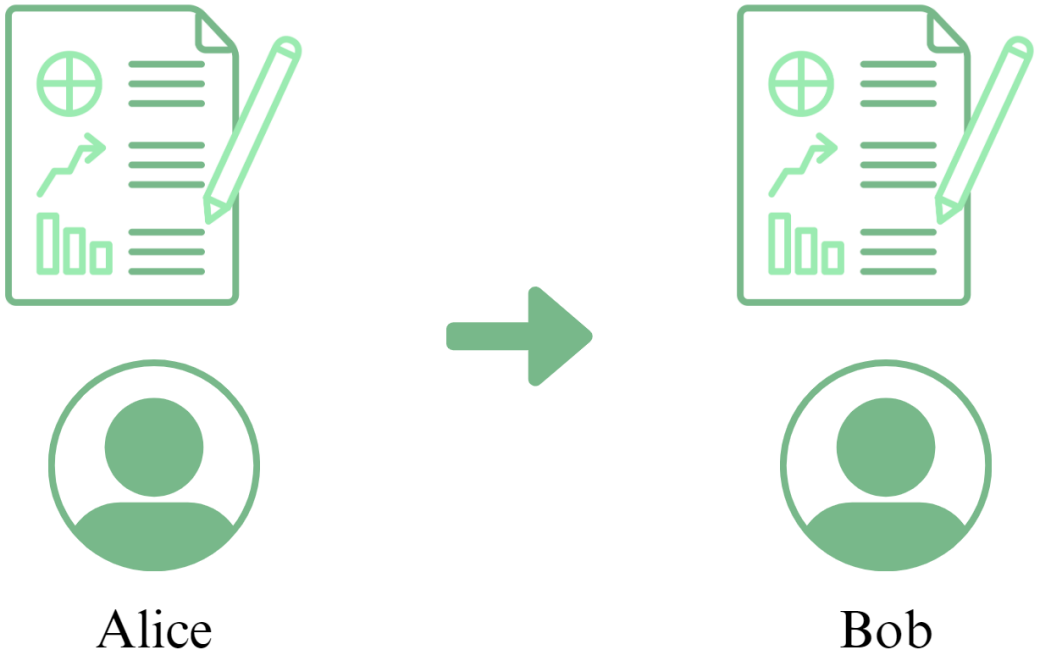
Linear Algebra HW2

Hill Cipher

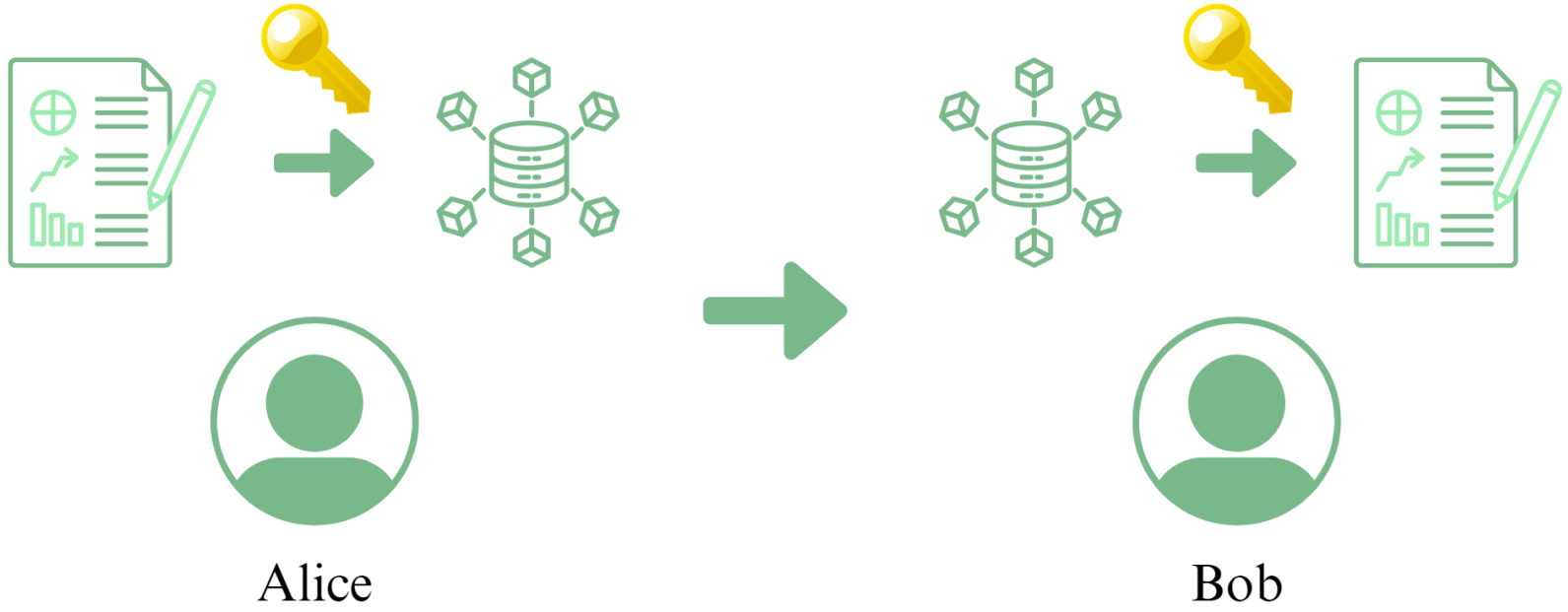
TA 陳品翔、何卓耀, Oct, 6th, 2023

Outline

Cryptography



Cryptography



Hill Cipher

- A simple cryptographic algorithm using matrix multiplication
- We have a letter set S and divide the plaintext into several groups (every group has n letters)
- In this homework, we choose following letter set ($S = 31$) and $n = 3$

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

Hill Cipher

- E.g. Plaintext is THIS_IS_AN_APPLE.

$$\Rightarrow \text{THI}\ \ \text{S\_I}\ \ \text{S\_A}\ \ \text{N\_A}\ \ \text{PPL}\ \ \text{E..}$$

$$\Rightarrow \begin{bmatrix} 19 & 18 & 18 & 13 & 15 & 4 \\ 7 & 26 & 26 & 26 & 15 & 27 \\ 8 & 8 & 0 & 0 & 11 & 27 \end{bmatrix}$$

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

Encoding

- Public key (Encoding matrix) @ plaintext ≡ ciphertext (mod S)
- @ means matrix multiplication
- mod means modulo
- E.g. $35 \equiv 4 \pmod{31}$, $-3 \equiv 28 \pmod{31}$

Encoding

- Public key (Encoding matrix) @ plaintext ≡ ciphertext (mod *S*)
- E.g.

$$\begin{bmatrix} 4 & 9 & -2 \\ 3 & 5 & 7 \\ 1 & -6 & 11 \end{bmatrix} \begin{bmatrix} 19 & 18 & 18 & 13 & 15 & 4 \\ 7 & 26 & 26 & 26 & 15 & 27 \\ 8 & 8 & 0 & 0 & 11 & 27 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 30 & 11 & 27 & 7 & 13 & 19 \\ 24 & 23 & 29 & 14 & 11 & 26 \\ 3 & 12 & 17 & 12 & 15 & 15 \end{bmatrix} \pmod{31}$$

Decoding

- Private key (Decoding matrix) @ ciphertext ≡ plaintext (mod *S*)
- E.g.

$$\begin{bmatrix} 18 & 27 & 3 \\ 7 & 21 & 2 \\ 5 & 9 & 15 \end{bmatrix} \begin{bmatrix} 30 & 11 & 27 & 7 & 13 & 19 \\ 24 & 23 & 29 & 14 & 11 & 26 \\ 3 & 12 & 17 & 12 & 15 & 15 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 19 & 18 & 18 & 13 & 15 & 4 \\ 7 & 26 & 26 & 26 & 15 & 27 \\ 8 & 8 & 0 & 0 & 11 & 27 \end{bmatrix} \pmod{31}$$

Decoding

- Private key (decoding matrix) is the modular inverse of public key
- E.g. $\begin{bmatrix} 18 & 27 & 3 \\ 7 & 21 & 2 \\ 5 & 9 & 15 \end{bmatrix}$ is the modular inverse of $\begin{bmatrix} 4 & 9 & -2 \\ 3 & 5 & 7 \\ 1 & -6 & 11 \end{bmatrix}$

How to hack?

- Public key (Encoding matrix) @ plaintext ≡ ciphertext (mod S)
- Given a pair of plaintext and ciphertext, we can calculate ciphertext @ plaintext^{-1} (mod S) to get public key
- Private key (Decoding matrix) @ ciphertext ≡ plaintext (mod S)
- If we get public key, we can get private key and decrypt other ciphertexts easily

Inverse

- The inverse of a matrix A is $A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)$
- For a 2×2 matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $\det(A) = ad - bc$, $\operatorname{adj}(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Inverse

- For a 3×3 matrix $A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$, $\det(A) = aei + bfg + cdh - ceg - bdi - afh$, $\operatorname{adj}(A) = \begin{bmatrix} +\begin{vmatrix} e & f \\ h & i \end{vmatrix} & -\begin{vmatrix} b & c \\ h & i \end{vmatrix} & +\begin{vmatrix} b & c \\ e & f \end{vmatrix} \\ -\begin{vmatrix} d & f \\ g & i \end{vmatrix} & +\begin{vmatrix} a & c \\ g & i \end{vmatrix} & -\begin{vmatrix} a & c \\ d & f \end{vmatrix} \\ +\begin{vmatrix} d & e \\ g & h \end{vmatrix} & -\begin{vmatrix} a & b \\ g & h \end{vmatrix} & +\begin{vmatrix} a & b \\ d & e \end{vmatrix} \end{bmatrix}$

Modular Inverse

- How to calculate 1/200 mod 31?

  Ans: Since $200 \times 20 \equiv 1 \pmod{31}$, $1/200 \equiv 20 \pmod{31}$

- How to calculate inverse of a matrix A?

  Ans: $A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$

- If $\det(A) = 200$, then $A^{-1} = 1/200 \times \text{adj}(A)$

Modular Inverse

- How to calculate modular inverse of a matrix A?

  Ans: $A^{-1} \equiv \frac{1}{\det(A)} \text{adj}(A) \pmod{S}$

- If $S = 31$, $\det(A) = 200$, then $A^{-1} \equiv 1/200 \times \text{adj}(A) \equiv 20 \times \text{adj}(A) \pmod{31}$

- How to calculate modular inverse in the homework?

  Ans: We provide a function, mod_inv(), in colab

HW2 Description

- Problem 1

  Given a pair of ciphertext and public key, find the plaintext

- Problem 2

  Given a pair of ciphertext and plaintext, find the public key first.

  Besides, we provide a ciphertext encrypted with same public key, find the plaintext

HW2 Description

- Please download your own file (B11901XXX.txt) at this link

p1 ciphertext ----------
p1 public key ----------

```
LBXJKZYNB,FZFYD
14 30 9 8 15 21 2 12 24
```

p2 ciphertext_1 ---------
p2 plaintext_1 ----------
p2 ciphertext_2 ---------

```
TFBS.QML?
S_WOKEISM
Y.J!FUMXW
```

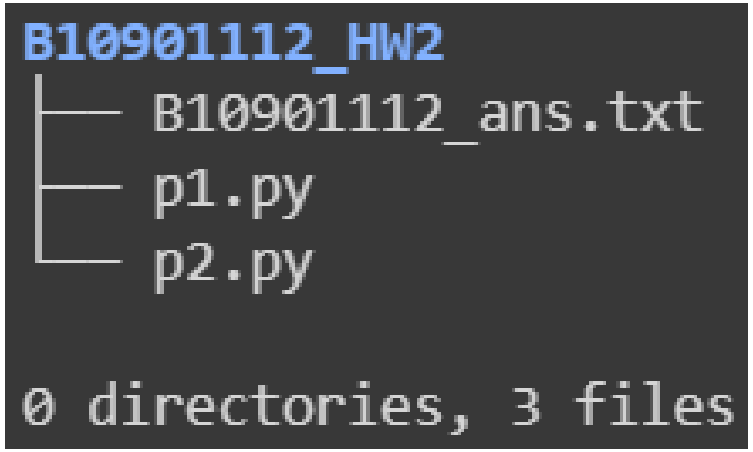
HW2 Description

- After completing p1.py, p2.py and running HW2.ipnyb, you will get an answer text file (B11901XXX_ans.txt)

```
student ID ---------- B10901112
p1 plaintext -------- OD,_A_SNOWBALL_
p2 public key ------- 21 6 9 2 26 20 28 23 19
p2 plaintext_2 ------ TH_VILENE
```

HW2 Description

- Archive p1.py, p2.py and B11901XXX_ans.txt in a folder (named B11901XXX_HW2), compress B11901XXX_HW2 into B11901XXX_HW2.zip and upload to NTU Cool



Turn Key & Text into Matrix

- Please use numpy.reshape to turn key & text into matrix
- E.g. Key is 11 12 13 14 15 16 17 18 19

np.reshape (key, (3, 3)) ⇒

```
[[11,12,13],
 [14,15,16],
 [17,18,19]]
```

Turn Key & Text into Matrix

- Remember to transpose after reshaping text
- E.g. Plaintext is ABCDEFGHIJKLMNO

$$\text{np.reshape (plaintext, } (-1,\ 3)).\text{T} \Rightarrow \begin{matrix}[[0,3,6,9,12],\\ [1,4,7,10,13],\\ [2,5,8,11,14]]\end{matrix}$$

Sample Outputs

```
IVXOVNEU_NG.THK
18 11 22 26 0 3 16 15 16


Z.XIAHKLM
EXCEPT_I_
GTKWUVQVV
```

```
XB?WOCEG.?.KTYC
6 30 19 11 7 6 27 2 3


HZMM.PYBY
SO_WE_FAK
BQJVE.,G,
```

```
B10901112
DAMN_IT_,_HENRY
30 0 30 9 14 5 9 7 6
GET_YOUR_
```

```
B10901112
WHYNOTJUSTGETA_
20 23 11 17 19 4 5 11 3
JUST_GET_
```

Grading Policy

- Total score of HW2: 100
- Problem 1 (p1.py) accounts for 40% of the total score
- Problem 2 (p2.py) accounts for 40% of the total score
- B11901XXX_ans.txt accounts for 10% of the total score
- Correct submission format accounts for 10% of the total score

Grading Policy

- No plagiarism and don't submit other's answer, or your grade will be 0 in this homework
- Date due: Nov. 3rd, 2023 (Fri.), 23:59 (GMT+8)
- Late submissions will get a penalty of 20% deduction per day
- No work will be accepted after three day past the due date

Colab Link

- https://colab.research.google.com/drive/1y-5kN7O_h6JNRUPr5IqNvBEjl0iCyMqB?usp=drive_link

Reference

- Colab of LA_2022_HW2 (https://colab.research.google.com/drive/17sROjCLCoxV897TSXWMjEEm3QrSG3bdA?usp=sharing)
- PDF of LA_2022_HW2