

# 110學年度新北市立中平國中 數學領域專書導讀

導讀者：張齡尹老師



# 2021 最常見的10個密碼

# 2021 最常見的十個密碼

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

~ ,	! 1	@ 2	# 3	\$ 4	% 5	^ 6	& 7	* 8	( 9	) 0	- _	+ =	← Backspace
Tab ⇄	Q	W	E	R	T	Y	U	I	O	P	{ [	} ]	 \ _
Caps Lock ⇧ A	A	S	D	F	G	H	J	K	L	:	" '	;	Enter ↵
Shift ⇧ ↑	Z	X	C	V	B	N	M	< ,	> .	? /	Shift ⇧ ↑		
Ctrl	Win Key	Alt							Alt	Win Key	Menu	Ctrl	



# 世界第一簡單密碼學



## 作者簡介

三谷 政昭 (Mitani Masaaki)

工學博士。

現為東京電機大學工學部資訊通訊工學科教授。

專業領域為數位訊號處理工學、通訊工學、教育工學。

佐藤 伸一 (Satou Shinichi)

出生於日本福島縣伊達市。1990年修畢東京電機大學研究所電氣工學碩士課程。

現為東京電機大學工學部資訊通訊工學科助手。

# 書 本 簡 介

網路為現代人帶來無限便利，「密碼」已然成為守護安全的利器。

但是關於密碼，我們了解多少？

本書將從密碼基礎知識至實際應用方法，分四章節層層剝開密碼的神秘面紗

---

密碼學  
基礎

共通金鑰  
加密系統

公開金鑰  
加密系統

實際的  
密碼應用

# 如果沒有密碼...

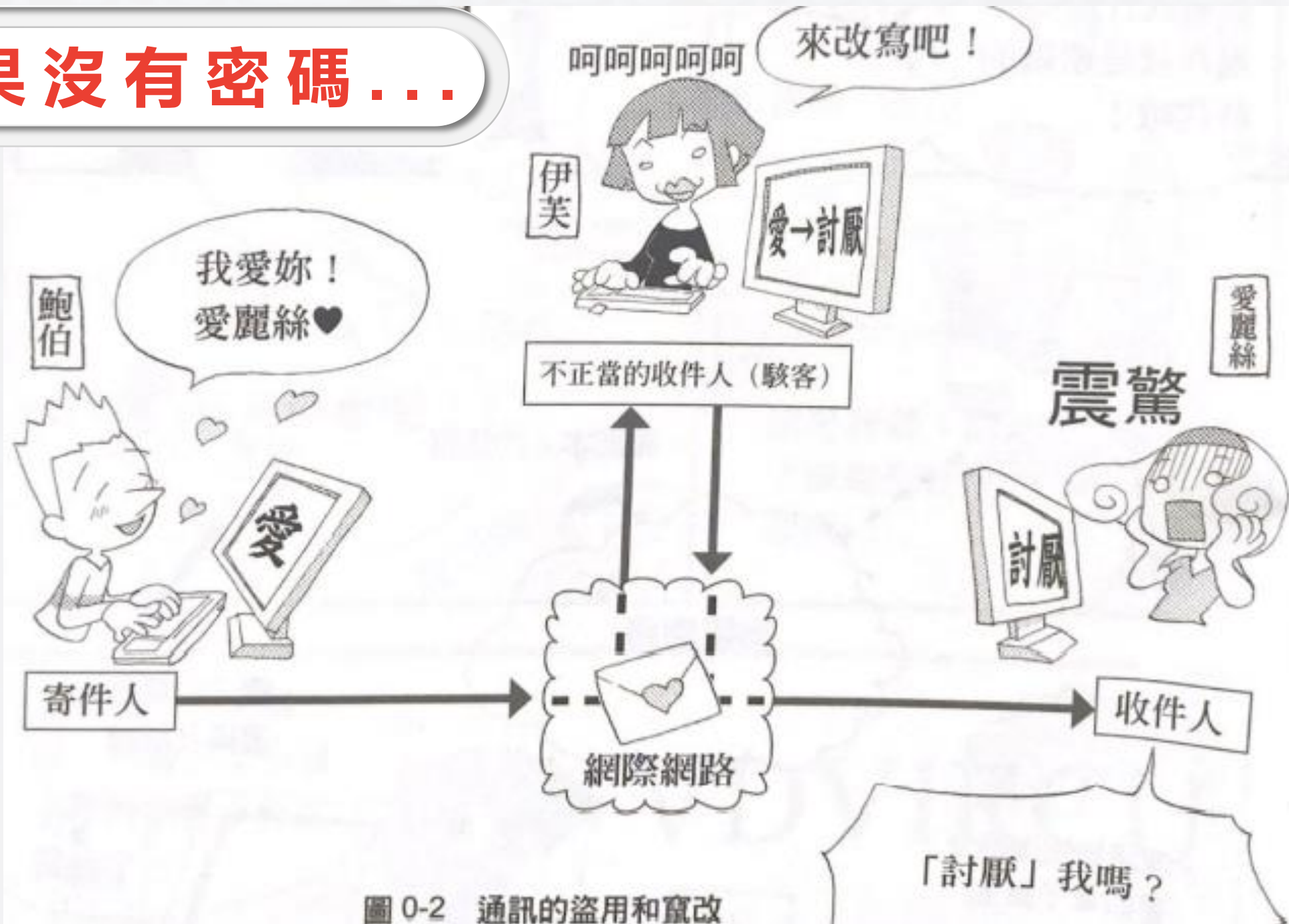
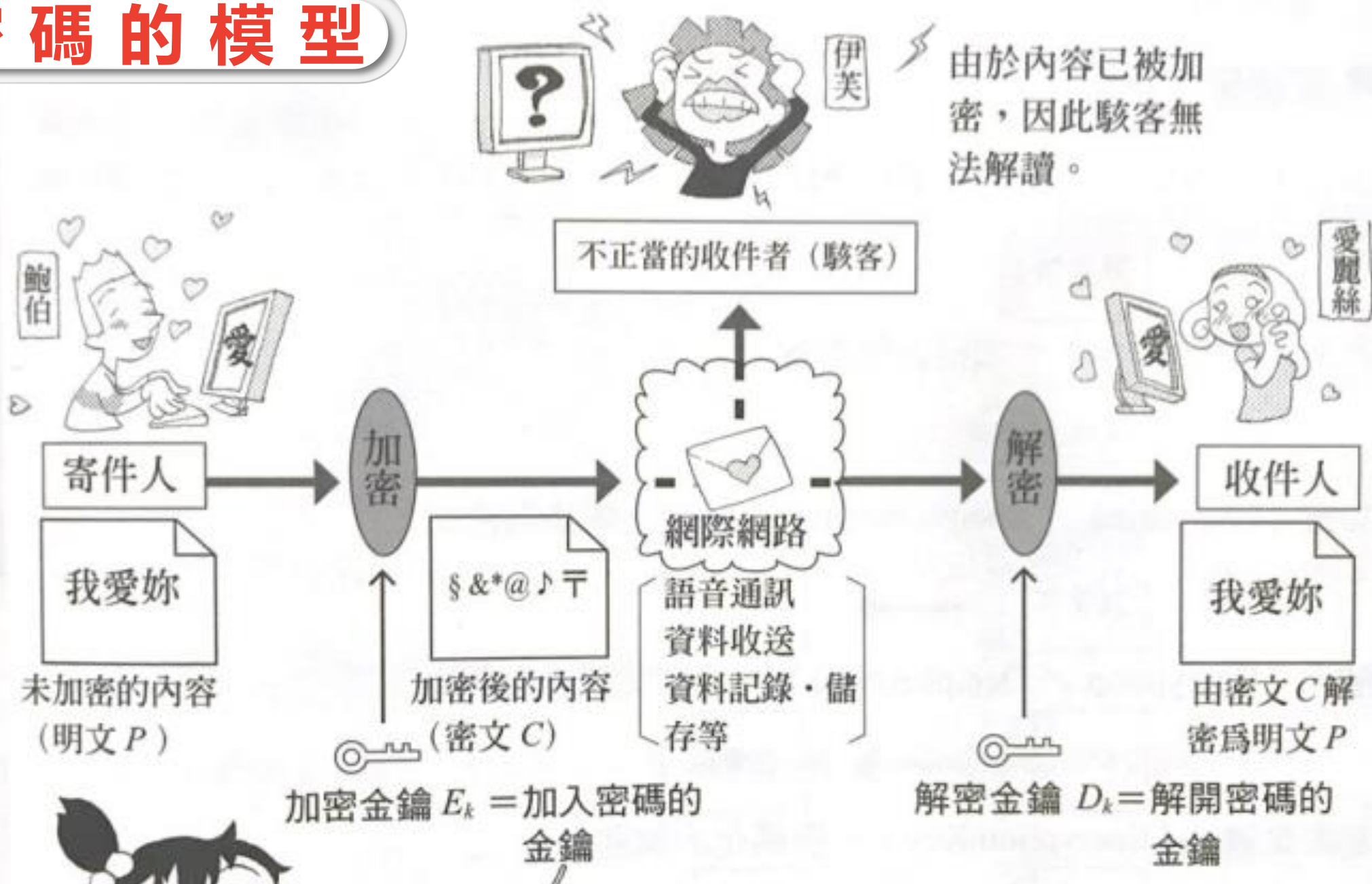


圖 0-2 通訊的盜用和竄改

# 密碼的模型



# 美術館畫作放置處....

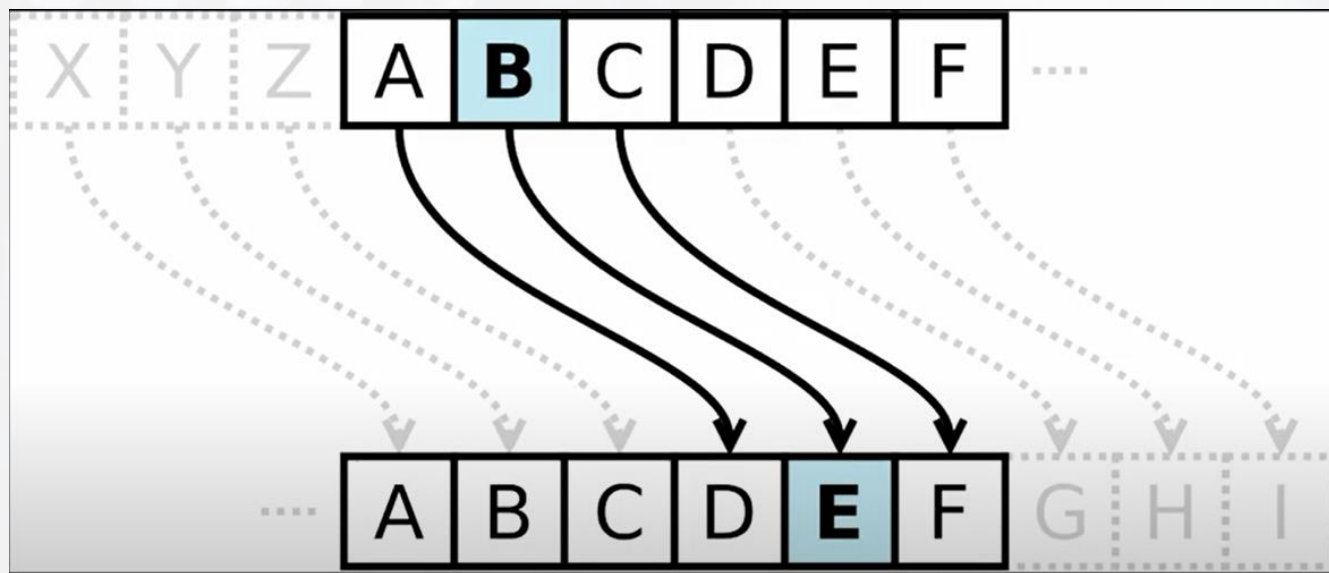
ㄇ ㄣ	ㄇ ㄣ	ㄇ	ㄋ
ㄣ	ㄣ	一	ㄣ
ㄇ	ㄣ	ㄣ	ㄇ
ㄣ	ㄣ	ㄣ	ㄣ



PASSWORD

古典密碼

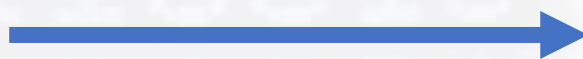
# 凱薩密碼



範

例

password



ufxxbtwi

PASSWORD

khoor

你好~



## 替代密碼

凱薩密碼的缺點被發現後，有人做出進階版  
將原文中的字母由另一個字母來取代，  
取代的順序不一定有一定的規則。  
加密與解密雙方必須共同擁有一份替換表，  
而此替換表便就是雙方共享『鑰匙』。

範

例

原字  
母：

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

替換字母

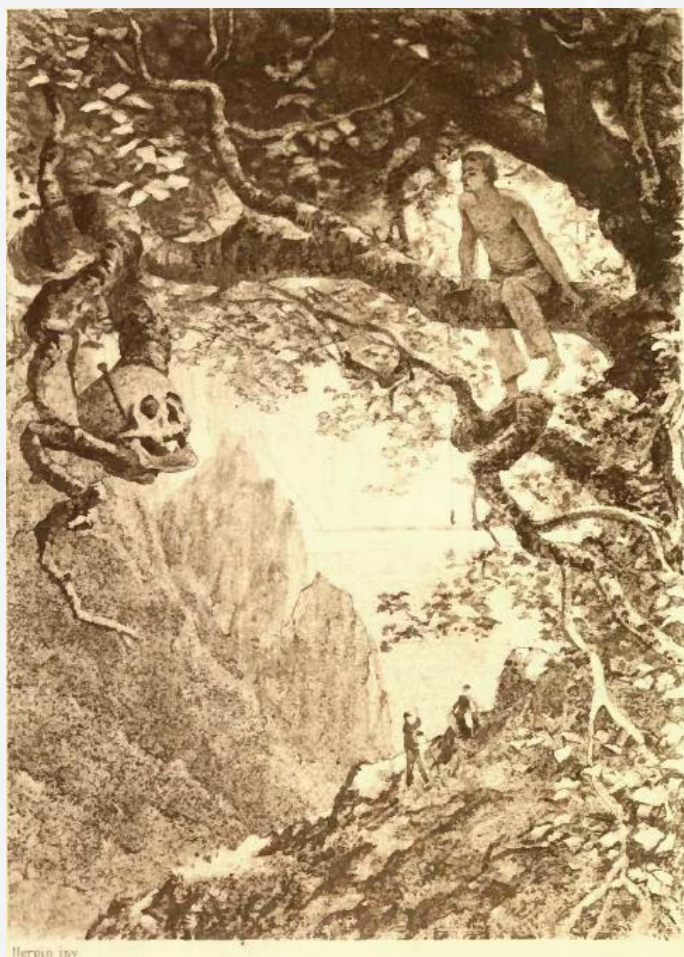
明文：I SIT BY MY WINDOW WAITING FOR YOU

密文：RHRGYBNBDRMWLDDZRGRMTULIBLF

PASSWORD

安全性

# 金 甲 蟲



密碼如下：

53‡‡‡305))6\*;4826)4‡.)4‡);806\*;48‡8  
¶60))85;1‡(;‡\*8‡83(88)5\*‡;46(;88\*96  
\*?;8)\*‡(;485);5\*‡2:\*‡(;4956\*2(5\*—4)8  
¶8\*;4069285);)6‡8)4‡‡;1(‡9;48081;8:8‡  
1;48‡85;4)485‡528806\*81(‡9;48;(88;4  
(‡?34;48)4‡;161;:188;‡?;

## 頻率分析

53†††305))6\*;4826)4†.)4†);806\*;48†8  
¶60))85;1†(;:†\*8†83(88)5\*†;46(;88\*96  
\*?;8)\*†(;485);5\*†2:\*†(;4956\*2(5\*—4)8  
¶8\*;4069285);)6†8)4††;1(†9;48081;8:8†  
1;48†85;4)485†528806\*81(†9;48;(88;4  
(†?34;48)4†;161;:188;†?;

# 安 全 性

可能被竊密的條件：

1. 知道加密的演算法
2. 文字出現的頻率型態(統計性)
3. 擁有大量的加密範本

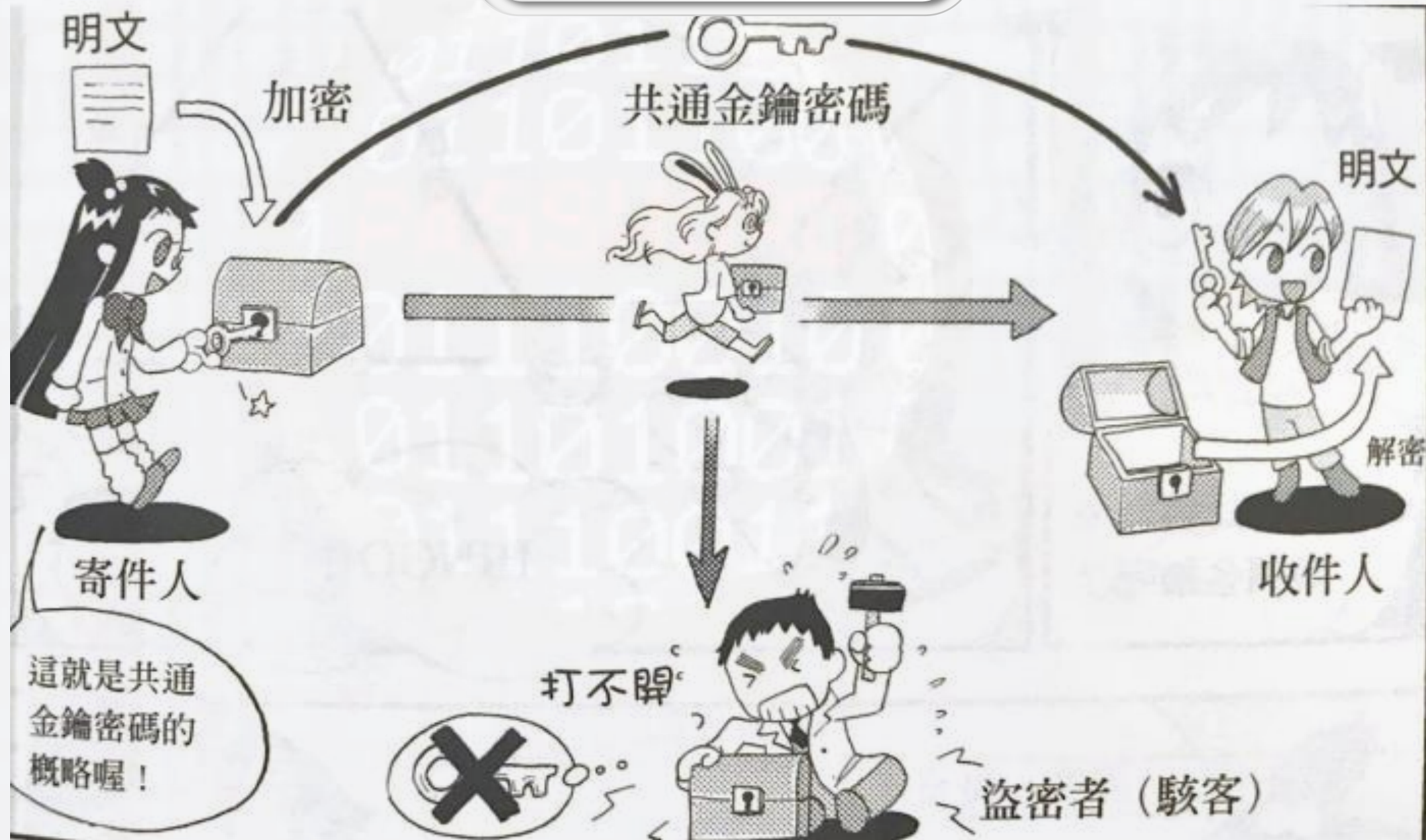
安全密碼：

1. 絕對安全的密碼(弗納姆密碼)
2. 計算量上的安全密碼(解讀需花費很多的時間，例如：現代的商用密碼)

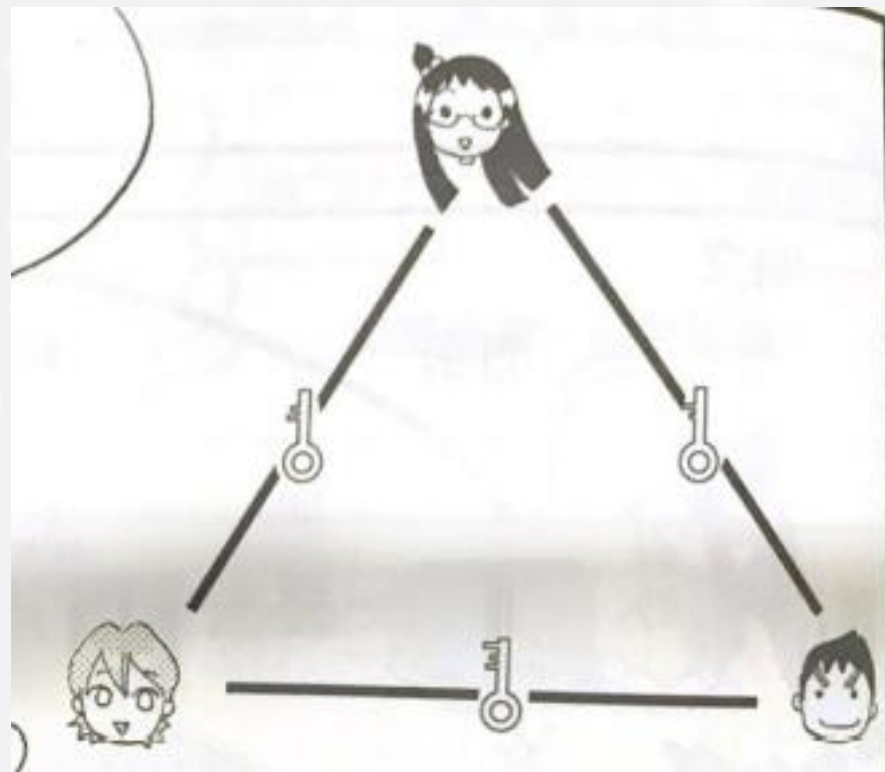
PASSWORD

# 加密系統

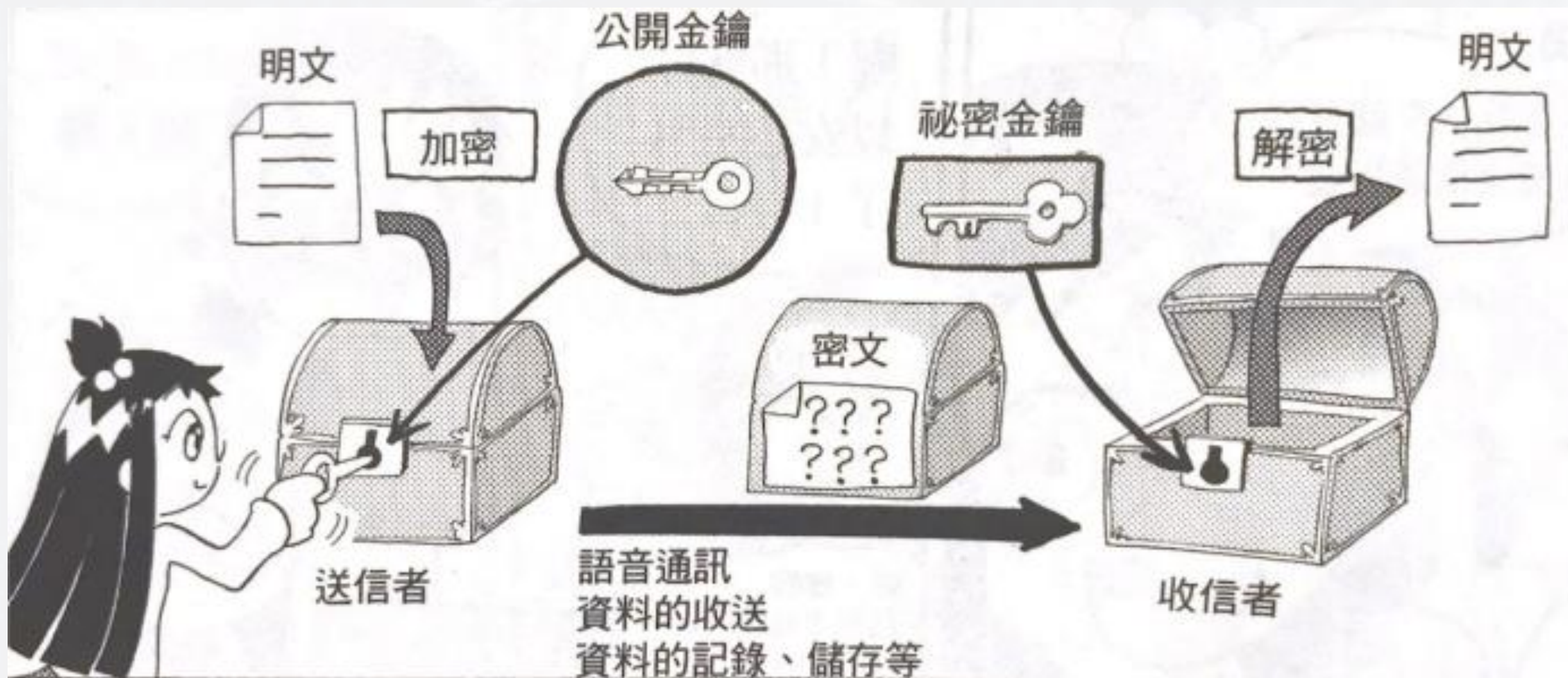
# 對稱金鑰



**若三個人以共通金鑰來通訊，  
大家覺得要幾個金鑰呢？**



# 非對稱金鑰



# 非對稱金鑰的加密方式

依加密技巧的種類不同，大致被區分為2種：

## 質因數分解 問題

- RSA密碼
- Rabin密碼

## 離散對數 問題

- ElGamal密碼
- 橢圓曲線密碼
- DSA認證

A magnifying glass is positioned over a background of binary code (0s and 1s). The word "PASSWORD" is written in a red, pixelated font and is the central focus of the magnifying glass. The background is a light blue-grey color with a subtle pattern of binary digits.

PASSWORD

結論

## 維吉尼亞密碼

維吉尼亞密碼（又譯維熱納爾密碼）  
是使用一系列凱撒密碼組成密碼字母  
表的加密算法，屬於多表密碼的一種  
簡單形式。

# 維吉尼亞密碼

例如：  
我們使用密鑰C，  
加密hello這個單詞，  
根據字母表的順序，  
hello加密後就為jgnnq。

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



eslyv jzf

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

ㄅ	ㄆ	ㄇ	ㄏ	ㄏ	ㄏ	ㄏ	ㄏ	ㄏ	ㄏ	ㄏ
2	3	5	7	11	13	17	19	23	29	31
ㄌ	ㄋ	ㄊ	ㄌ	ㄋ	ㄌ	ㄌ	ㄌ	ㄌ	ㄌ	ㄌ
37	41	43	47	53	59	61	67	71	73	79
ㄍ	ㄍ	ㄍ	ㄍ	ㄍ	ㄍ	ㄍ	ㄍ	ㄍ	ㄍ	ㄍ
83	89	97	101	103	107	109	113	127	131	137
ㄎ	ㄎ	ㄎ	ㄎ	一聲	二聲	三聲	四聲	輕聲		
139	149	151	157	163	167	173	179	181		



5

215  
395  
535  
895

215  
395  
535  
895

95  
395  
755  
835

65  
395  
755  
815