Encryption and codes
Lecture 11b: 2022-03-30

MAT A02 – Winter 2022 – UTSC

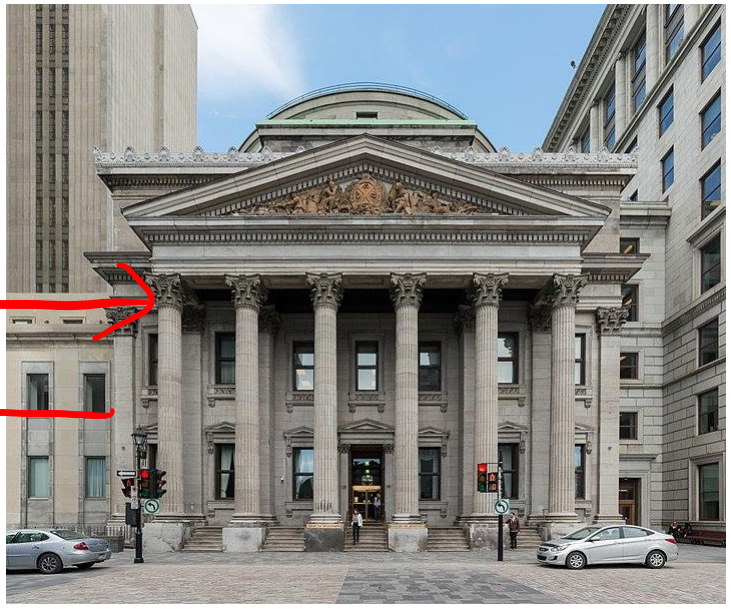
Prof. Yun William Yu

A Communications Story

B

A

(A)lice from Alice's Adventures in Wonderland
Illustration by Arthur Rackham, 1907



(B)ank of Montreal
https://commons.wikimedia.org/wiki/File:Bank_of_Montreal_Head_Office,_Montr%C3%A9al,_Southeast_view_20170410_1.jpg

(E)ve by Lucas Cranach the Elder (1528)

Eaves dropper

Encoding letters as decimal numbers

- Simple encoding is to just look at position in alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

- Computers use more complicated ASCII

0	NUL	16	DLE	32	SPACE	48	0	64	@	80	P	96	`	112	p
1	SOH	17	DC1	33	!	49	1	65	A	81	Q	97	a	113	q
2	STX	18	DC2	34	"	50	2	66	B	82	R	98	b	114	r
3	ETX	19	DC3	35	#	51	3	67	C	83	S	99	c	115	s
4	EOT	20	DC4	36	$	52	4	68	D	84	T	100	d	116	t
5	ENQ	21	NAK	37	%	53	5	69	E	85	U	101	e	117	u
6	ACK	22	SYN	38	&	54	6	70	F	86	V	102	f	118	v
7	BEL	23	ETB	39	'	55	7	71	G	87	W	103	g	119	w
8	BS	24	CAN	40	(	56	8	72	H	88	X	104	h	120	x
9	TAB	25	EM	41	)	57	9	73	I	89	Y	105	i	121	y
10	LF	26	SUB	42	*	58	:	74	J	90	Z	106	j	122	z
11	VT	27	ESC	43	+	59	;	75	K	91	[	107	k	123	{
12	FF	28	FS	44	,	60	<	76	L	92	\	108	l	124	|
13	CR	29	GS	45	-	61	=	77	M	93	]	109	m	125	}
14	SO	30	RS	46	.	62	>	78	N	94	^	110	n	126	~
15	SI	31	US	47	/	63	?	79	O	95	_	111	o	127	DEL

Try it out

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

- Match each of the following phrases:
  - 25 15 21 18 5 1 12 9 1 18 15 14 5
    YOUREALIARONE
  - 14 21 13 2 12 9 20 20 12 5 2 21 7
    NUMBLITTLEBUG
  - 14 5 22 5 18 7 15 14 14 1 7 9 22
    NEVERGONNAGIV

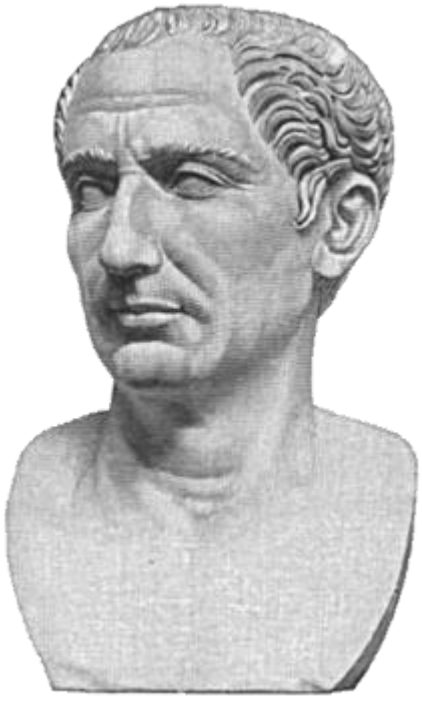
B

C

A

Caesar Cipher – mod 26 addition

- One simple cipher is to add in mod 26 arithmetic, or equivalently, shift all letters by the same amount.



Ex. $A \to D$ $\quad 1 \to 1+3 \equiv 4 \mod 26$

$B \to E$ $\quad 2 \to 2+3 \equiv 5 \mod 26$

$\vdots$

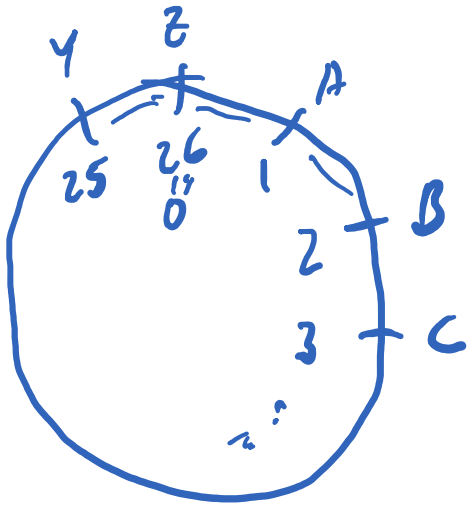
$Y \to B$ $\quad 25 \to 25+3 \equiv 28 \equiv 2 \mod 26$

$Z \to C$ $\quad 26 \equiv 0 \to 0+3 \equiv 3 \mod 26$

Gaius Julius Caesar

Caesar shift 3

key



Try it out

9 1 13 20 8 5 → 19, 11, 23, 36≡4, 18, 15 → S K W D R O

- Encrypt: “I AM THE VERY MODEL OF A MODERN MAJOR GENERAL” using Caesar cipher with shift 10.

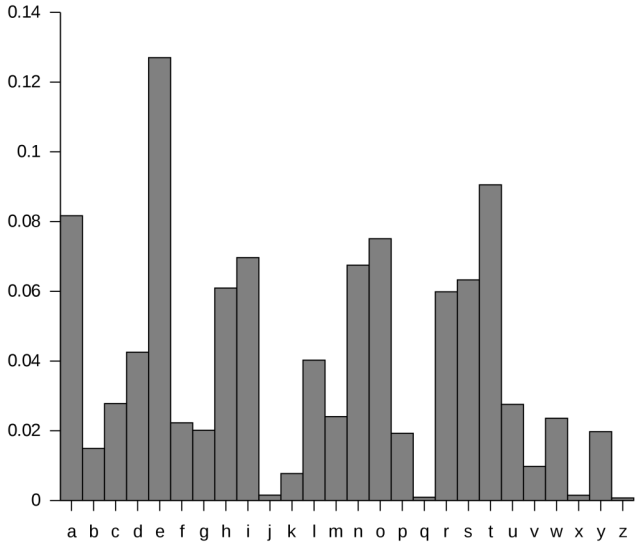
A: VNZGURIRELZBQRYBSNZBQREAZNWBETRARENY
B: SKWDROFOBIWYNOVYPKWYNOBXWKTYBQOXOBKV
C: ZRDKYVMVIPDFUVCFWRDFUVIEDRAFIXVEVIRC
D: IAMTHEVERYMODELOFAMODERNMAJORGENERAL
E: None of the above

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Decrypting simple Caesar shift

- How would we decrypt?
  SDGKCDROLOCDYPDSWOCSDGKCDROGYBCDYPDSWOC
- Could brute force all possibilities.
- Or can make use of common letters (RSTLNE).



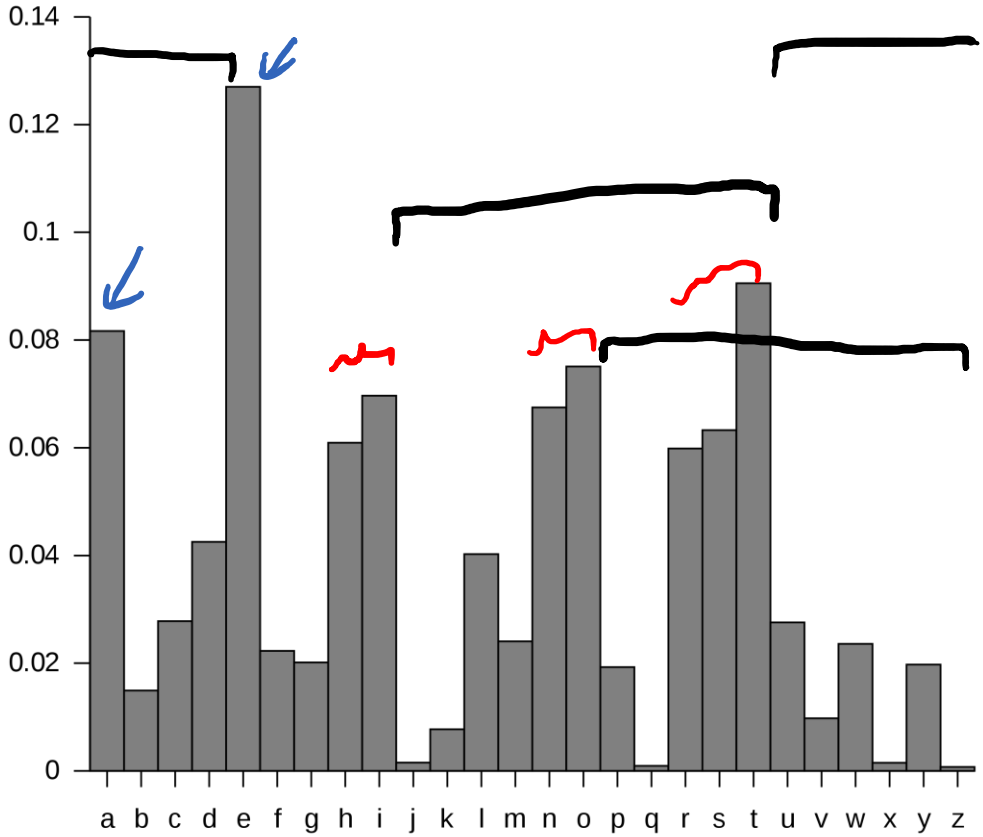
Code-breaking using frequencies

T ST E EST T ES T ST E ST T ES

- SDGKCDROLOCDYPDSWOCSDGKCDROGYBCDYPDSWOC
- D: 8
- C: 6

} 2 common letters next to each other

- O: 5 ← isolated common letter
- S: 4
- G: 3
- Y: 3
- K: 2
- R: 2
- P: 2
- W: 2
- L: 1
- B: 1



C, D = 3, 4

O = 15

} separation about 11-12

Guess O → E, C, D, → S, T

shift 10/16

- ITWASTHEBESTOFTIMESITWASTHEWORSTOFTIMES

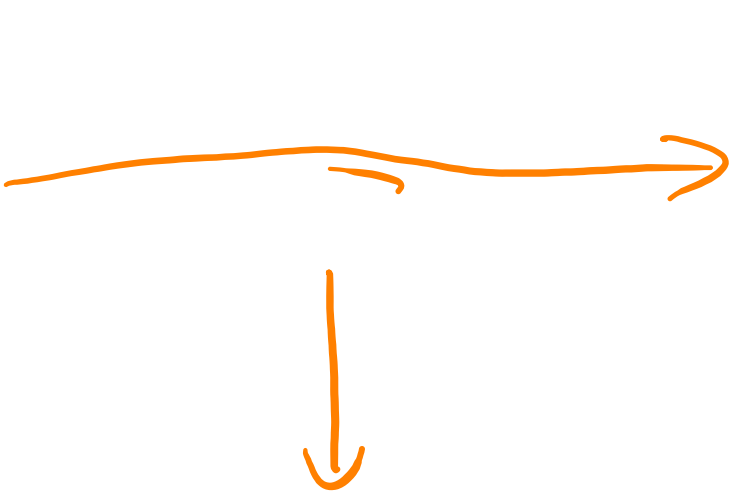
In-class exercise

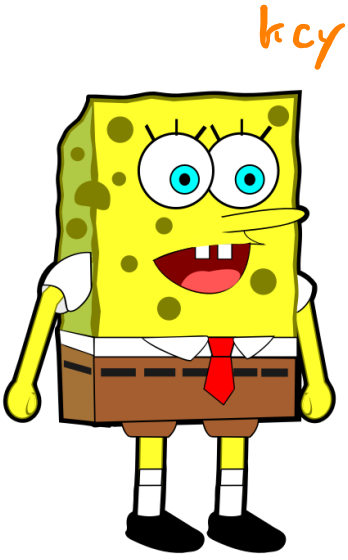
>100 characters

- Break up into clusters of 10 students.
- Split each cluster into two groups of about 5 people.
- Each group will write *two* messages encrypted with Caesar ciphers using *different* shifts.
- They will give the other group both encrypted messages, but only tell them the key to one of them.
- The goal is to then decrypt both messages.
- Whichever group decrypts both messages first gets a mango gummy prize?

Exercise modelling communication

- When you are sending a message, you are playing the role of Alice.
- When you are decrypting a message with a key, you are Bob.
- When you are decrypting a message without a key, you are Eve.





Vigenère Cipher

- The weakness of the Caesar cipher is twofold:
  - There are only 26 possible keys.
  - You can do a frequency analysis on letters.
- Another cipher invented in the 1500s by Blaise de Vigenère fixes both these problems and uses a longer key.
- Instead of using a single shift letter as a key we use an entire phrase, like “MAGIC”, repeat that phrase, and then add it using modular arithmetic to the message.

Vigenère Example

- TOBEORNOTTOBETHATISTHEQUESTION
- MAGICMAGICMAGICMAGICMAGICMAGIC

Encoded message:

20 15 02 05 15 18 14 15 20 20 15 02 05 20 08 01 20 09 19 20 08 05 17 21 05 19 20 09 15 14

Repeated key:

13 01 07 09 03 13 01 07 09 03 13 01 07 09 03 13 01 07 09 03 13 01 07 09 03 13 01 07 09 03

Summed mod 26:

07 16 09 14 18 05 15 22 03 23 02 03 12 03 11 14 21 16 02 23 21 06 24 04 08 06 21 16 24 17

- GPINREOVCWBCLCKNUPBWUFXDHFUPXQ

frequencies no longer match English

decryption is just subtract

In-class exercise

- Break up into clusters of 10 students.
- Split each cluster into two groups of about 5 people.
- Each group will write *two* messages encrypted with Vigenère ciphers using *different* keys.
- They will give the other group both encrypted messages, but only tell them the key to one of them.
- The goal is to then decrypt both messages.
- Whichever group decrypts both messages first gets a mango gummy prize?

Safely communicating secrets

- If Alice and Bob have a shared secret key, they can communicate reasonably securely. Sometimes, Eve can crack the code, but modern codes are thought to be extremely hard to crack.
- But that relies on having a way to communicate the secret key to begin with.

https://ndla.no/subject:1:b40855bb-9e21-4944-9257-c96679da549a/topic:2:108941/resource:1:109074

- Is it possible to securely communicate when Eve can intercept any keys you might send?