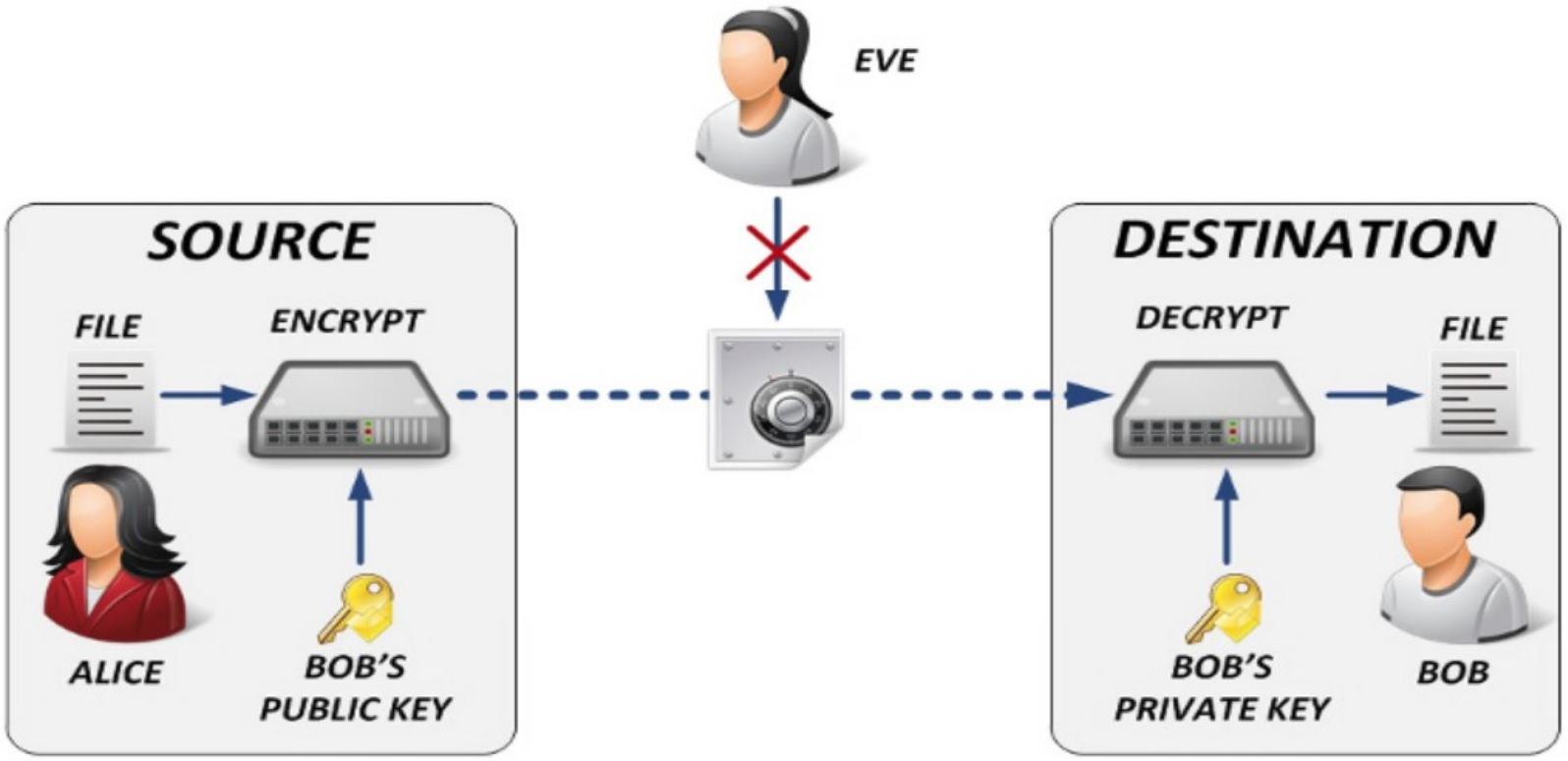
HW2 Hill cipher

TA 吳元魁

Cryptography



Hill cipher

- Hill cipher 是一種簡單的加密方式，利用矩陣的乘法就可以達到線性加密的效果。
- 首先要確定字母集S (= 31)

對 照 表																												
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_	.	,	?	!
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

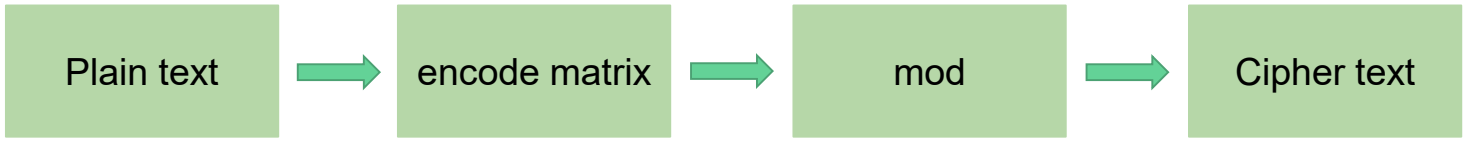
- Plain text: THIS IS AN APPLE.
- if n = 3
- THI S_I S_A N_A PPL E.. (最後一個不足n則重複末字母補齊)
- Key:

```
[[ 4  9 -2]
 [ 3  5  7]
 [ 1 -6 11]]
```

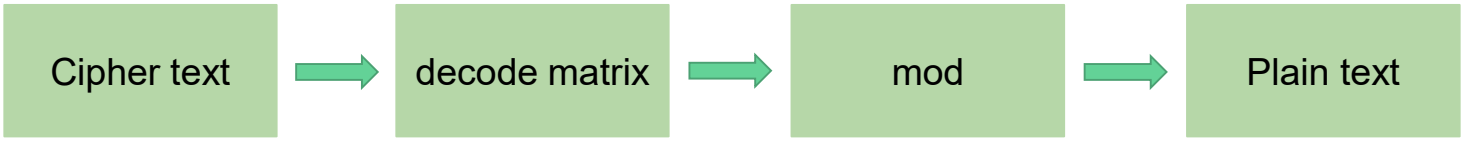
- 經過加密之後：WPK_FJEIIXZ.OQFPM_

Flow chart

encode stage:



decode stage:



Crack password:

[encode matrix] * [Plain] = [Cipher]

[encode matrix] = [Cipher] * [Plain]^-1

How to do

- Encode
  1. Tranform “THI S_I S_A N_A PPL E..” into matrix [redacted]
  2. Cipher = key*Plain (mod S)

     => WPK_[redacted]
- Decode
  1. Find modular inverse of a matrix (a little different to inverse matrix)
  2. Plain = mod_inv_key * Cipher (mod S)

     util.py (**在ceiba的檔案裡**)

     a. inv_key(key) may help, import it and use it.
     b. key is a numpy array.

破解Hill Cipher

- 利用線性獨立的Plain-Cipher pair 解 Key

  明文：POT TOP OPT

  密文：DQY ?AN ISR

- 將明文、密文化成矩陣，若線性獨立則可逆。
  - 加密式子 $AP = C$ (mod S)
  - 反推key $A = CP^{-1}$ (mod S)

- 利用線性獨立之P推出Key之後，則可反推所有密文之明文。

作業規定

```
ENFFISWLX_EYIJR
15 20 13 27 9 20 17 18 25

VRJO_PBB?OXOYSQ
YOU_HAD_TO_LIE_
EEE.FJAZUOQ??ZC
```

1. 每個人依據學號得到密文和明文(https://goo.gl/nyCKFN)，請依照自己的學號作答。
   a. 第一行為問題一的密文，第二行為問題一的public key，第四、五行分別為問題二的" a pair of cipher text(第四行) and plain text(第五行)"，第六行為需要問題二解密的密文(the other cipher text)
2. 請將答案存成「學號_ans.txt」上傳到CEIBA.
   a. 第1行請輸入學號，第2行輸入第一題答案，3~4行第二題答案，其中第3行為KEY，第4行是decode的結果。
   b. ex: (非第一項說明圖片的解答)

```
3 b02901137
2 IF_I_HAD_THE_NE
1 25 24 23 2 6 18 20 14 26
4   AFTER_A_WHILE_,
```

1. 題目請見LinearAlgebraHW#2.pdf
2. deadline: 10/26(五) 3:00 遲交每24小時: 分數*0.8

key, text轉換成矩陣

無論是key還是plain text, cipher text，請用numpy.reshape來轉換成矩陣
numpy.reshape(a, (3, 4))是將 a 這個numpy array轉換成 3x4 的矩陣
ex:
key: 11 12 13 14 15 16 17 18 19
plain text: ABCDEFGHIJKLMNO
key會變成[[11, 12, 13], [14, 15, 16], [17, 18, 19]]
plain text會變成[[1, 2, 3, 4, 5], [6, 7, 8, 9, 10], [11, 12, 13, 14, 15]]

測資:

cipher: VJWUV,EDI

plain: IS_THAT_W

key: 25 8 25 9 9 16 28 21 18

請注意臉書社團的Q&A

作業的一些補充規定會在上面和ceiba上做更新

Reference

李宏毅老師的說明影片：https://www.youtube.com/watch?v=G_dATE22UqY

現代啟示錄：Hill Cipher
https://ccjou.wordpress.com/2013/09/10/%E5%B8%8C%E7%88%BE%E5%AF%86%E7%A2%BC/?fbclid=IwAR175SK34eqCXJfhOsDnlk_0cEQ4bLSDG1BSSsd36JQSMaq436LxlpJolok

Appendix

modular inverse of a matrix

- The principle is the same, but one has to calculate the modular inverse of the matrix determinant.

$$A^{-1} = (\det A)^{-1} \operatorname{adj} A$$

det(A) = 200 ; (det(A))^-1 = 1/200 = 20 (mod 31)

$$A^{-1} = 20 \begin{bmatrix} \begin{vmatrix} 5 & 7 \\ -6 & 11 \end{vmatrix} & -\begin{vmatrix} 9 & -2 \\ -6 & 11 \end{vmatrix} & \begin{vmatrix} 9 & -2 \\ 5 & 7 \end{vmatrix} \\ -\begin{vmatrix} 3 & 7 \\ 1 & 11 \end{vmatrix} & \begin{vmatrix} 4 & -2 \\ 1 & 11 \end{vmatrix} & -\begin{vmatrix} 4 & -2 \\ 3 & 7 \end{vmatrix} \\ \begin{vmatrix} 3 & 5 \\ 1 & -6 \end{vmatrix} & -\begin{vmatrix} 4 & 9 \\ 1 & -6 \end{vmatrix} & \begin{vmatrix} 4 & 9 \\ 3 & 5 \end{vmatrix} \end{bmatrix} \pmod{31}$$

not 1/200

hint: when you call np.linalg.inv(), you will get $A^{-1} = (\det A)^{-1} \operatorname{adj} A$

but what you ne $A^{-1} = (\det A)^{-1} \operatorname{adj} A$

In this case, not 1/200, replace it by det(A)^-1 mod(31)

modular inverse of the matrix determinant

- What is 1/200 mod 31 ?
  - 200 * 20 (mod 31) = 1
  - 1/200 (mod 31) = 20