Lecture 8

Application (1):

15-Puzzle &

Introduction to Cryptography

What you will learn in Lecture 8

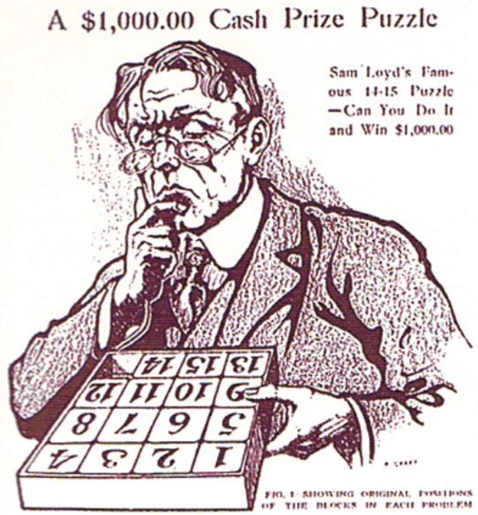
8.1 *15-Puzzle (15パズル)

8.2 *Introduction to Cryptography **(暗号理論)**

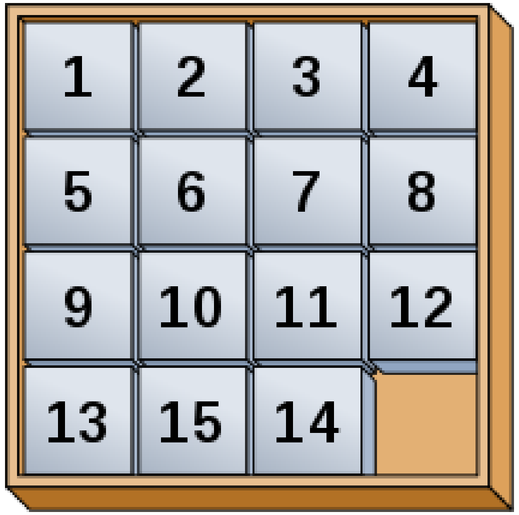
Notice: * mark is optional material. It will not be included in the final examination.

*8.1 15-Puzzle (15パズル)

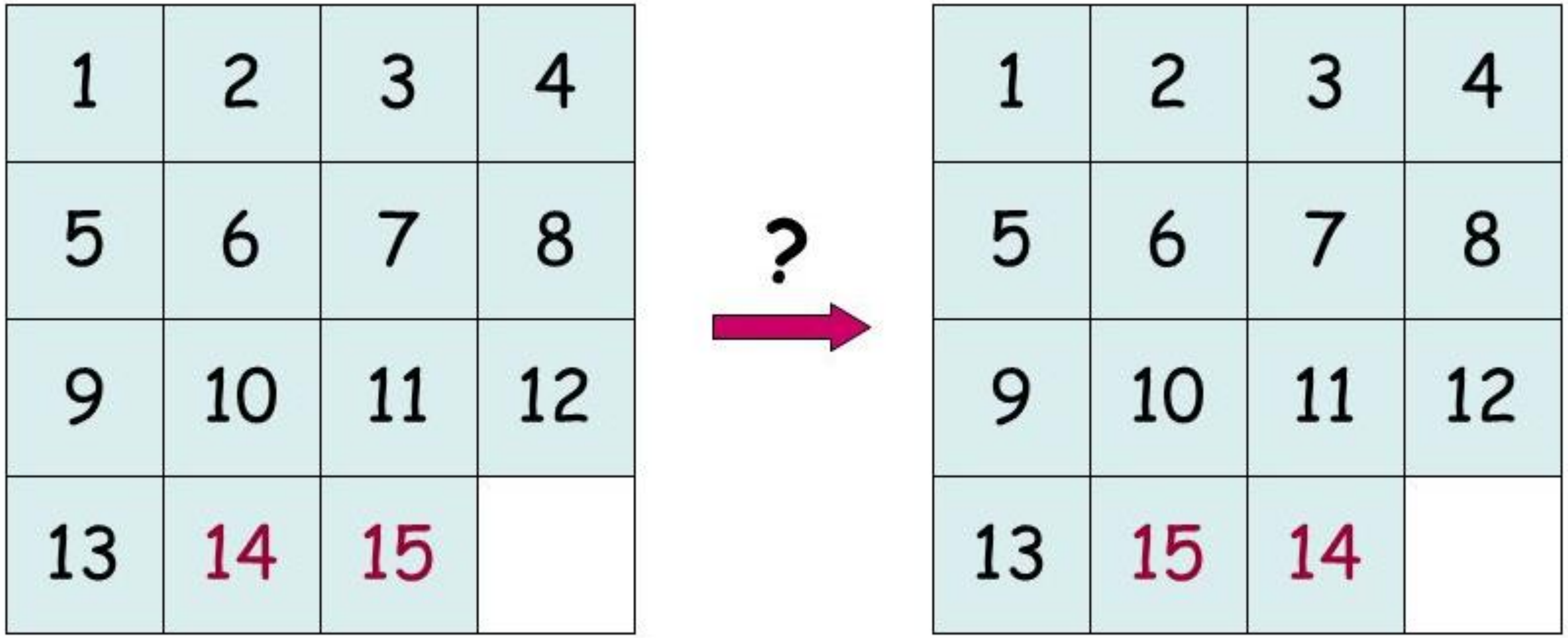
*8.1 15-Puzzle (15パズル)


A $1,000.00 Cash Prize Puzzle
Sam Loyd's Famous 14-15 Puzzle —Can You Do It and Win $1,000.00
FIG. 1 SHOWING ORIGINAL POSITIONS OF THE BLOCKS IN EACH PROBLEM

Starting in the 1890s, Sam Loyd offered a **$1000 prize (worth over $25000 today)** for anyone who could show a solution



1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

?

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

standard configuration

question configuration

*8.1 15-Puzzle (15パズル)

Assume empty space be piece 16. We can regard the standard configuration of 15-puzzle as a permutation:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \end{pmatrix}$$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

standard configuration

Easy to check for 15-puzzle, we have a permutation set S_{16} (recall S_3), then the question configuration:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 15 & 14 & 16 \end{pmatrix}$$

$$= (14\ 15)$$

Recall that a transposition is a 2-cycle.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	16

question configuration

*8.1 15-Puzzle (15パズル)

Remark

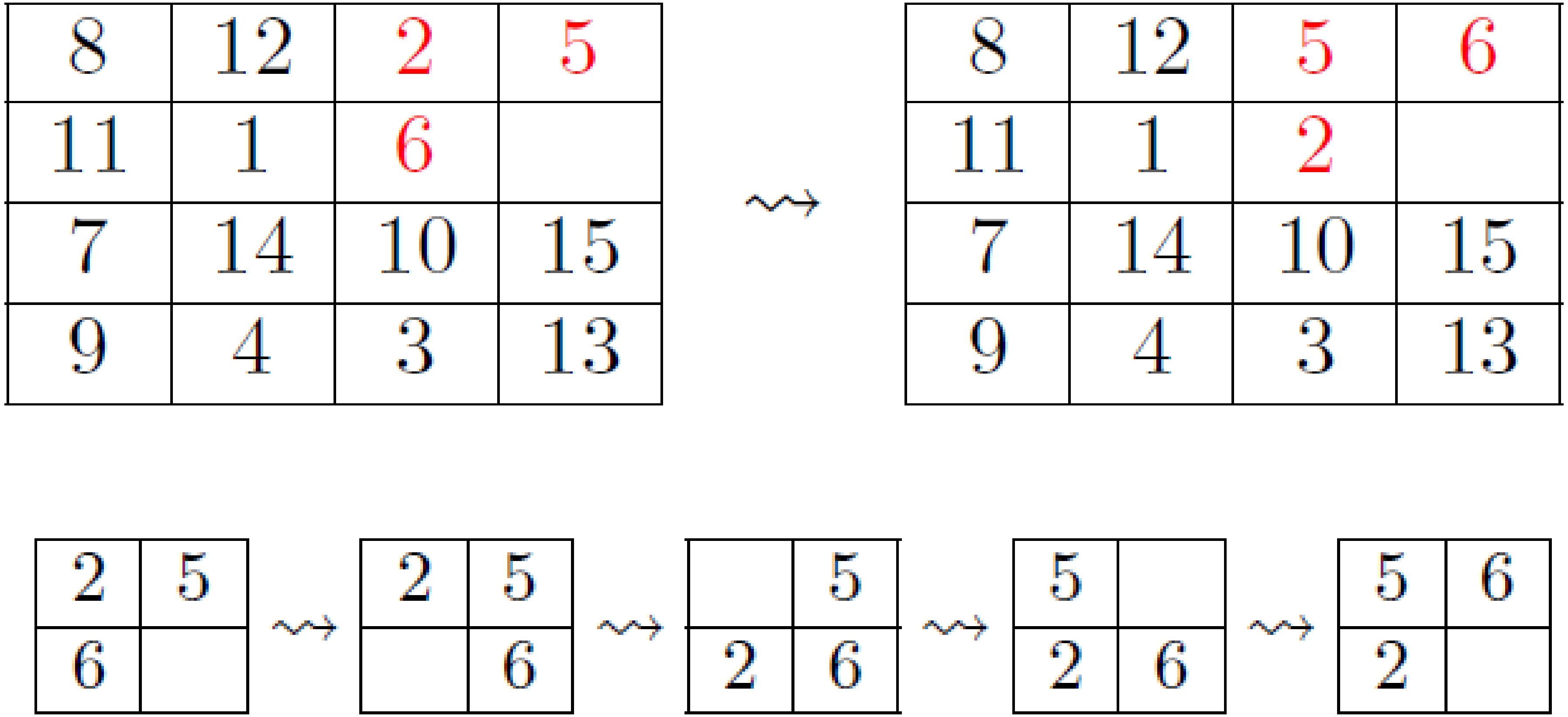
Any permutation can be written as either

(i) A product of an even number of transpositions or

(ii)A product of an odd number of transpositions.

*8.1 15-Puzzle (15パズル)

For example, the puzzle moves



8	12	2	5
11	1	6	
7	14	10	15
9	4	3	13

⇝

8	12	5	6
11	1	2	
7	14	10	15
9	4	3	13

2	5
6	

⇝

2	5
	6

⇝

	5
2	6

⇝

5	
2	6

⇝

5	6
2	

*8.1 15-Puzzle (15パズル)

Theorem 8.1

It is impossible to pass between standard configuration and question configuration (14 15) by sliding the pieces.

Proof:

Each basic move of the 15-puzzle involves an exchange of positions between piece 16 (the empty space) and an actual piece. If pieces in positions i and j are swapped and other pieces stay put, that move is described by the permutation $(i\ j)$ (no matter what pieces are in positions i and j).

The permutation for the *standard configuration* is the identity $e = (1)$ and the permutation for the *question configuration* is the transposition $\sigma = (14\ 15)$, so going from *standard configuration* to *question configuration* in the 15-puzzle means there are r times transpositions $\sigma_1, \sigma_2, \ldots, \sigma_r$ in S_{16}, then we can have

$$(14\ 15) = \sigma_r \cdots \sigma_2 \sigma_1$$

Because the empty space is in the same location in *standard configuration* and *question configuration*, after all the moves are carried out the empty space had to move up and down an equal number of times, and right and left an equal number of times. Since the empty space changes position by each σ_i, the number of transpositions on the right side of above equation is even. Therefore the right side of above equation is a product of an even number of transpositions, but the left side has an odd number of transpositions. This is a contradiction, so the theorem is proved.

*8.1 15-Puzzle (15パズル)

Corollary 8.1

Every movement of pieces in the 15-puzzle starting from the standard configuration that brings the empty space back to its original position must be an even permutation of the other 15 pieces.

*8.2 Introduction to Cryptography

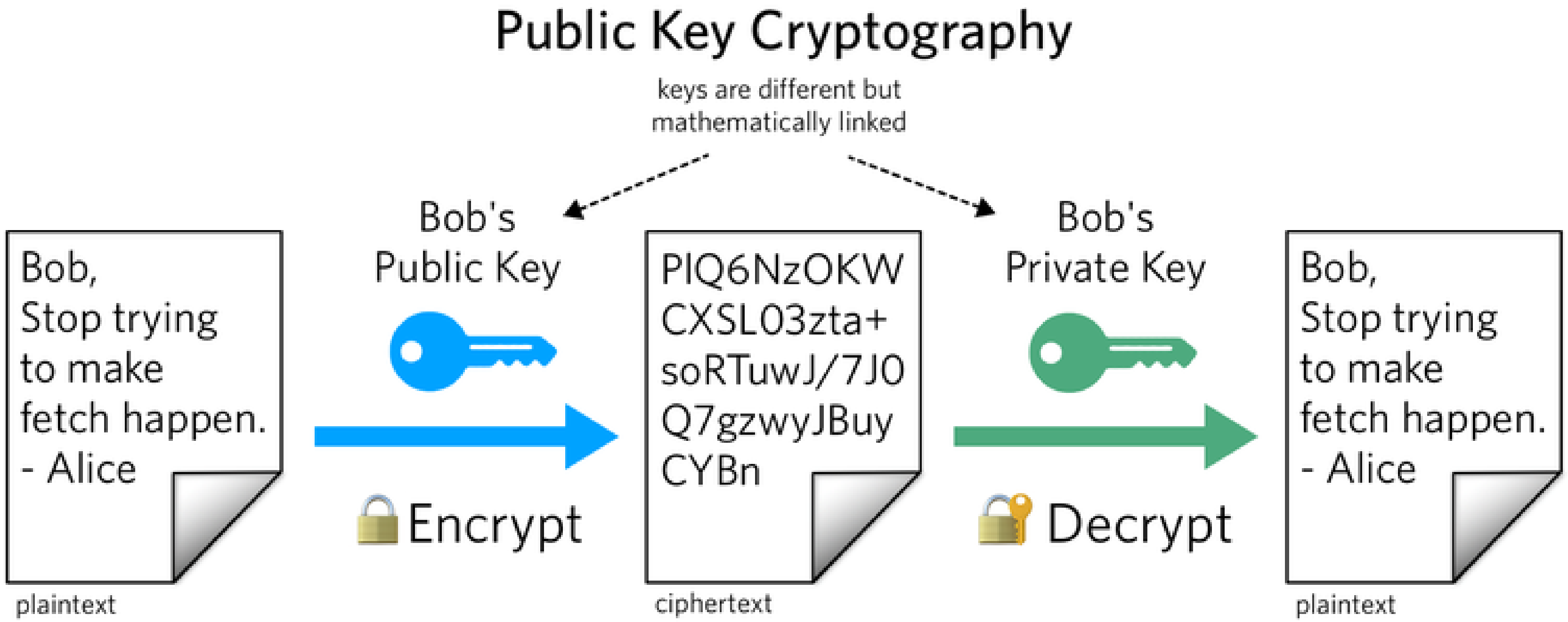
(暗号理論)

*8.2 Introduction to Cryptography (暗号理論)

Cryptography is the study of sending and receiving secret messages.

- The aim of cryptography is to send messages across a channel so that only the intended recipient (対象受信者) of the message can read it. In addition, when a message is received, the recipient usually requires some assurance that the message is authentic (本物の); that is, this message has not been sent by someone who is trying to deceive (欺く) the recipient.

Modern cryptography is heavily dependent on abstract algebra (抽象代数学) and number theory (数論).


Public Key Cryptography
keys are different but mathematically linked
Bob's Public Key
Bob's Private Key
Bob, Stop trying to make fetch happen. - Alice
plaintext
Encrypt
PIQ6NzOKW CXSL03zta+ soRTuwJ/7J0 Q7gzwyJBuy CYBn
ciphertext
Decrypt
Bob, Stop trying to make fetch happen. - Alice
plaintext

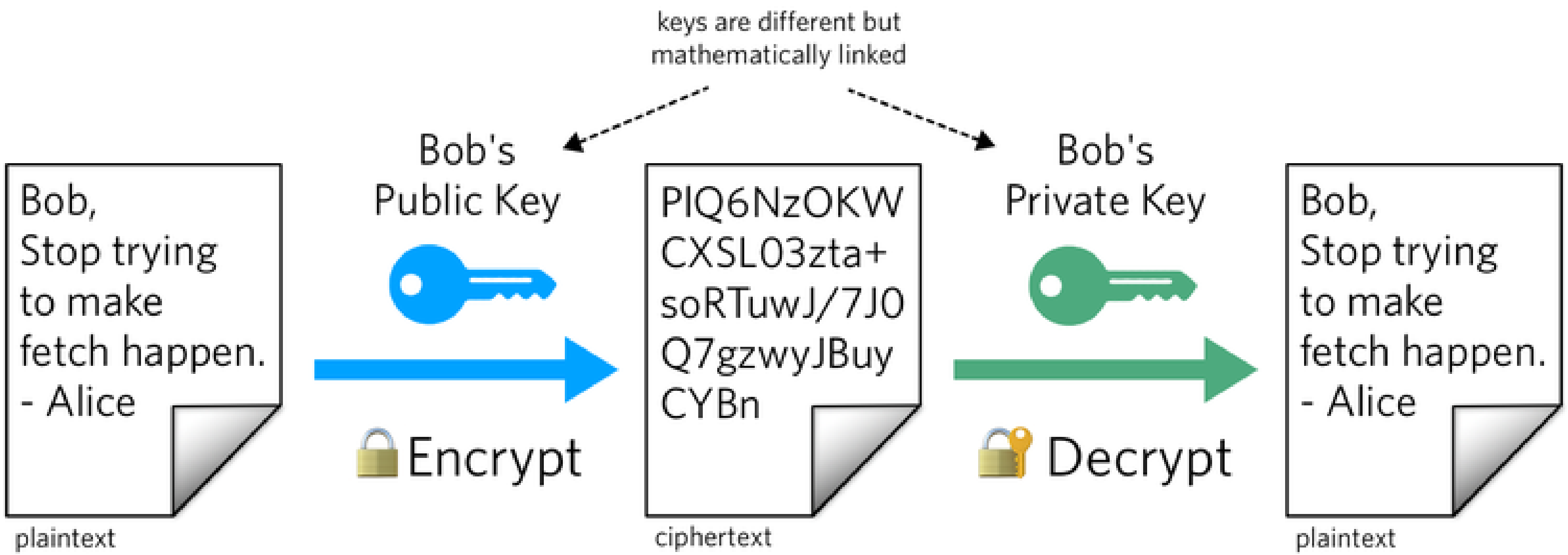
*8.2 Introduction to Cryptography (暗号理論)

- The message to be sent is called the plaintext (プレーンテキスト) message.
- The disguised message is called the ciphertext (暗号文).

The **plaintext** and the **ciphertext** are both written in an alphabet, consisting of letters or characters. Characters can include not only the familiar alphabetic characters $A, \dots, Z$ and $a, \dots, z$ but also digits, punctuation marks, and blanks.

A **cryptosystem (暗号システム)**, or **cipher**, has two parts:
(1)Encryption (暗号化), the process of **transforming a plaintext message to a ciphertext message** ;
(2)Decryption (復号化), the **reverse transformation of changing a ciphertext message into a plaintext message**.

Public Key Cryptography

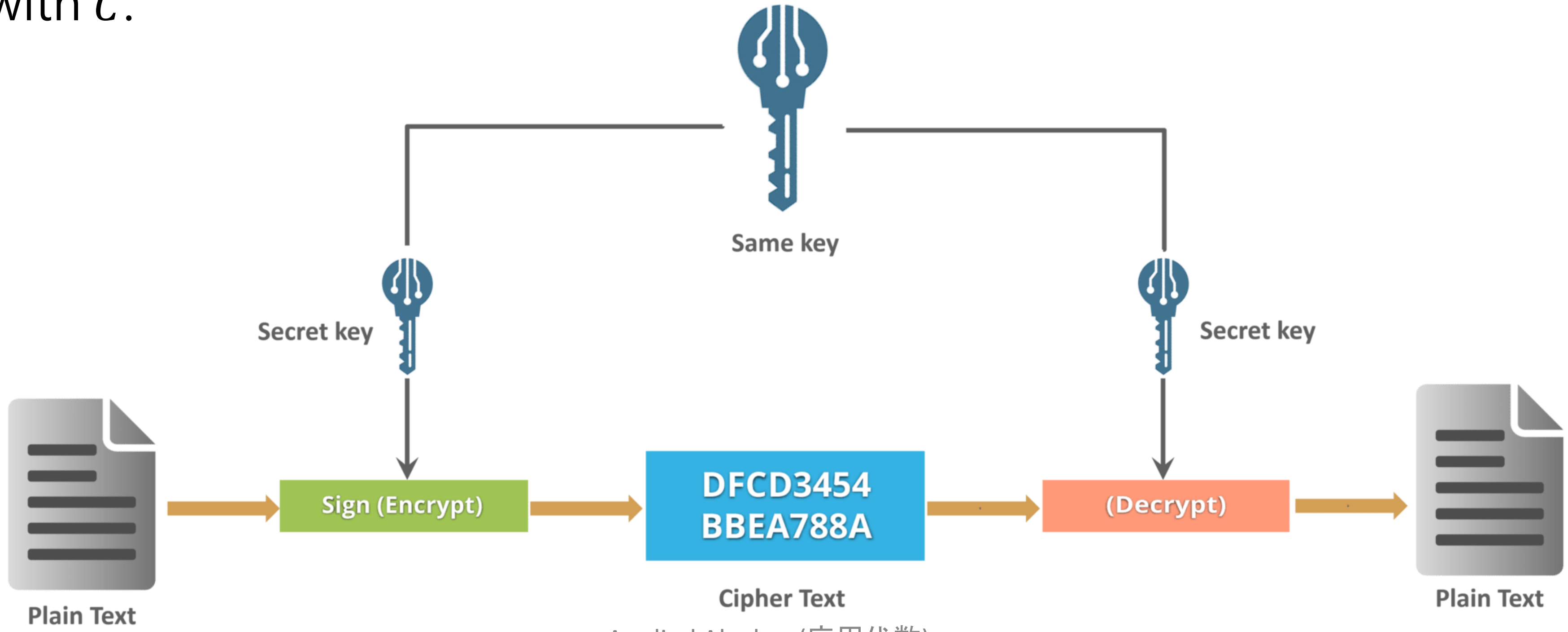


*8.2 Introduction to Cryptography (暗号理論)

Cryptosystems in a specified cryptographic family are distinguished from one another by a parameter to the encryption function called a **key (鍵)**.

(1) A ***Private Key Cryptosystem*** has a single key, which **must be kept secret**, known only to the sender and the receiver of the message (they share the **same single key**).

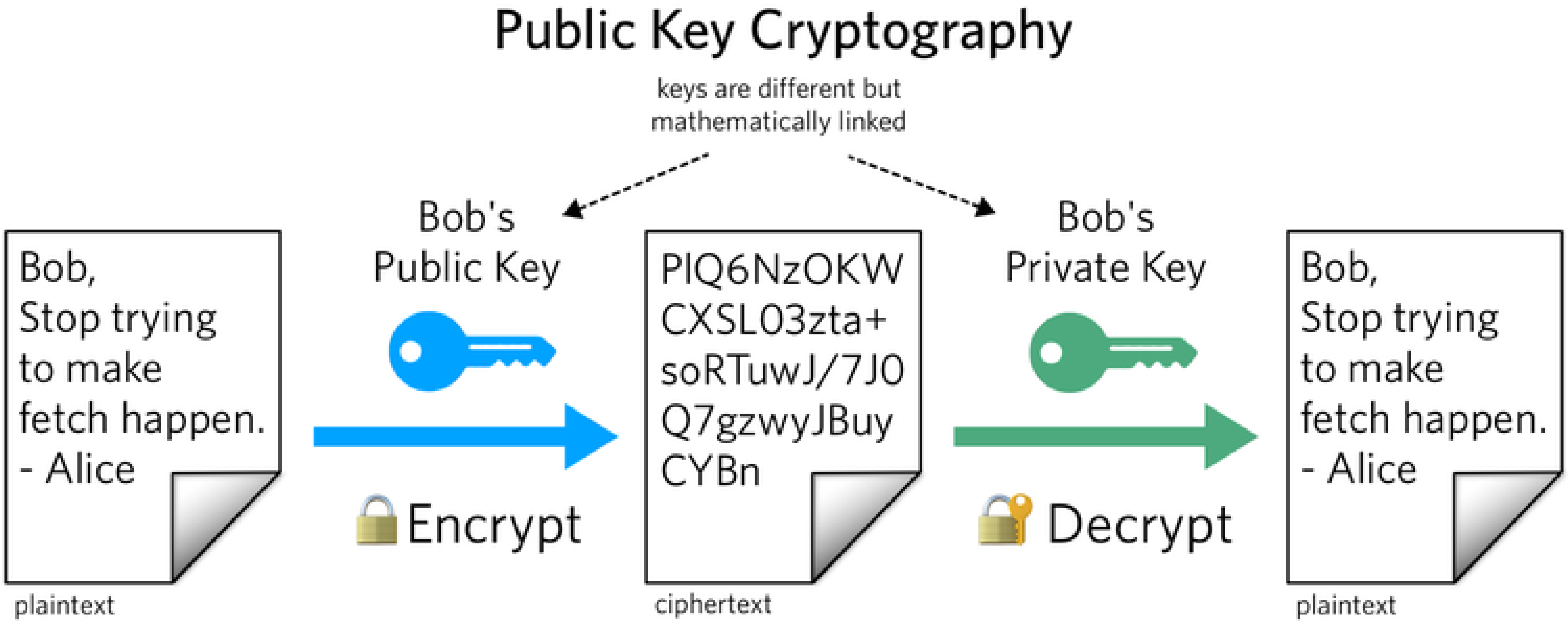
- If person A wishes to send secret messages to two different people B and C, and does not wish to have B understand C's messages or vice versa, A must use two separate keys, so one cryptosystem is used for exchanging messages with B, and another is used for exchanging messages with C.



*8.2 Introduction to Cryptography (暗号理論)

(2) The *Public Key Cryptosystem (公開鍵暗号系)* use **two separate keys**, **one for encoding** and **another for decoding**. Since knowledge of the encoding key does not allow anyone to guess at the decoding key, the encoding key can be made public.

- A **public key cryptosystem** allows A and B to send messages to C using the same encoding key. **Anyone is capable of encoding a message to be sent to C**, **but only C knows how to decode such a message**.



*8.2 Introduction to Cryptography (暗号理論)

8.2.1 Private Key Cryptography

In single or private key cryptosystems the same key is used for both encrypting and decrypting messages.

- To encrypt a plaintext message, we apply to the message some function which is kept secret, say f. This function will yield an encrypted message.
- Given the encrypted form of the message, we can recover the original message by applying the inverse transformation f^{-1}.

The transformation f must be relatively easy to compute, as must f^{-1}; however, f must be extremely difficult to guess from available examples of coded messages.

*8.2 Introduction to Cryptography (暗号理論)

8.2.1 Private Key Cryptography

Example 8.1. One of the first and most famous private key cryptosystems was the **shift code** used by Julius Caesar. We first digitize the 26-letter alphabet by letting $A = 00;\ B = 01, C = 02, \ldots, Z = 25$. The encoding function will be

$$f(x) \ = x + 3 \ (\mathrm{mod}\ 26);$$

that is, $A \rightarrow D; B \rightarrow E, \ldots, Z \rightarrow C$. Let encoded result $c = f(x)$, then the decoding function is then

$$f^{-1}(c) = c - 3 \ (\mathrm{mod}\ 26) \ = c \ + \ 23 \ (\mathrm{mod}\ 26)$$

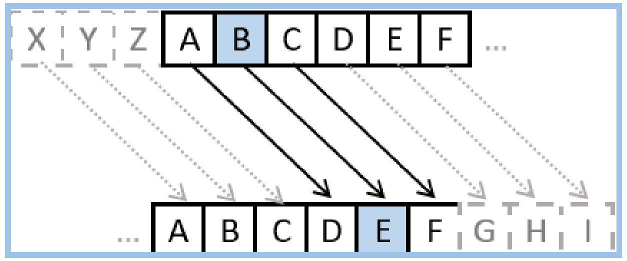
Suppose we receive the encoded message DOJHEUD. To decode this message, we first digitize it as:

$$3, 14, 9, 7, 4, 20, 3.$$

Next we apply the inverse transformation $f^{-1}(x)$ to get

$$0, 11, 6, 4, 1, 17, 0.$$

or ALGEBRA. Notice here that there is nothing special about either of the numbers 03 or 26. We could have used a larger alphabet or a different shift.



<u>Shift+3</u>

This cipher has a shift of 3 characters.

The letter “A” becomes “D”, The letter “B” becomes “E”.

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	Plaintext
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	Ciphertext

*8.2 Introduction to Cryptography (暗号理論)

8.2.1 Private Key Cryptography

- In fact, in a simple shift as described in Example 8.1, there are only 26 possible keys. **It would be quite easy to try them all rather than to use frequency analysis.**
- Simple shift codes are examples of **monoalphabetic cryptosystems**. In these ciphers a character in the enciphered message represents exactly one character in the original message. Such cryptosystems **are not very sophisticated and are quite easy to break.**
- Let us investigate **a slightly more sophisticated cryptosystem**. Suppose that the encoding function is given by

$$f(x) = ax + b \pmod{26}:$$

We first need to find out when a decoding function f^{-1} exists. Such a decoding function exists when we can solve the equation

$$c = ax + b \pmod{26}$$

for x, where c is the encoded result. This is possible exactly when a has an inverse or, equivalently, when $\gcd(a, 26) = 1$. In this case

$$x = f^{-1}(c) = a^{-1}c - a^{-1}b \pmod{26}$$

Such a cryptosystem is called an ***affine cryptosystem***.

*8.2 Introduction to Cryptography (暗号理論)

8.2.1 Private Key Cryptography

Example 8.2.

Let us consider the **affine cryptosystem** $f(x) = ax + b \pmod{26}$. For this cryptosystem to work we must choose an $a \in \mathbb{Z}_{26}$ that is invertible. This is only possible if $\gcd(a, 26) = 1$.

Recognizing this fact, we will let $a = 5$ since $\gcd(5,26) = 1$. It is easy to see that $a^{-1} = 21$. Therefore, we can take our encryption function to be

$$f(x) = 5x + 3 \pmod{26} = \mathrm{c}$$

Thus, ALGEBRA is encoded as $3,6,7,23,8,10,3$, or DGHXIKD. The decryption function will be

$$f^{-1}(c) = 21c - 21 \cdot 3 \pmod{26} = 21c + 15 \pmod{26}$$

*8.2 Introduction to Cryptography (暗号理論)

8.2.1 Private Key Cryptography

A cryptosystem would be more secure if a ciphertext letter could represent more than one plaintext letter. To give an example of this type of cryptosystem, called a *polyalphabetic cryptosystem*, we will generalize affine codes by using matrices. The idea works roughly the same as before; however, instead of encrypting one letter at a time we will encrypt pairs of letters. We can store a pair of letters x_1 and x_2 in a vector

$$\boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Let A be a 2×2 invertible matrix with entries in $\mathbb{Z}_{26}$. We can define an encoding function by

$$f(\boldsymbol{x}) = A\boldsymbol{x} + \boldsymbol{b}$$

where $\boldsymbol{b}$ is a fixed column vector and matrix operations are performed in $\mathbb{Z}_{26}$. The decoding function must be

$$f^{-1}(\boldsymbol{c}) = A^{-1}\boldsymbol{c} - A^{-1}\boldsymbol{b}$$

*8.2 Introduction to Cryptography (暗号理論)

8.2.1 Private Key Cryptography

Example 8.3.

Suppose that we wish to encode the word HELP. The corresponding digit string is $7, 4, 11, 15$. If

$$A = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$$

then

$$A^{-1} = \begin{pmatrix} 2 & 21 \\ 25 & 3 \end{pmatrix}$$

If $\boldsymbol{b} = \begin{bmatrix} 2 \\ 2 \end{bmatrix}$, then our message is encrypted as RRGR. The encrypted letter R represents more than one plaintext letter.

*8.2 Introduction to Cryptography (暗号理論)

8.2.2 Public Key Cryptography

- If traditional cryptosystems are used, anyone who knows enough to encode a message will **also know enough to decode** an intercepted message. This is not quite safe.
- In 1976, W. Diffie and M. Hellman proposed **public key cryptography**, which is based on the observation that the encryption and decryption procedures need not have the same key. **This removes the requirement that the encoding key be kept secret.**
- The encoding function f **must be relatively easy to compute**, but f^{-1} **must be extremely difficult to compute without some additional information**, so that someone who knows only the encrypting key cannot find the decrypting key without prohibitive computation.

*8.2 Introduction to Cryptography (暗号理論)

8.2.2 Public Key Cryptography

- The **RSA cryptosystem** introduced by R. Rivest, A. Shamir, and L. Adleman in 1978, is based on **the difficulty of factoring large numbers**. Though it is not a difficult task to find two large random primes and multiply them together, **factoring a 150-digit number that is the product of two large primes would take 100 million computers operating at 10 million instructions per second about 50 million years under the fastest algorithms available in the early 1990s**.
- Although the algorithms have improved, factoring a number that is a product of two large primes is still computationally prohibitive.

R. Rivest, A. Shamir, and L. Adleman

*8.2 Introduction to Cryptography (暗号理論)

8.2.2 Public Key Cryptography

The RSA cryptosystem works as follows.

Step 1 Key generation:

(1)Suppose that we choose two random **prime numbers** p and q.

(2)Next, we compute the product $n = pq$ and also compute $\phi(n) = (p-1)(q-1) = m$, where ϕ is the Euler ϕ-function (Euler's totient function counts the positive integers up to a given integer n that are relatively prime to n: https://en.wikipedia.org/wiki/Euler%27s_totient_function).

(3)Now we **start choosing random integers** E until we find one that is relatively prime to m; that is, we choose E satisfies $\gcd(E, m) = 1$. Using the **Euclidean algorithm** (computing the greatest common divisor (GCD) of two numbers: https://en.wikipedia.org/wiki/Euclidean_algorithm), we can find a number D such that $DE \equiv 1 \pmod{m}$, it implies that exists a k such that $DE = km + 1 = k\phi(n) + 1$.

Step 2 Key distribution: The numbers n and E are now known by the public.

*8.2 Introduction to Cryptography (暗号理論)

8.2.2 Public Key Cryptography

Step 3 Public-key encryption:

Suppose now that person B (Bob) wishes to send person A (Alice) a message x over a public line. Since E and n are known to everyone, **anyone can encode messages**. Bob first digitizes the message according to some scheme, say $A = 00, B = 01, \dots, Z = 25$. Suppose x is the message to send.

Bob can generate ciphertext by using $c = x^E \pmod{n}$ and sends c to Alice.

Step 4 Private-key decryption: Only Alice can recover plaintext by using $x = c^D \pmod{n}$ because only Alice knows D.

Complete Explanation of RSA: https://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://www.amsi.org.au/teacher_modules/pdfs/Maths_delivers/Encryption5.pdf (Step 4, page 23)

8.2.2 Public Key Cryptography

Example 8.4.
Before exploring the theory behind the RSA cryptosystem or attempting to use large integers, we will use some small integers just to see that the system does indeed work. Suppose that we wish to send some message, which when digitized is $x = 25$. Let $p = 23$ and $q = 29$. Then

$$n = pq = 667 \text{ and } \phi(n) = m = (p-1)(q-1) = 616$$

We can let $E = 487$, since $\gcd(616, 487) = 1$. The encoded message is computed to be

$$c = x^E \pmod n) = 25^{487} \pmod{667} = 169$$

Using the **Euclidean algorithm**, we determine that $191E = 1 + 151m$, then $D = 191$; therefore, the decrypting key is $(n, D) = (667{,}191)$. We can recover the original message by calculating

$$x = c^D (\text{mod } n) = 169^{191} \pmod{667} = 25$$

We can now ask how one would go about breaking the RSA cryptosystem. To find D given n and E, we need to factor n and solve for D by using the Euclidean algorithm. But it is extremely difficult for modern computer when n has large digits. Quantum computer is regarded to have the potential that can solve this problem with huge improvement of computation ability.

Review for Lecture 8

- Symmetric Group
- Transposition
- Odd/Even Permutation
- Private Key Cryptography
- Public Key Cryptography

Assignment

Please Check https://github.com/uoaworks/Applied-Algebra

References

[1] Thomas W. Judson etc. Abstract Algebra Theory and Applications, 2018
[2] D. S. Malik, John N. Mordeson, M.K. Sen, Introduction to Abstract Algebra, 2007
[3] **(おすすめ)** 松本 眞, 代数系への入門, http://www.math.sci.hiroshima-u.ac.jp/~m-mat/TEACH/daisu-nyumon2014.pdf
[4] Keith Conrad, The 15-Puzzle (and Rubik's Cube)
https://kconrad.math.uconn.edu/blurbs/grouptheory/15puzzle.pdf
[5] Michael Evans, A guide for teachers, RSA Encryption
http://www.amsi.org.au/teacher_modules/pdfs/Maths_delivers/Encryption5.pdf
[6] Wikipedia
[7] Materials from internet.