equiv 13 \cdot 13 \equiv 8 \mod 23,$$
$$x_{q,2} = -8 \equiv 15 \mod 23.$$

Formulate $tq + sp = 1$:

$$23 = 2 \cdot 11 + 1$$
$$\Rightarrow 1 = 23 - 2 \cdot 11$$

We set $a = tq = 23$ and $b = sp = -22$. Compute all four possible solutions:

$$m_{11} = ax_{p,1} + bx_{q,1} = 23 \cdot 4 - 22 \cdot 8 = -84 \equiv 169 \mod 253 \Rightarrow (...1001)_2 \quad \cdot$$
$$m_{12} = ax_{p,1} + bx_{q,2} = 23 \cdot 4 - 22 \cdot 15 = -238 \equiv 15 \mod 253 \Rightarrow (...1111)_2 \quad \cdot$$
$$m_{21} = ax_{p,2} + bx_{q,1} = 23 \cdot 7 - 22 \cdot 8 = -15 \equiv 238 \mod 253 \Rightarrow (...1110)_2 \quad \cdot$$
$$m_{22} = ax_{p,2} + bx_{q,2} = 23 \cdot 7 - 22 \cdot 15 = -169 \equiv 84 \mod 253 \Rightarrow (...0100)_2 \quad \checkmark$$

The solution is $m = m_{21} = 84$ since it ends on 0100 in the binary representation.

// Checking all solutions yields $c = 225$.

c) Since $c = 225$, one is enabled to compute two square roots in the reals, $m = \pm 15$. If naive Nelson chooses 1111, the result $m = 15$ is obvious, without knowing the factors in $n = pq$. 
Solution of Problem 2
Decipher $m = \sqrt{c} \mod n$ with $c = 1935$.

- Check $p, q \equiv 3 \mod 4 \checkmark$

- Compute the square roots of $c$ modulo $p$ and $c$ modulo $q$.
  \[
  k_p = \frac{p + 1}{4} = 17, \quad k_q = \frac{q + 1}{4} = 18,
  \]
  \[
  x_{p,1} = c^{k_p} \equiv 1935^{17} \equiv 59^{17} \equiv 40 \mod 67,
  \]
  \[
  x_{p,2} = -x_{p,1} \equiv 27 \mod 67,
  \]
  \[
  x_{q,1} = c^{k_q} \equiv 1935^{18} \equiv 18^{18} \equiv 36 \mod 71,
  \]
  \[
  x_{q,2} = -x_{q,1} \equiv 35 \mod 71.
  \]

- Compute the resulting square root modulo $n$. $m_{i,j} = ax_{p,i} + bx_{q,j}$ solves $m_{i,j}^2 \equiv c \mod n$ for $i, j \in \{1, 2\}$. We substitute $a = tq$ and $b = sp$. Then $tq + sp = 1$ yields
  \[
  1 = 17 \cdot 71 + (-18) \cdot 67 = tq + sp \text{ from the Extended Euclidean Algorithm.}
  \]
  \[
  \Rightarrow a \equiv tq \equiv 17 \cdot 71 \equiv 1207 \mod n
  \]
  \[
  \Rightarrow b \equiv -sp \equiv -18 \cdot 67 \equiv -1206 \mod n.
  \]

The four possible solutions for the square root of ciphertext $c$ modulo $n$ are:

- $m_{1,1} \equiv ax_{p,1} + bx_{q,1} \equiv 107 \mod n \Rightarrow 0000001101011$,
- $m_{1,2} \equiv ax_{p,1} + bx_{q,2} \equiv 1313 \mod n \Rightarrow 0010100100001$,
- $m_{2,1} \equiv ax_{p,2} + bx_{q,1} \equiv 3444 \mod n \Rightarrow 0110101110100$,
- $m_{2,2} \equiv ax_{p,2} + bx_{q,2} \equiv 4650 \mod n \Rightarrow 1001000101010$.

The correct solution is $m_1$, by the agreement given in the exercise.
Solution of Problem 3

a) Given \( x \equiv -x \mod p \), prove that \( x \equiv 0 \mod p \).

Proof. The inverse of \( 2 \) modulo \( p \) exists. Then,

\[
-x \equiv x \mod p \\
\iff 0 \equiv 2x \mod p \\
\iff 0 \equiv x \mod p.
\]

\[\square\]

b) Looking at the protocol, we can show that Bob always loses to Alice, if she chooses \( p = q \).

i) Alice calculates \( n = p^2 \) and sends \( n \) to Bob.

ii) Bob calculates \( c \equiv x^2 \mod n \) and sends \( c \) to Alice. With high probability \( p \nmid x \iff x \not\equiv 0 \mod p \) (therefore, Bob almost always loses).

iii) The only two solutions \( \pm x \) are calculated by Alice (see below) and sent to Bob. Bob cannot factor \( n \), as

\[
\gcd(x - (\pm x), n) = \begin{cases} 
\gcd(0, n) = n \\
\gcd(2x, n) = \gcd(2x, p^2) = 1 
\end{cases}.
\]

Alice always wins.

c) If Bob asks for the secret key as confirmation, the square is revealed and Alice will be accused of cheating. Bob can factor \( n \) by calculating \( p = \sqrt{n} \) as a real number and win the game.

Note: The two solutions \( \pm x \) to \( x^2 \equiv c \mod p^2 \) can be calculated as follows.

Let \( p \) be an odd prime and \( x, y \not\equiv 0 \mod p \). If \( x^2 \equiv y^2 \mod p^2 \), then \( x^2 \equiv y^2 \mod p \), so \( x \equiv \pm y \mod p \).

Let \( x \equiv y \mod p \). Then

\[
x = y + \alpha p.
\]

By squaring we get

\[
x^2 = y^2 + 2\alpha py + (\alpha p)^2 \\
\Rightarrow x^2 \equiv y^2 + 2\alpha py \mod p^2.
\]

Since \( x^2 \equiv y^2 \mod p^2 \), we obtain

\[
0 = 2\alpha py \mod p^2.
\]

Divide by \( p \) to get

\[
0 = 2\alpha y \mod p.
\]

Since \( p \) is odd and \( p \nmid y \), we must have \( p \nmid \alpha \). Therefore, \( x = y + \alpha p \equiv y \mod p^2 \). The case \( x \equiv -y \mod p \) is similar.
In other words, if \( x^2 \equiv y^2 \mod p^2 \), not only \( x \equiv \pm y \mod p \), but also \( x \equiv \pm y \mod p^2 \). At this point, we have shown that only two solutions exist.

Now, we show how to find \( \pm x \), where \( x^2 \equiv c \mod p^2 \). As we can find square roots modulo a prime \( p \), we have \( x = b \) solves \( x^2 \equiv c \mod p \). We want \( x^2 \equiv c \mod p^2 \). Square \( x = b + ap \) to get

\[
\begin{align*}
  b^2 + 2bap + (ap)^2 &\equiv b^2 + 2bap \equiv c \mod p \\
  \Rightarrow b^2 &\equiv c \mod p.
\end{align*}
\]

Since \( b^2 \equiv c \mod p \) the number \( c - b^2 \) is a multiple of \( p \), so we can divide by \( p \) and get

\[
2ab \equiv \frac{c - b^2}{p} \mod p.
\]

Multiplying by the multiplicative inverse modulo \( p \) of 2 and \( b \), we obtain:

\[
a \equiv \frac{c - b^2}{p} \cdot 2^{-1} \cdot b^{-1} \mod p.
\]

Therefore, we have \( x = b + ap \).

This procedure can be continued to get solutions modulo higher powers of \( p \). It is the numeric-theoretic version of Newton’s method for numerically solving equations, and is usually referred to as Hensel’s Lemma.

Example: \( p = 7, p^2 = 49, c = 37 \). Then

\[
\begin{align*}
  b &= c^{\frac{p+1}{2}} = 37^{\frac{7+1}{2}} = 37^2 \equiv 4 \mod p, \\
  b^{-1} &\equiv 2 \mod p, \ 2^{-1} \equiv 4 \mod p, \\
  a &= \frac{c - b^2}{p} \cdot 2^{-1} \cdot b^{-1} = \frac{37 - 4^2}{7} \cdot 4 \cdot 2 \equiv 3 \mod p \Rightarrow x = b + ap = 4 + 3 \cdot 7 = 25
\end{align*}
\]

Check: \( x^2 = 25^2 \equiv 37 \equiv c \mod p^2 \).