- Find all eigenvectors and eigenvalues of the matrix $\begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 3 \\ 0 & 0 & 2 \end{pmatrix}$ [2+2+2=6 Marks]

  We can use here properties of Eigenvector/eigenvalues or can calculate them otherwise. Using a diagonal property: $\lambda_1 = 1, x_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and and $\lambda_2 = -1, x_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$. Finally, using row sum property, we get $\lambda_3 = 2, x_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$.

- Find factors of $N = 35$ using Shor's algorithm. [5 Marks]

  Given marks based on the steps even when students have not calculate the final result.

  1. choose a random x from 2 to 76
  2. Check that x is itself not a factor of n (which it should not be. If student choose x as a factor please deduct his/her marks.)
  3. find order r, such that $x^r \equiv 1 \mod 77$
  4. check if r is even and $GCD(x^{\frac{r}{2}}+1, n) > 1)$ (or $GCD(r^{\frac{r}{2}}-1, n) > 1)$),
  5. Then factors are p= $GCD(r^{\frac{r}{2}}+1, n) > 1)$ (or $GCD(r^{\frac{r}{2}}-1, n) > 1)$) and $q = \frac{n}{p}$

- Given RSA algorithm if prime number p=5, q=11, and public key e=3 is used. What will be the private key? [4 Marks]

  $n = 5 = 55$
  $\phi(n) = (5-1) \times (11-1) = 40$
  Choose public key $e = 3$ where $e \mod \phi(n) = 1$
  Calculate private key d such that $e.d = 1 \mod$
  $d = 27$

- Find all eigenvectors and eigenvalues of the matrix $\begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 3 \end{pmatrix}$ [2+2+2=6 Marks]

  We can use here properties of Eigenvector/eigenvalues or can calculate them otherwise. Using a diagonal property: $\lambda_1 = 2, x_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and and $\lambda_2 = 1, x_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$. Finally, using row sum property, we get $\lambda_3 = 3, x_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$.

- Find factors of $N = 77$ using Shor's algorithm. [5 Marks]

  Given marks based on the steps even when students have not calculate the final result.

  1. choose a random x from 2 to 76
  2. Check that x is itself not a factor of n (which it should not be. If student choose x as a factor please deduct his/her marks.)
  3. find order r, such that $x^r \equiv 1 \mod 77$
  4. check if r is even and $GCD(x^{\frac{r}{2}}+1, n) > 1)$ (or $GCD(r^{\frac{r}{2}}-1, n) > 1)$),
  5. Then factors are p= $GCD(r^{\frac{r}{2}}+1, n) > 1)$ (or $GCD(r^{\frac{r}{2}}-1, n) > 1)$) and $q = \frac{n}{p}$

- Given RSA algorithm if prime number p=7, and q=17 used. Find appropriate public and private keys. Please show your steps clearly. [4 Marks]

  $n = 7 = 119$
  $\phi(n) = (7-1) \times (17-1) = 96$
  Choose public key $e = 5$ where $e \mod \phi(n) = 1$ (student may choose different)
  Calculate private key d such that $e.d = 1 \mod$
  $d = 77$

- Find all eigenvectors and eigenvalues of the Hadamard matrix. [6 Marks] We know that $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ Let's find eigenvector and eigenvalues of this matrix. Note, H is both Unitary and Hermition matrix therefore it eigenvalues could be 1 and -1 only. But lets check. We first calculate eigenvalues by solving $|H - \lambda I| = 0$. This indeed gives us $\lambda_1 = 1$ and $\lambda_2 = -1$. Now we use $(H - \lambda I)\vec{x} = \vec{0}$ which gives us eigenvectors of $\begin{pmatrix}1+\sqrt{2}\\ 1\end{pmatrix}$, $\begin{pmatrix}-\sqrt{2}+1\\ 1\end{pmatrix}$ (Student may have found multiples of these vectors which is also fine).

- Find factors of $N = 35$ using Shor's algorithm. [5 Marks] Given marks based on the steps even when students have not calculate the final result.

    1. choose a random x from 2 to 76
    2. Check that x is itself not a factor of n (which it should not be. If student choose x as a factor please deduct his/her marks.)
    3. find order r, such that $x^r \equiv 1 \mod 77$
    4. check if r is even and $GCD(x^{\frac{r}{2}} + 1, n) > 1)$ (or $GCD(r^{\frac{r}{2}} - 1, n) > 1)$),
    5. Then factors are p= $GCD(r^{\frac{r}{2}} + 1, n) > 1)$ (or $GCD(r^{\frac{r}{2}} - 1, n) > 1)$) and $q = \frac{n}{p}$

- Compute $\phi(185)$ [2 Marks] $185 = 5 \times 37$
  $\phi(185) = (5 - 1) \times (37 - 1) = 144$

- Compute $GCD(630, 231)$ [2 Marks] We can use Euclidean algorithm as follows:

$$\begin{aligned}
&GCD(630, 231)\\
&= GCD(231, 630 \mod 231 = 168)\\
&= GCD(168, 231 \mod 168 = 63)\\
&= GCD(63, 168 \mod 63 = 42)\\
&= GCD(42, 63 \mod 42 = 21)\\
&= GCD(21, 42 \mod 21 = 0)\\
&= 21
\end{aligned}$$