# UEE4611 Assignment #2, 2020 due April 2

1. Show that if $n$ is an odd composite integer, then the Miller-Rabin test will return "inconclusive" for $a = 1$ and $a = n - 1$. (10%)

2. One way to solve the key distribution problem is to use a line from a book that both the sender and the receiver possess. Consider the following message:

   ```
   K HFRC LQJNAF
   ```

   This ciphertext was produced using the first sentence of The Other Side of Silence (a book about the spy Kim Philby):

   ```
   The snow lay thick on the steps and the snowflakes driven by the wind
   looked black in the headlights of the cars...
   ```

   A simple substitution cipher was used. (Hint: Second and subsequent occurrences of a letter in the key sentence are ignored.) What is the plaintext? (10%)

3. (a) Encrypt the message "meet me at nctu" using the Hill cipher with the key $\begin{pmatrix} 7 & 3 \\ 2 & 5 \end{pmatrix}$. Show your calculations and the result. (10%)

   (b) Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext. (10%)

4. Determine the inverse mod 26 of $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$. (10%)

5. Using the Vigenère cipher, encrypt the word "cryptographic" using the word "eng". (10%)