UEE4611 Assignment #2 Solution

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

Suppose that $n - 1 = 2^k q$, where q is odd.
By step 3 of Miller-Rabin algorithm, we know that if $a^q \mod n = 1$, it will return "inconclusive".
If $a = 1$, $a^q \mod n = 1^q$. (always true while $n \neq 1$)

If $a = n - 1$, $a^q \mod n = (n-1)^q \equiv (-1)^q \equiv -1$, since q is odd.
In step 4, for $j = 1$, $(-1)^{2^0 q} = (-1)^q = -1 \equiv n - 1$. $\Rightarrow$ *return"inconclusive"*.

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?

First we reduce the sentence by deleting the letters showed up before.
Then,we get "**thesnowlayickpdfrvbg**", and decrypt these letters starting from $t \Rightarrow A$, $h \Rightarrow B$, $e \Rightarrow C$ ...
After the decryption of each letters, we can get the plaintext of "K HFRC LQJNAF", which is "I LOVE CRYPTO".

3. (a) Encrypt the message "meet me at nctu" using Hill cipher with the key $\begin{pmatrix} 7 & 3 \\ 2 & 5 \end{pmatrix}$. Show your calculations and result.
(b)Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

(a) Let $k = \begin{pmatrix} 7 & 3 \\ 2 & 5 \end{pmatrix}$.

$$\begin{gathered}(m\ e) \Rightarrow (12\ 4) \\ (e\ t) \Rightarrow (4\ 19) \\ \vdots \\ (12\ 4) \times k = (92\ 56)(\mod 26) \equiv (14\ 4)(\mod 26) \Rightarrow (o\ e)\end{gathered}$$

Therefore the ciphertext is *oeod oe mr rxrb*.

(b)

$$\begin{aligned} \det k &= = 29 \\ 29 \mod 26 &= 3 \\ \det k \times \det k^{-1} &\equiv 1 \mod 26 \\ 3 \times 9 = 27 &\equiv 1 \mod 26 \\ \Rightarrow \det k^{-1} &= 9 \end{aligned}$$

$$k^{-1} \mod 26 = 9 \begin{bmatrix} 5 & -2 \\ -3 & 7 \end{bmatrix} = \begin{bmatrix} 45 & -27 \\ -18 & 63 \end{bmatrix} = \begin{bmatrix} 19 & 8 \\ 25 & 11 \end{bmatrix}.$$

$$\begin{gathered}(o\ e) \Rightarrow (14\ 4) \\ (o\ d) \Rightarrow (14\ 3) \\ \vdots \\ (14\ 4) \times k^{-1} = (298\ 394)(\mod 26) \equiv (12\ 4)(\mod 26)\end{gathered}$$

Then we can get $(o\ e) \Rightarrow (m\ e)$.
Repeat the above steps, we can get the plaintexts = *meet me at nctu*

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

$$Let A = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

$$\begin{aligned} \det A \mod 26 &= \det \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \\ &= 441 \mod 26 \\ &= 25 \mod 26 \\ &= (-1) \mod 26 \end{aligned}$$

$$\begin{aligned} &\because (-1) \mod 26 \times (-1) \mod 26 \equiv 1 \mod 26 \\ &\therefore \det A^{-1} = (-1) \mod 26 = 25 \mod 26 \end{aligned}$$

$$A^{-1} \mod 26 = 25 \begin{pmatrix} 16 \times 15 - 10 & -(24 \times 15 - 1) & 24 \times 10 - 1 \times 16 \\ -(13 \times 15 - 10) & 6 \times 15 - 1 & -(6 \times 10 - 1) \\ 13 \times 17 - 16 & -(6 \times 17 - 24) & 6 \times 16 - 24 \end{pmatrix} \mod 26$$

$$= \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 9 \end{pmatrix}$$

5. Using the Vigenère cipher, encrypt the word "cryptographic" using the word "eng".

key	e	n	g	e	n	g	e	n	g	e	n	g	e
	4	13	6	4	13	6	4	13	6	4	13	6	4
plaintext	c	r	p	t	o	g	r	a	p	h	i	c	
	2	17	24	15	19	14	6	17	0	15	7	8	2
ciphertext	g	e	e	t	g	u	k	e	g	t	u	o	g