

Grade School

Crypto

Part 1

Dr. Rick Smith, Cryptosmith

October, 2013

What We'll Learn About

- ◆ Substitution ciphers, especially the Caesar Ciphers
- ◆ Algorithms and Keys
- ◆ Cipher Disks
- ◆ Cracking a cipher key using letter frequencies

Alice



Bob





Eve





perhaps have

the meaning

of text



Zfmebop efab
qeb jbxkfk
lc qbuq

The "Add One" Cipher

A COLD

A COLD

B

A COLD

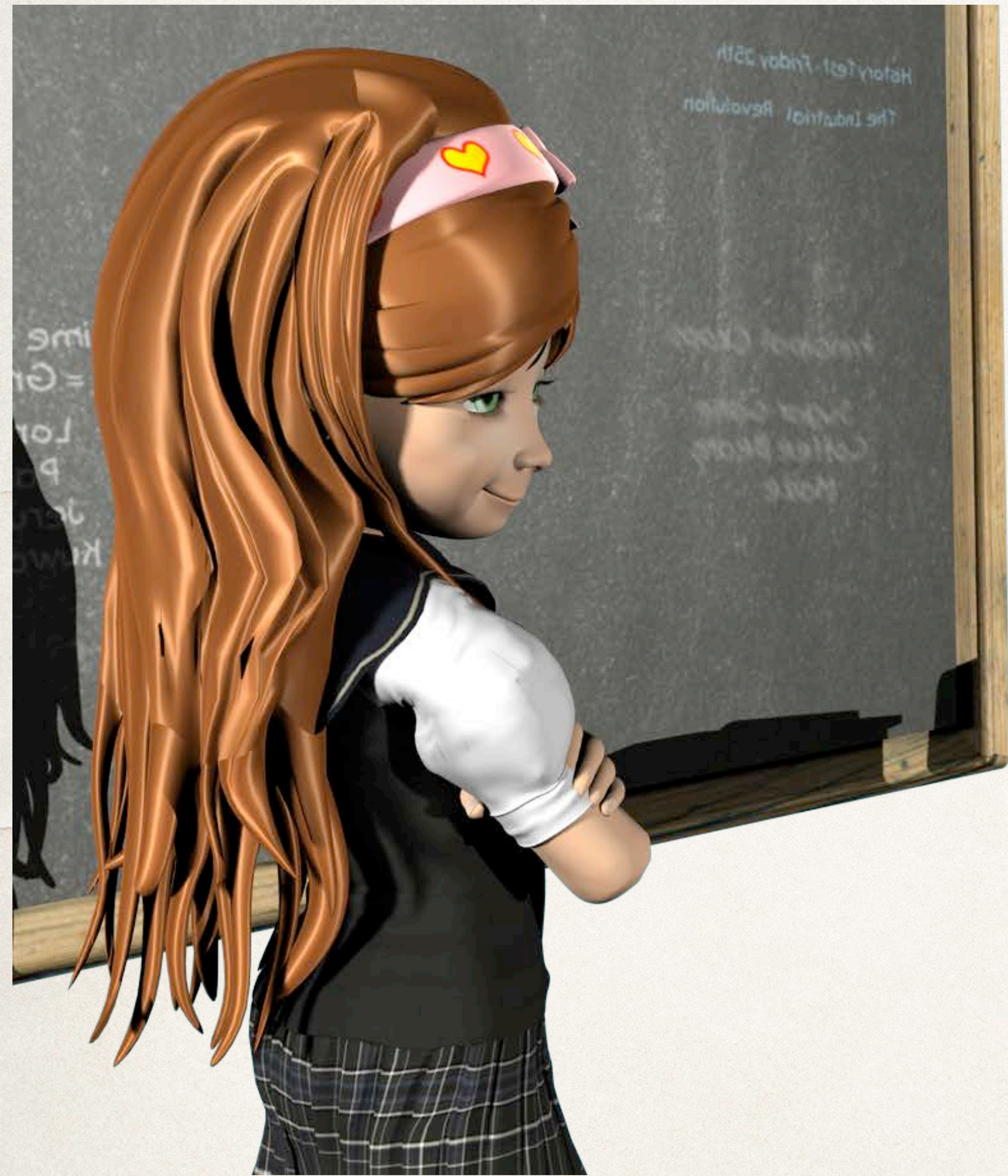
B D P M E



В ДЕМЕ

B D PME





B D P M E

A D P M E

B D P M E

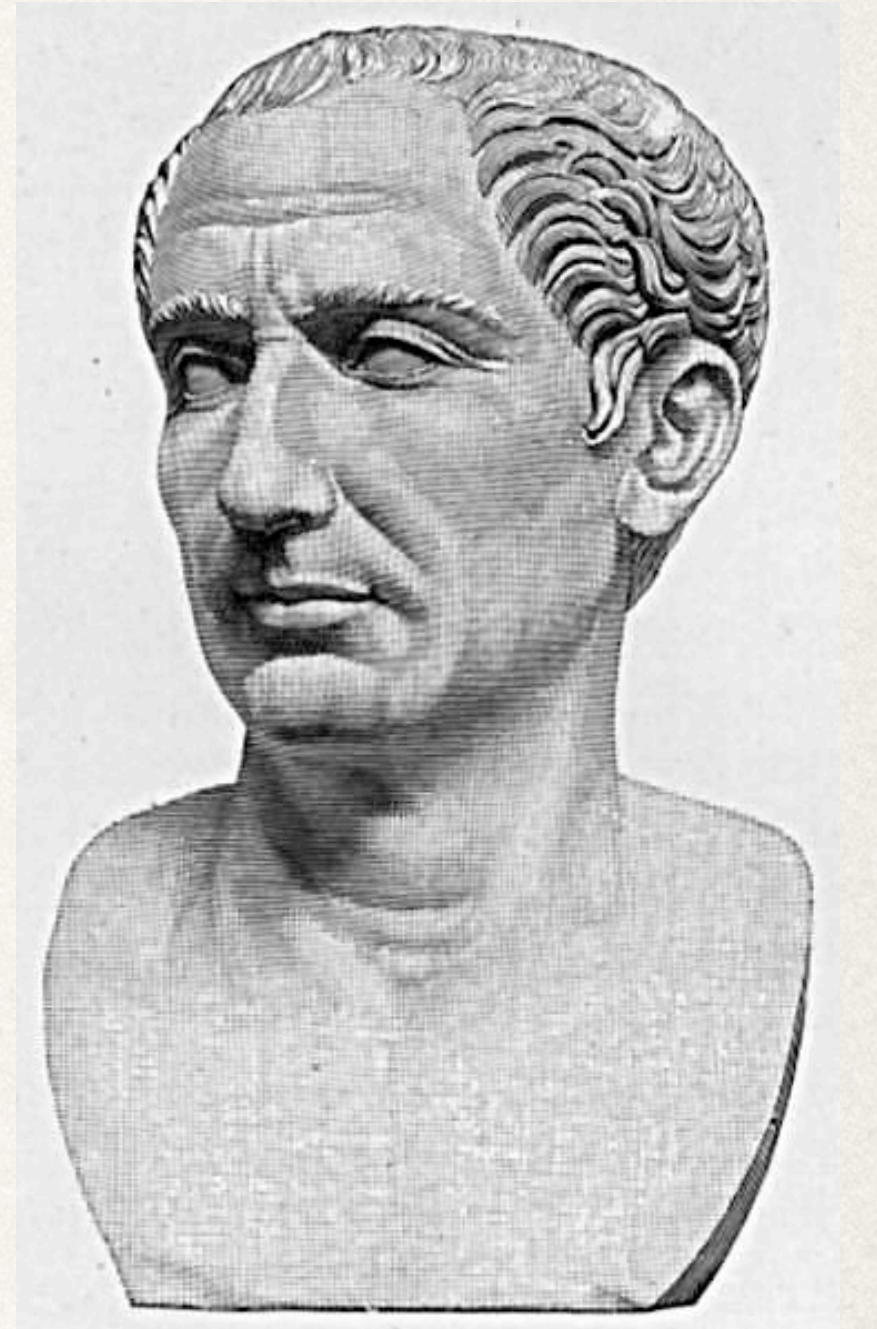
A C O L D



BOB HAS
A COLD

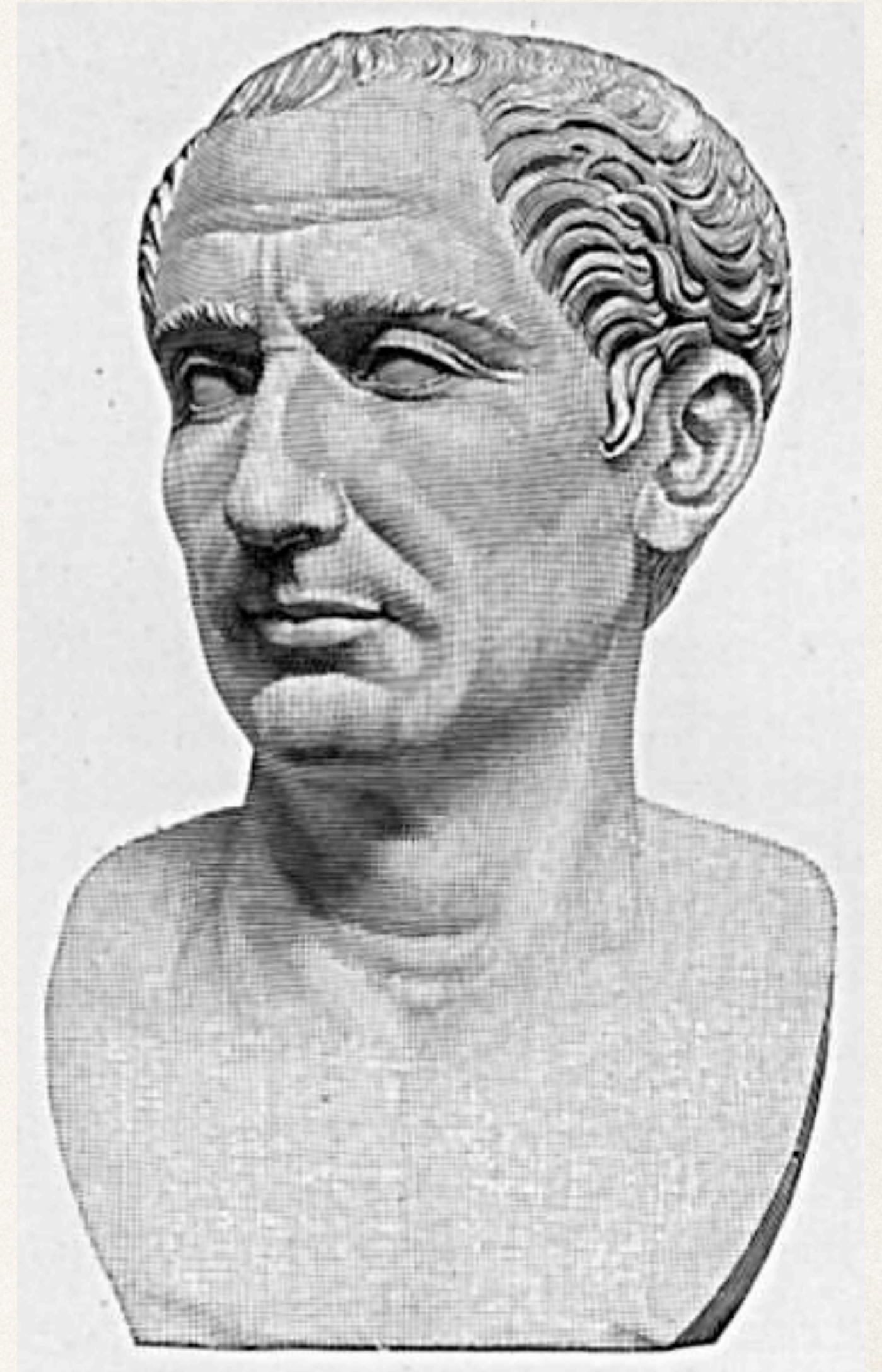
B DPME

The "Caesar" Cipher



Source: H. F. Helmolt (ed.): *History of the World*. New York, 1902.
Provided by Wikipedia.

Roman historians
recorded that Caesar
used this cipher to
protect messages of
military significance



Source: H. F. Helmolt (ed.): *History of the World*. New York, 1902.
Provided by Wikipedia.

The "Add Three" Cipher

A BREEZE

A BREEZE



A BREEZE

D EUGH

A BREEZE

D E U H H ? ?

What letter comes after Z?

No problem.
We just start the
alphabet over.

A BREEZE

D EUGHCH



Shifting
is the
Key

A ERDG





“Our Cipher”

To encrypt, we shift the
alphabet by 3

Modern Ciphers have Two Parts

- **ALGORITHM:** A Scrambling / Descrambling Rule
 - For Alice and Bob: shifting the alphabet
- **KEY:** A shared secret
 - For Alice and Bob: the amount of the shift
 - Agree on a specific value!

A Cipher Disk



History

These cipher disks were used during the American Civil War 1861-1865



Confederate Army

Reproduction based on a Confederate cipher disk shown in *The Codebreakers*, (David Kahn, Scribners, 1996)



Union Army

From the Gettysburg Battlefield Museum,
U.S. National Park Service

A Cipher Disk



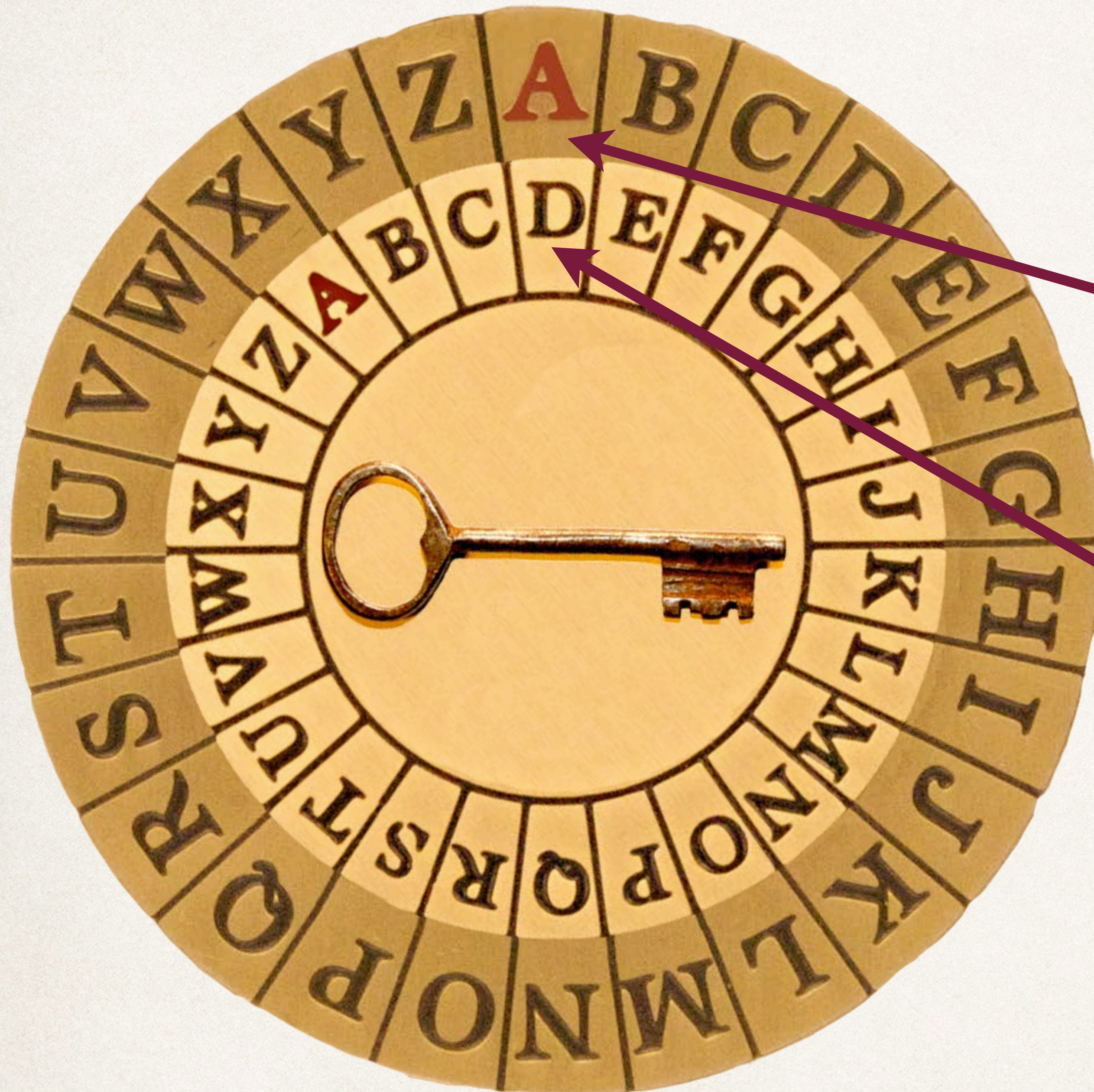
Shift 1 letter for the
“Add One” cipher

A Cipher Disk



Shift 3 letters for the
“Caesar” cipher

A Cipher Disk



Plain text on
the outside

Cipher text on
the inside

A Cipher Disk



The disk provides
the algorithm

The shift provides
the key

A Cipher Disk



A
“Substitution”
Cipher

Letters as
Numbers

Our Cipher Algorithm

$$P + S = C$$



Our Cipher Algorithm

$$P + S = C$$

$$A = 1, B = 2, C = 3$$

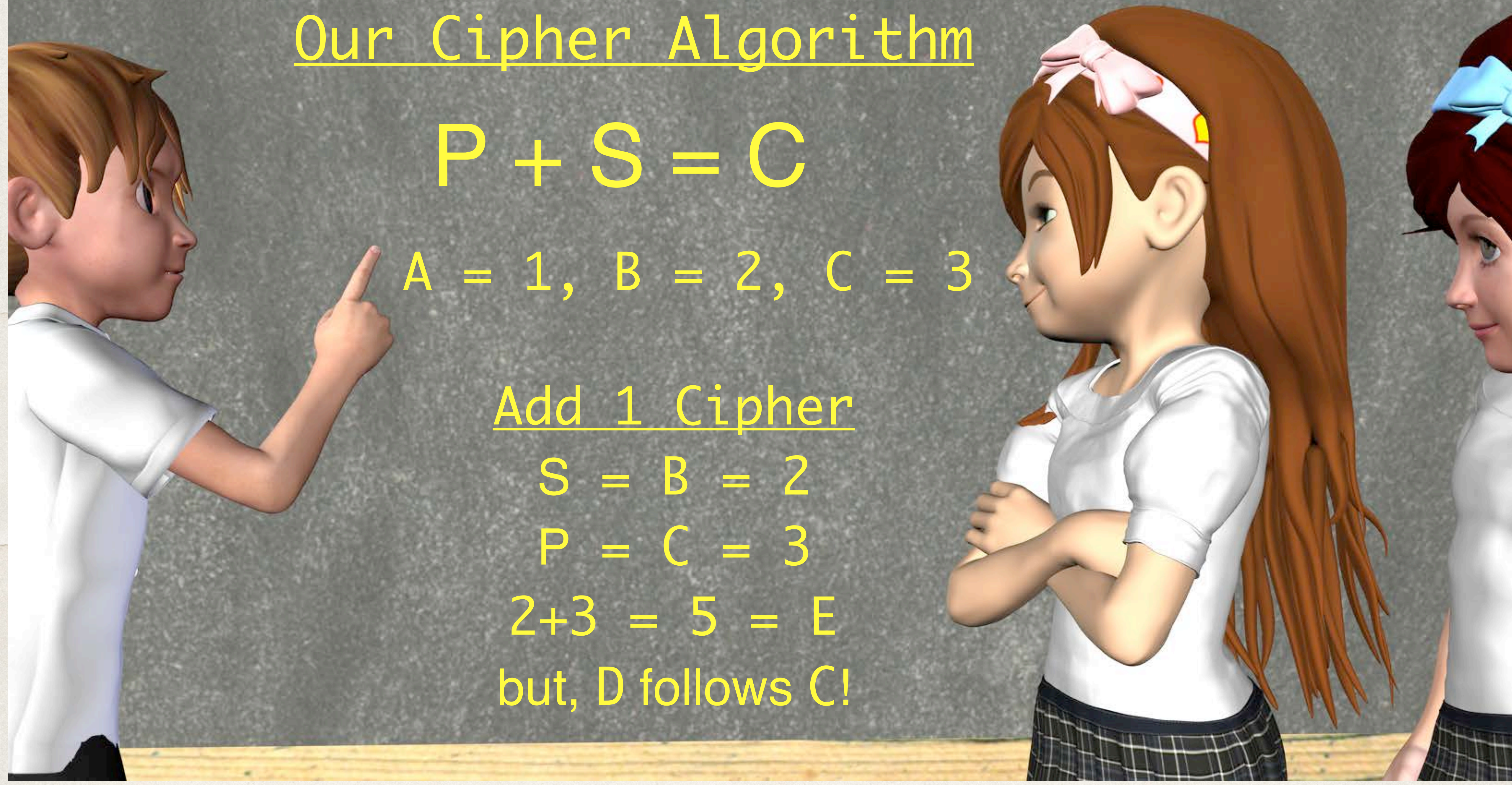
Add 1 Cipher

$$S = B = 2$$

$$P = C = 3$$

$$2 + 3 = 5 = E$$

but, D follows C!



Letters as Numbers

A $\neq$ 1



A = 0



Letters as Numbers

A = 0,

B = 1,

C = 2,

...

Y = 24,

Z = 25.

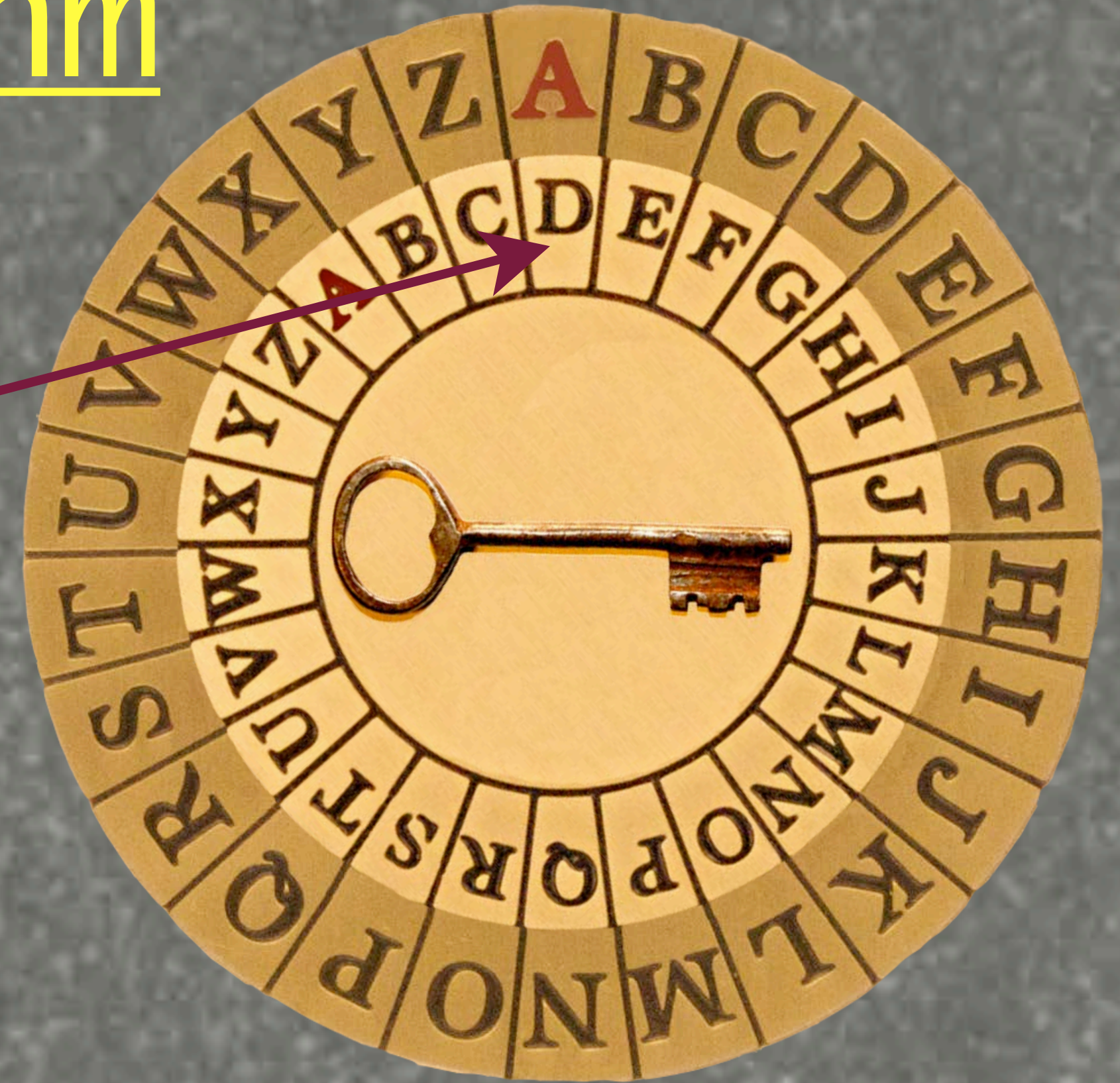


Our Cipher Algorithm

$$P + S = C$$

$$2 + 3 = 5$$

$$C + D = F$$



Our Cipher Algorithm

$$P + S = C$$

$$P + S - S = C - S$$

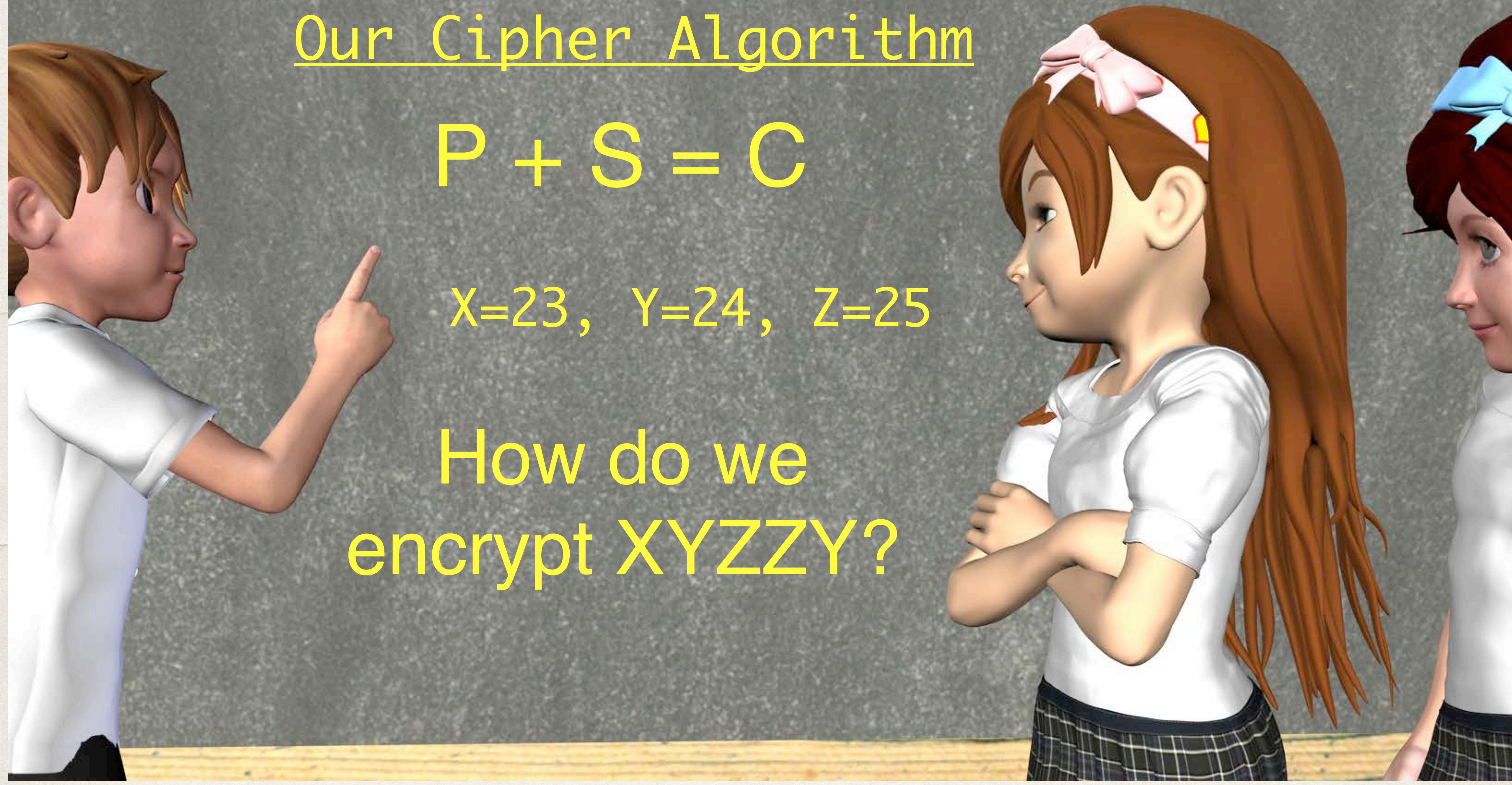
$$P = C - S$$

Our Cipher Algorithm

$$P + S = C$$

$X=23$, $Y=24$, $Z=25$

How do we
encrypt XYZZY?



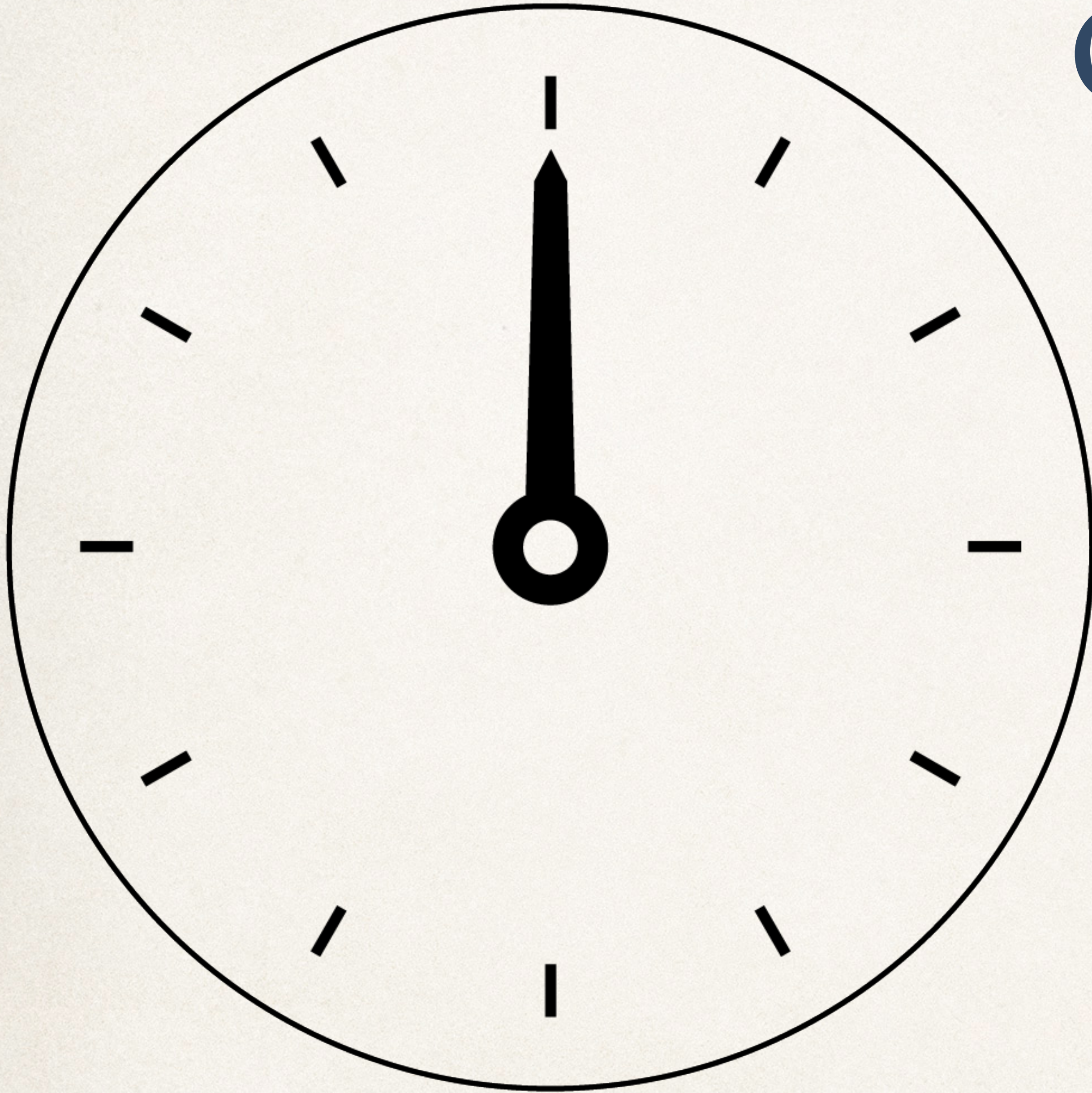
A Cipher Disk



ABCCB

Clock Arithmetic

Start time: 7:00



Clock Arithmetic



Start time: 7:00

End: 7 hours later

End time: ~~24:00~~?

Clock Arithmetic



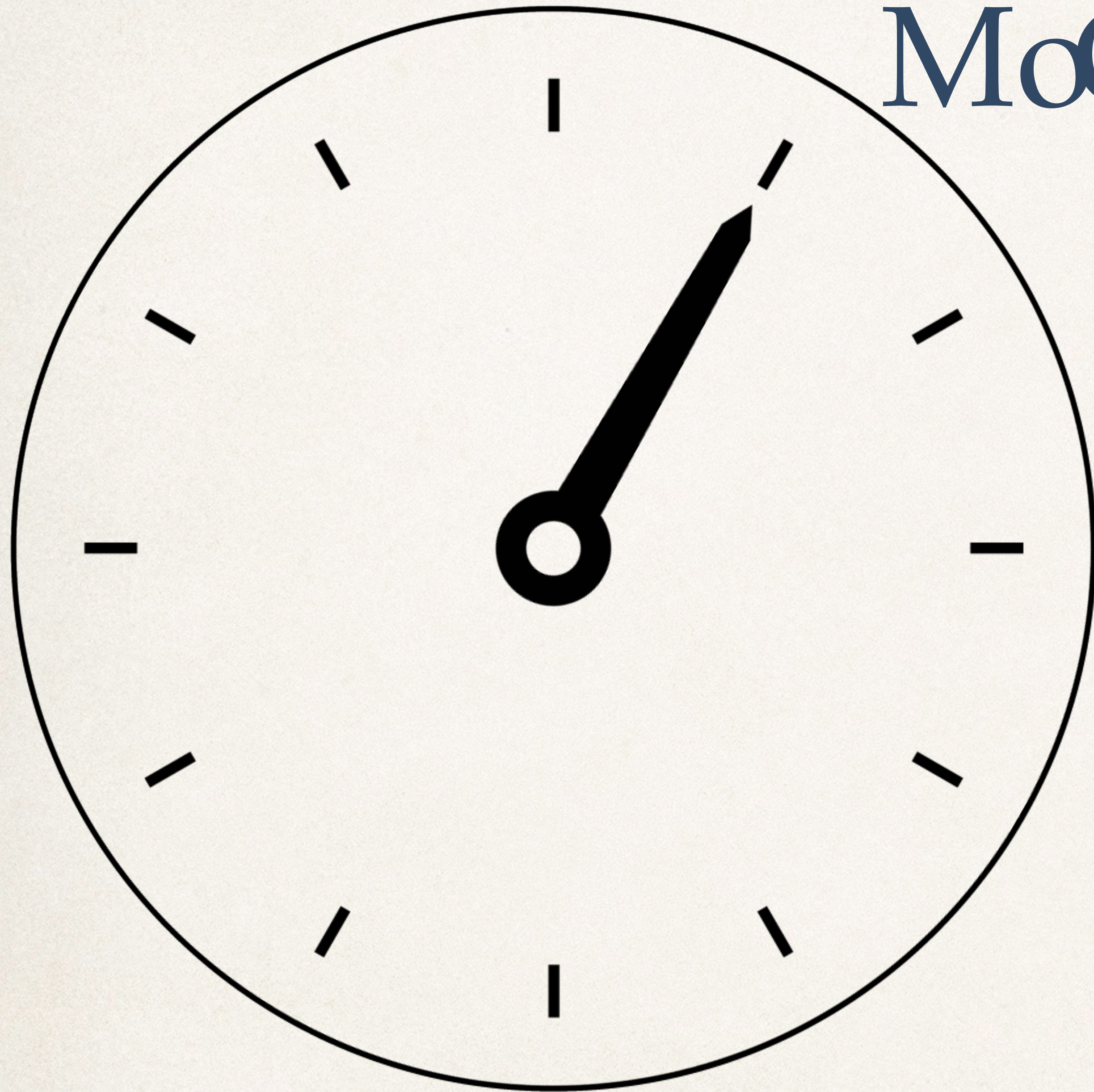
Start time: 7:00

End: 42 hours later

End time: ~~49:00~~ 12 and
keep the remainder.

$49 \div 12 = 4,$
remainder = 1

Modular Arithmetic



Clock Time =
 $(\text{Now} + \text{Length}) \bmod 12$

$$(7 + 42) \bmod 12 = 1$$

Cracking the Cipher Key

A COLD!





Cipher Disk:
simple
substitution
cipher

B DPME

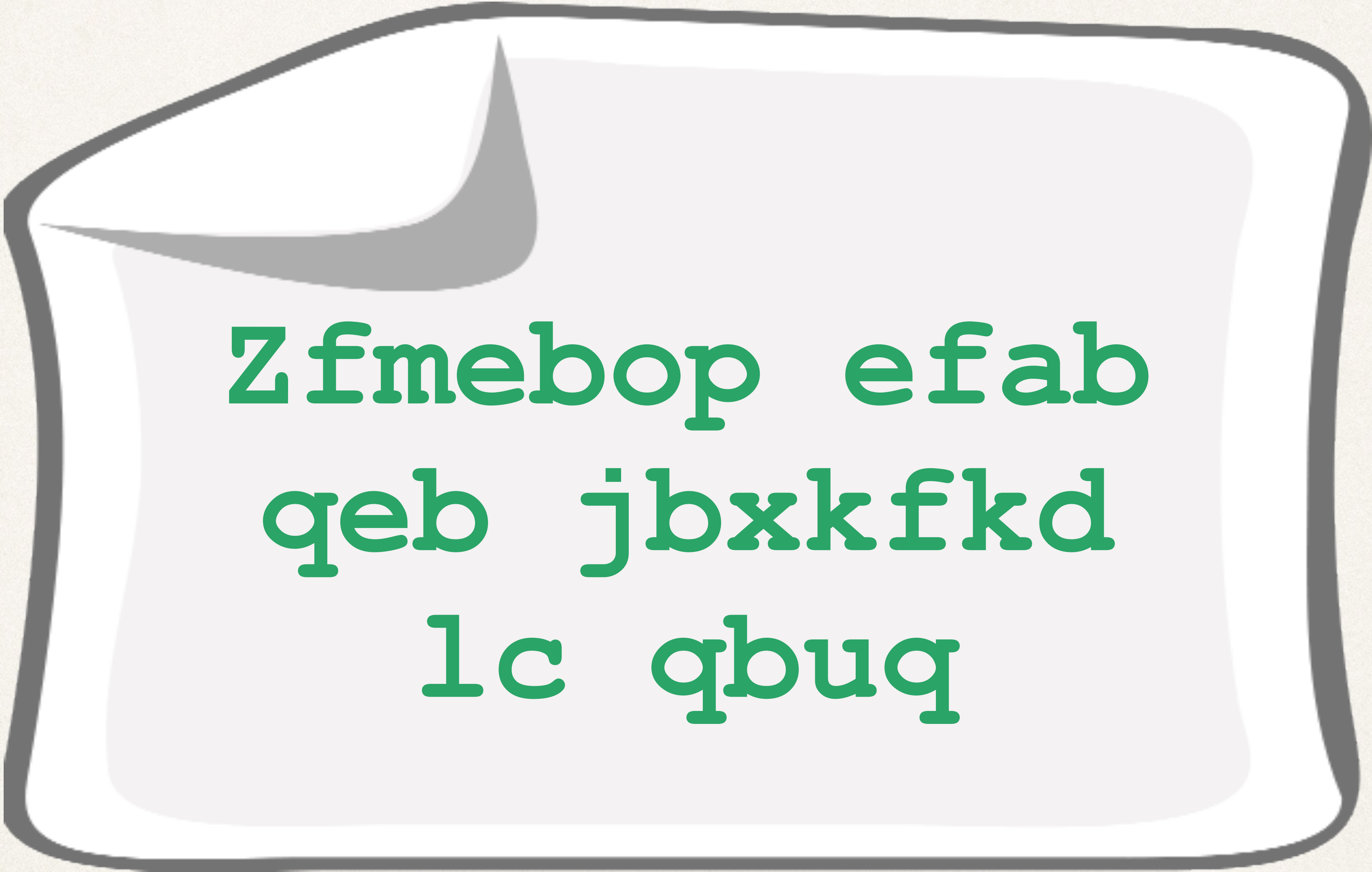
A COLD

Cipher Disk:

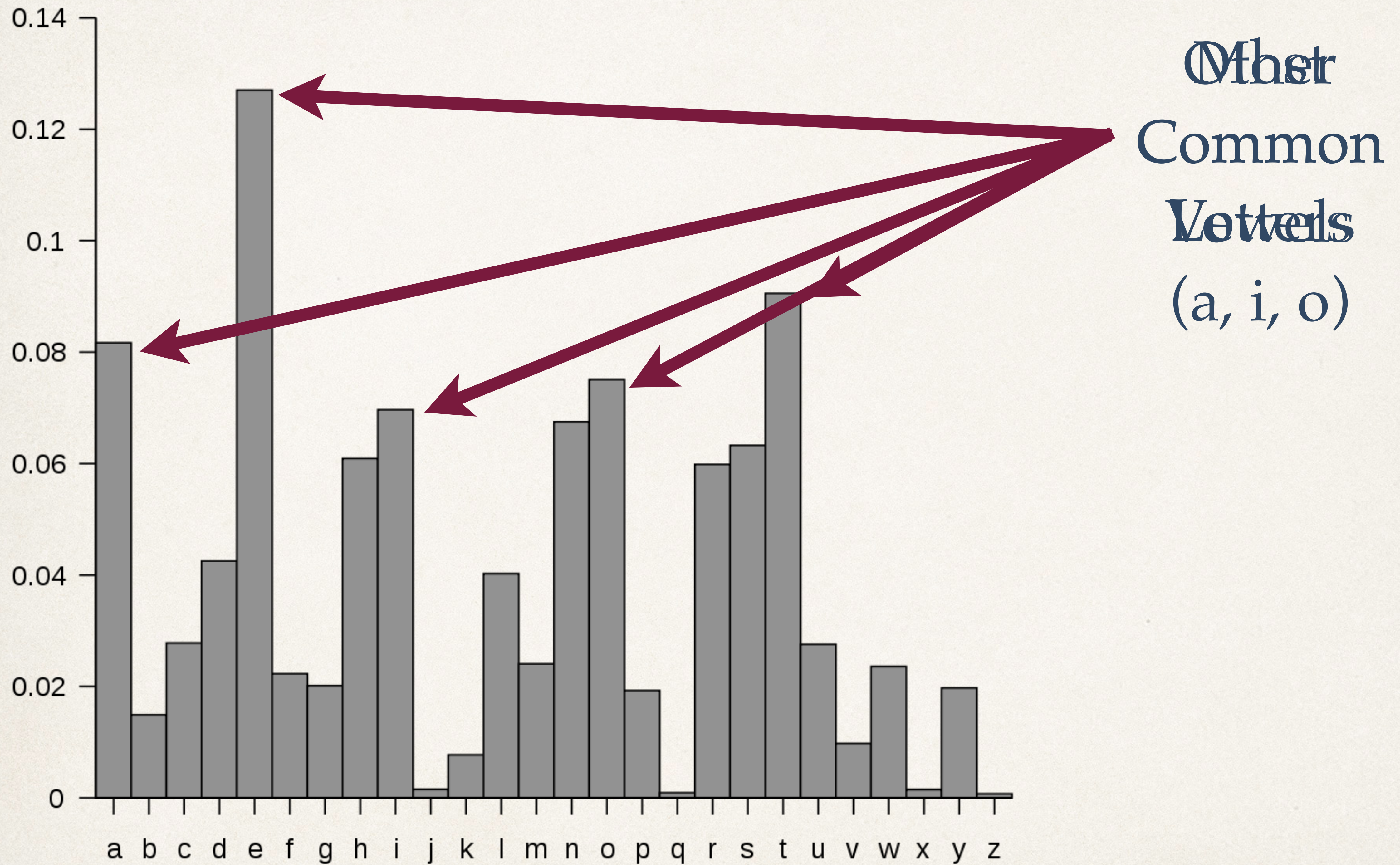


B D P M E

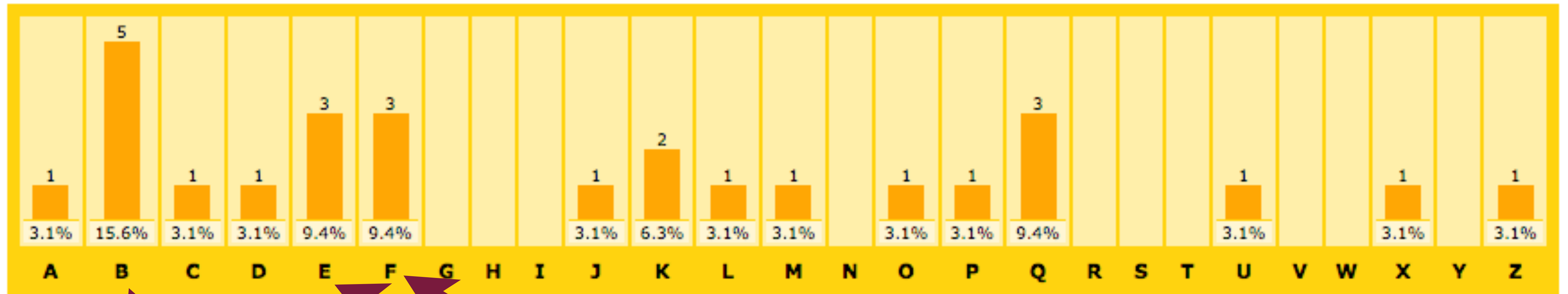
A C O L D



Zfmebop efab
qeb jbxkfk
lc qbuq



Zfmebop efab qeb
jbxkfk d lc qbuq



Most frequent

Very frequent



Ciphertext B =
Plaintext E?

Zfmebop
efab qeb
jbxkfkq dc
qbxq



Software Players in this Production:

- ◆DAZ Studio 4.6 Pro, by DAZ 3D
- ◆Keynote by Apple, Inc.
- ◆Sadie and Sam for Genesis, by 3D Universe
- ◆Saddle Oxfords for Genesis, by blondie9999
- ◆Interiors the Classroom, by Maclean
- ◆Rock_it Bundle, by SilvaAnt3d
- ◆Anime School Girl Uniform, by Bobbie25
- ◆Japanese School Uniform for boys, by Sickleyield
- ◆Clock face by markroth8 from openclipart.org
- ◆Frequency Analysis from from <http://www.counton.org/explorer/codebreaking/frequency-analysis.php>



Copyright 2013 Cryptosmith Institute

Grade School

Crypto

Part 2

Dr. Rick Smith, Cryptosmith

October, 2016

What We'll Learn About

“Mono-alphabetic ciphers”

- ◆ Trouble with Caesar-like ciphers
- ◆ Scrambled alphabets
- ◆ Symbol alphabets
- ◆ Decrypting/Solving an alphabet

Alice



Bob





A COLD!

Eve

B DPME

A Cipher Disk



We pick a cipher
to use by setting
the inner disk

A B C D E F G H I J K . . .

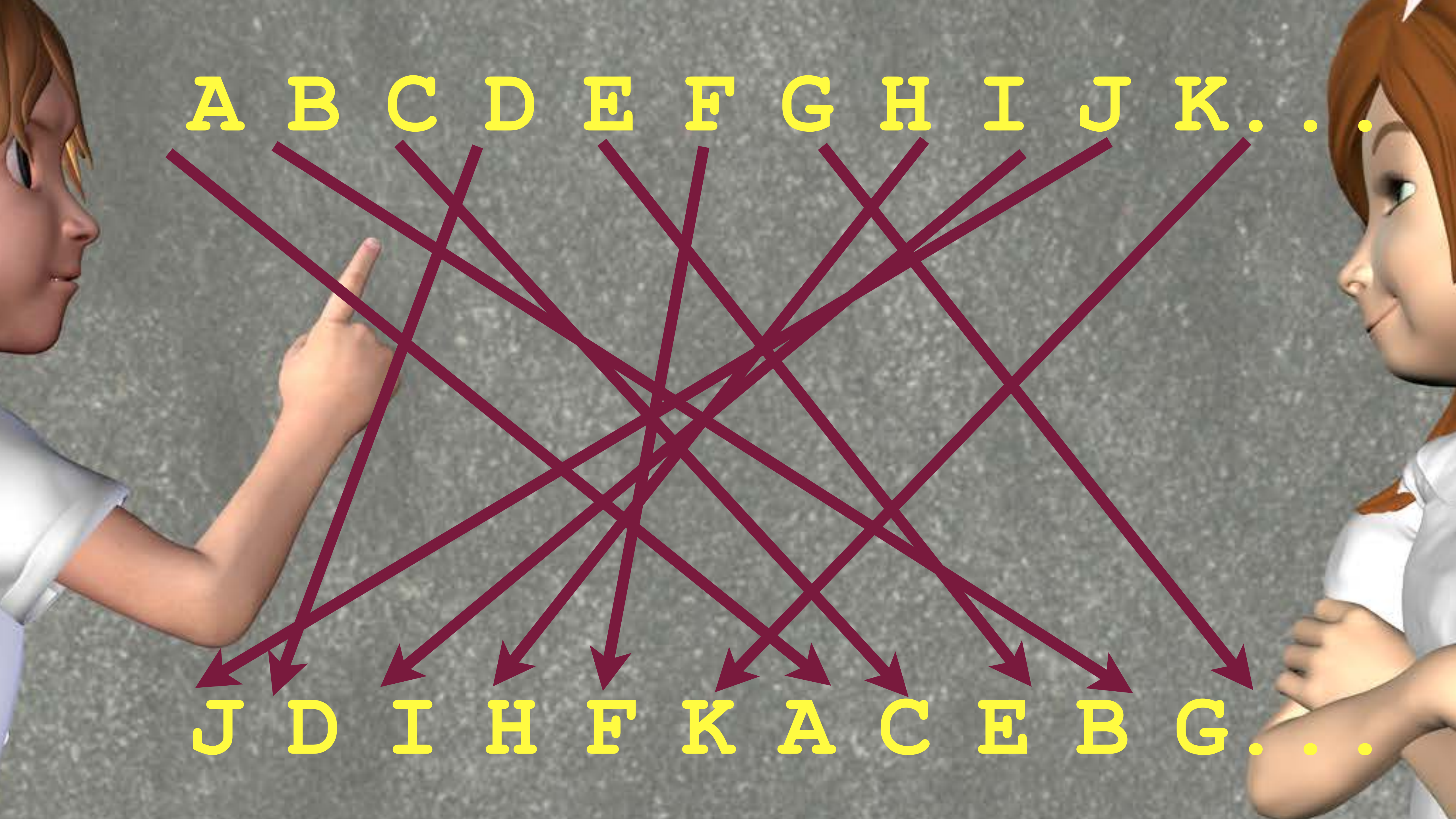
B C D E F G H I J K L . . .

B BEUVES DJQHEES?



A Simple Substitution Cipher

Zfmebor
efab qeb
jbxkfkq dc
qbuxq



A

B

C

D

E

F

G

H

I

J

K

...

J

D

I

H

F

K

A

C

E

B

G

...

A Better Cipher

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

J DFYYFN IELCFN

Symbol Alphabets

A B C D E F G H I J K L M N O P Q R



Symbol Alphabets

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 (+?3
4 ; 48) 4+ ; 161 ; : 188 ; +? ;

Symbols and Alphabets

A	B	C
D	E	F
G	H	I

JUL

LITIGATED

Pigpen Cipher



J .	K .	L .
M .	N .	O .
P .	Q .	R .

A L C O L D

Pigpen Cipher

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	

Ciphers
hide the
meaning
of text

Cracking Alphabets



NEED TO
THE QUIET

A close-up photograph of a person's hand holding a white smartphone. The hand has purple nail polish on the fingers. The phone's screen is on, showing a light blue background with the text 'NEFU BU' on the top line and 'UIF QBSL' on the bottom line in a green, serif font. The phone has a silver-colored circular button on the left side of the front face.

NEFU BU
UIF QBSL



THE
PARK!

Recognizing Patterns

⌞⏞⏞ ⌞ ⌞ ⌞ ⌞ ⌞ ⌞ ⌞ ⌞

NFFU BU UIF QBSL

RUUC WC CTU NWFB

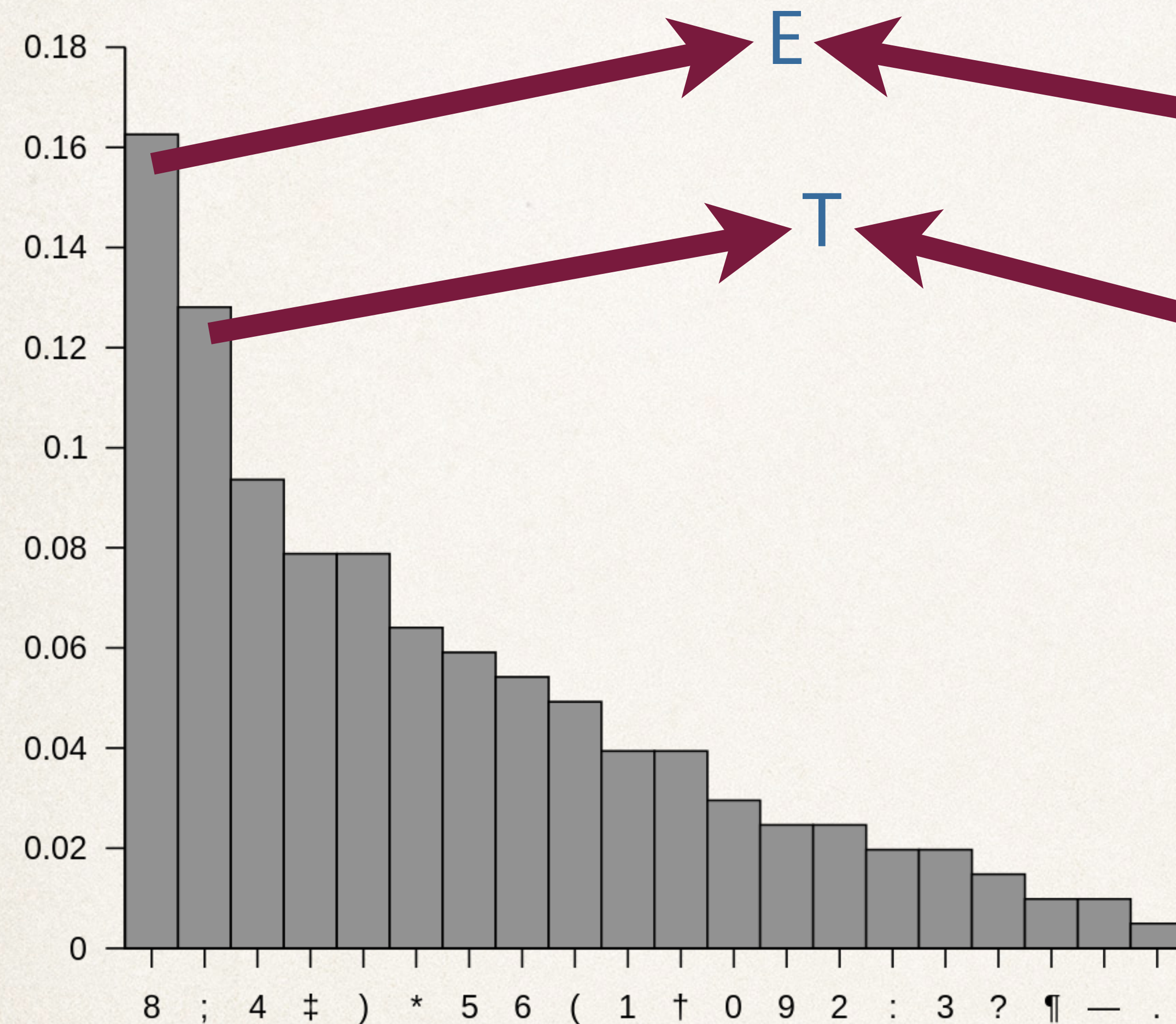
ZRRG NG GUR CNEX

PHHW DW WKH SDUN

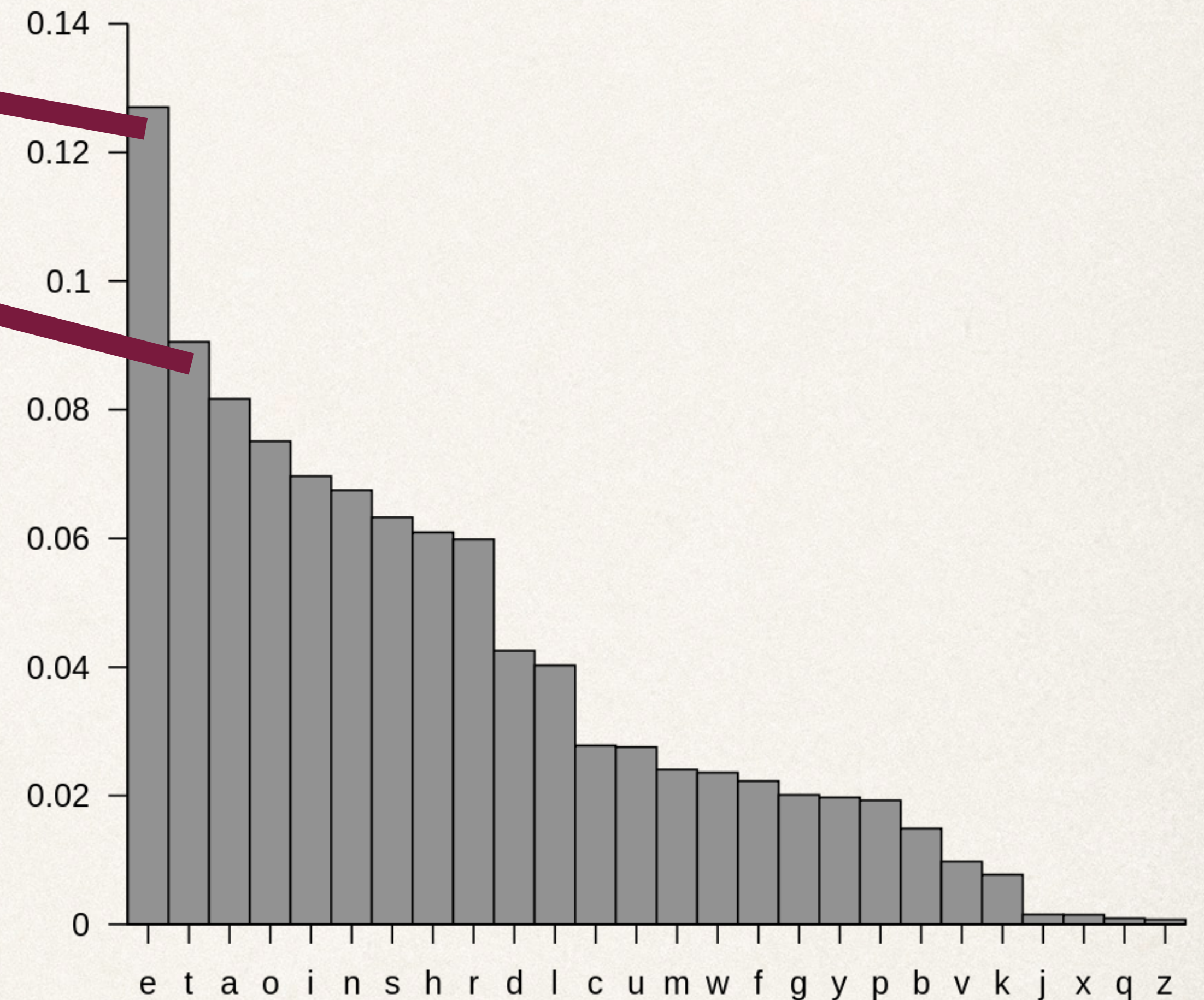
Cracking Symbols

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 (+?3
4 ; 48) 4+ ; 161 ; : 188 ; +? ;

Letter Frequencies



From “The Gold Bug”



From typical English

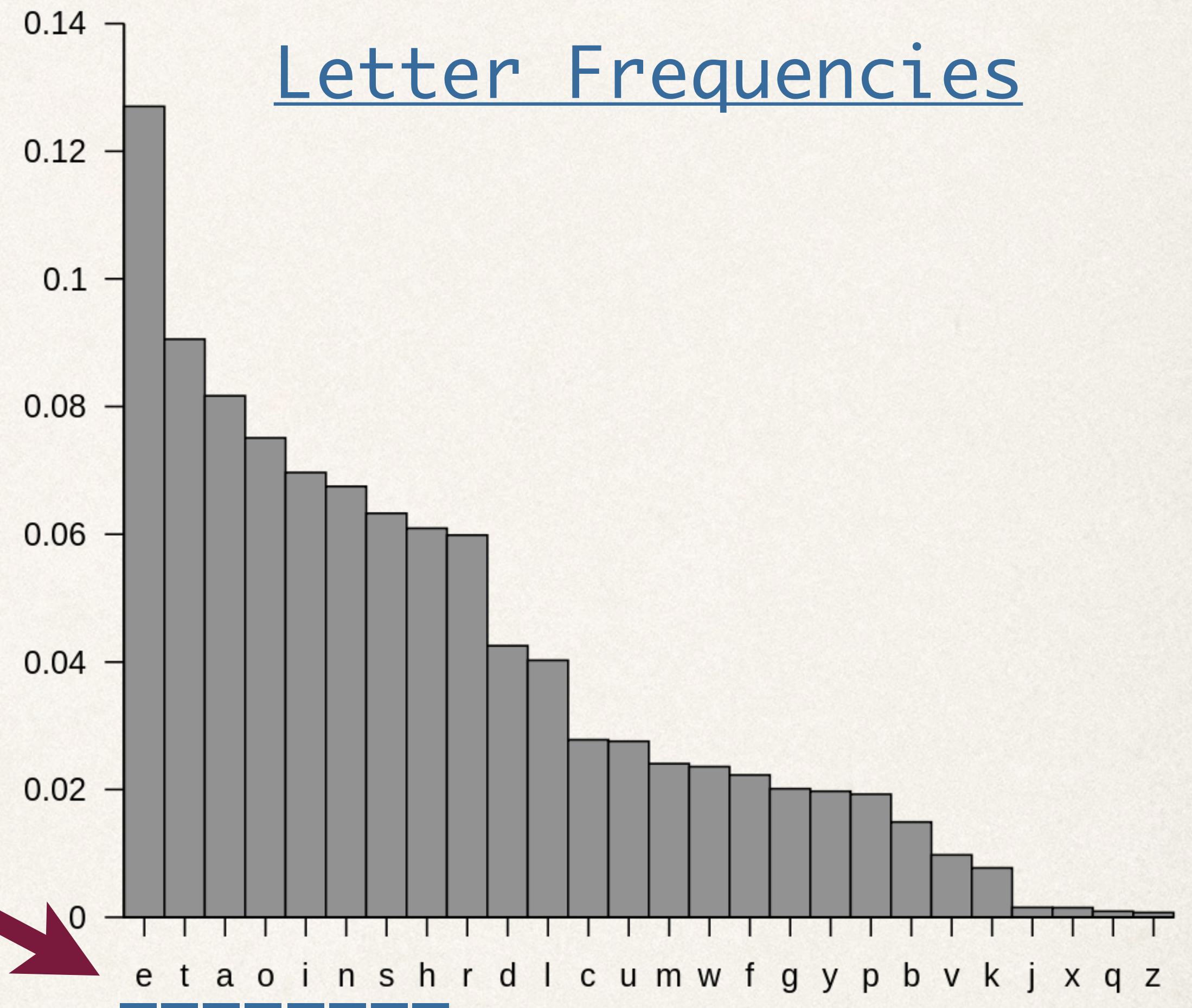
From “The Gold Bug”

A3⊕⊕!30A)) 6*TAE26) A⊕.) A⊕) TE06*T
AE!E`60)) EAT1⊕ (T:⊕*E!E3 (EE) A*!T
A6 (TEE*96*?TE) *⊕ (TAEA) TA*!2:*⊕
(TA9A6*2 (A*—A) E`E*TA0692EA) T) 6
!E) A⊕⊕T1 (⊕9TAE0E1TE:E⊕1TAE!EAT
A) AEA!A2EE06*E1 (⊕9TAET (EE TA (⊕?3
ATAE) A⊕T161T:1EET⊕?T

From “The Gold Bug”

ETAO

INSH



From typical English

From “The Gold Bug”

A300!30ASSINTHE2ISHO.SHOSTE0INT
HE!E`10\$SEAT1O(T:ONE!E3(EESAN!T
H6(TEEN9IN?TESNO(TEASTAN!2:NO
(TH9AIN2(AN—HSE`ENTH40192EASTSI
!E)HOOT1(O9THE0E1TE:EO1THE!EAT
H)HEA!A2EE0INE1(O9THET(EETH4(O?3
HTHESHOT161T:1EETO?T

From “The Gold Bug”

A GOOD GLASS IN THE BISHOP SHOP HOSTED IN
HE DEVILS SEAT FORTY ONE DEGREES AND
THIRTEEN MINUTES NORTH EAST AND BY NO
RTH MAIN BRANCH SEVENTH LIMB EAST SI
DE SHOOT FROM THE LEFT EYE OF THE DEATH
HIS HEAD A BEED LINE FROM THE TREE THROUG
H THE SHOT FIFTY FEET OUT



Software Players in this Production:

- ◆DAZ Studio 4.6 Pro, by DAZ 3D
- ◆Keynote by Apple, Inc.
- ◆Sadie and Sam for Genesis, by 3D Universe
- ◆Rock_it Bundle, by SilvaAnt3d
- ◆Pirate and Princess Sea Chests by JGreenlees
- ◆Cipher tools from <http://rumkin.com/tools/cipher/>
- ◆Statistics for “The Gold Bug” by Czech Wikipedia user Utar
- ◆Frequency analysis from <http://www.counton.org/explorer/codebreaking/frequency-analysis.php>



Copyright 2016 Cryptosmith Institute