HW2 Cryptography 0716074蘇靖呈

#1 Assume n is an odd composite, then we use Miller-Rabin Test, consider $n-1=2^k\cdot q$, k must greater than 0 because $n-1$ is an even number, we take $a=1$ and $a=n-1$

(i) $a=1$

$$a^q \bmod n = 1^q \bmod n = 1$$

$\hookrightarrow$ inconclusive

(ii) $a=n-1$

$$(n-1)^q \bmod n = (-1)^q \bmod n = -1$$

$\hookrightarrow$ inconclusive

from (i)(ii), $a=1$ or $n-1 \Rightarrow$ inconclusive

#

#2 1° ignore second and subsequent occurence of the key sentence

plain	The	snow	lay	ick	p	d	f	r	v	b	g
cipher	ABC	DEFG	HIJ	KLM	N	O	P	Q	R	S	T

2° Decrypt : K HFRC LQJNAF

i love crypto #

#3 plaintext: meet me at nctu

12 4 4 19 12 4 0 19 13 2 19 20

(a)

use key $= \begin{bmatrix} 7 & 3 \\ 2 & 5 \end{bmatrix}$,

$$\begin{bmatrix} 12 & 4 \\ 4 & 19 \\ 12 & 4 \\ 0 & 19 \\ 13 & 2 \\ 19 & 20 \end{bmatrix} \begin{bmatrix} 7 & 3 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 92 & 56 \\ 66 & 107 \\ 92 & 56 \\ 38 & 95 \\ 95 & 49 \\ 193 & 157 \end{bmatrix} \xrightarrow{\text{mod}26} \begin{bmatrix} 14 & 4 \\ 14 & 3 \\ 14 & 4 \\ 12 & 17 \\ 17 & 23 \\ 11 & 1 \end{bmatrix} \xrightarrow{\text{encrypt}} \text{oeodoemrrxlb}$$

(b) Inverse $K^{-1} = (\det A)^{-1} \cdot \begin{bmatrix} 5 & -3 \\ -2 & 7 \end{bmatrix} \bmod 26 = \begin{bmatrix} 45 & -27 \\ -18 & 63 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 & -1 \\ 8 & 11 \end{bmatrix}$

$$\det A = 7\cdot 5 - 2\cdot 3 = 29 \xrightarrow{\text{mod}26} 3$$

$$(\det A)^{-1} = 3^{-1} \bmod 26 = 9$$

$$\begin{bmatrix} 14 & 4 \\ 14 & 3 \\ 14 & 4 \\ 12 & 17 \\ 17 & 23 \\ 11 & 1 \end{bmatrix} \begin{bmatrix} 19 & -1 \\ 8 & 11 \end{bmatrix} \cdot \text{mod}26 = \begin{bmatrix} 12 & 4 \\ 4 & 19 \\ 12 & 4 \\ 0 & 19 \\ 13 & 2 \\ 19 & 20 \end{bmatrix} \xrightarrow{\text{decrypt}} \text{meet me at nctu}$$

#4

inverse of $A = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$ mod 26.

$\det A = 6\begin{bmatrix} 16 & 10 \\ 17 & 15 \end{bmatrix} - 13\begin{vmatrix} 24 & 1 \\ 17 & 15 \end{vmatrix} + 20\begin{vmatrix} 24 & 1 \\ 16 & 10 \end{vmatrix}$

$= 420 - 4459 + 4480 = 441$

$(\det A)^{-1} = 441^{-1} \bmod 26 = (-1)^{-1} \bmod 26 = -1$

$$A^{-1} = -1\begin{bmatrix} +70 & -\,-5 & +\,-99 \\ -\,343 & +\,60 & -\,-378 \\ +\,224 & -\,47 & +\,-216 \end{bmatrix}^{T} = \begin{bmatrix} -70 & +343 & -224 \\ -+5 & -60 & +47 \\ 99 & -378 & 216 \end{bmatrix} \xrightarrow{\bmod 26} \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

#5

c r y p t o g r a p h i c

2, 17, 24, 15, 19, 14, 6, 17, 0, 15, 7, 8, 2

key "eng": 4, 13, 6, 4, 13, 6, 4, 13, 6, 4, 13, 6, 4

mod 26: 6, 4, 4, 19, 6, 20, 10, 4, 6, 19, 20, 14, 6

encrypted: g e e t g u k e g t u o g #