MATH120
Discrete Mathematics

Assignment 6 **Due 5pm on Friday 16 September 2022**

1. The ciphertext

   `X W U U X X R J W W`

   was encrypted with an affine cipher. Given that the plaintext letters `E`, `T` are encrypted as the ciphertext letters `W`, `X` respectively.

   (a) Determine the encryption function $e(x) = ax + b$.

   (b) Decrypt the ciphertext message.

2. Suppose that Bob wants to set-up an RSA cryptosystem. He chooses $p = 17$ and $q = 31$, so $n = 17 \times 31 = 527$.

   (a) Determine whether $(n, e) = (527, 35)$ would be a valid public key.

   (b) Bob decides to use $(n, e) = (527, 37)$ as his public key. Find the corresponding private key d.

3. Alice sets up an RSA system with $p = 11$, $q = 13$, and public key $(n, e) = (143, 17)$. She also computes $d = 113$.

   Note: You may use a computer to calculate the exponents for (a) and (b) below but you must clearly communicate what these calculations are.

   (a) Suppose Bob wants to send the message $m = 53$ to Alice without Eve knowing the message. What does he send?

   (b) Next, suppose Alice receives the encrypted message $c = 81$ from Bob. What was this original message?

   (c) Suppose Eve discovers $p = 11$. Explain all the steps she would need to follow in order to decrypt messages.