# Cryptography - Part 1

Feb. 20, 2025

# Recap question:

Feb. 20, 2025

A disease in the SIR model is estimated to have parameter values $\beta = 2$ and $\gamma = 1$. What is the herd immunity threshold for the disease?

The herd immunity threshold is

$$p_c = 1 - \frac{1}{R_0}.$$

To compute this, we need to find the value of $R_0$ . We use the definition of $R_0$ :

$$R_0 = \frac{\beta}{\gamma} = \frac{2}{1} = 2$$

so

$$p_c = 1 - \frac{1}{R_0} = 1 - \frac{1}{2} = \frac{1}{2}.$$

# Cryptography - Part 1

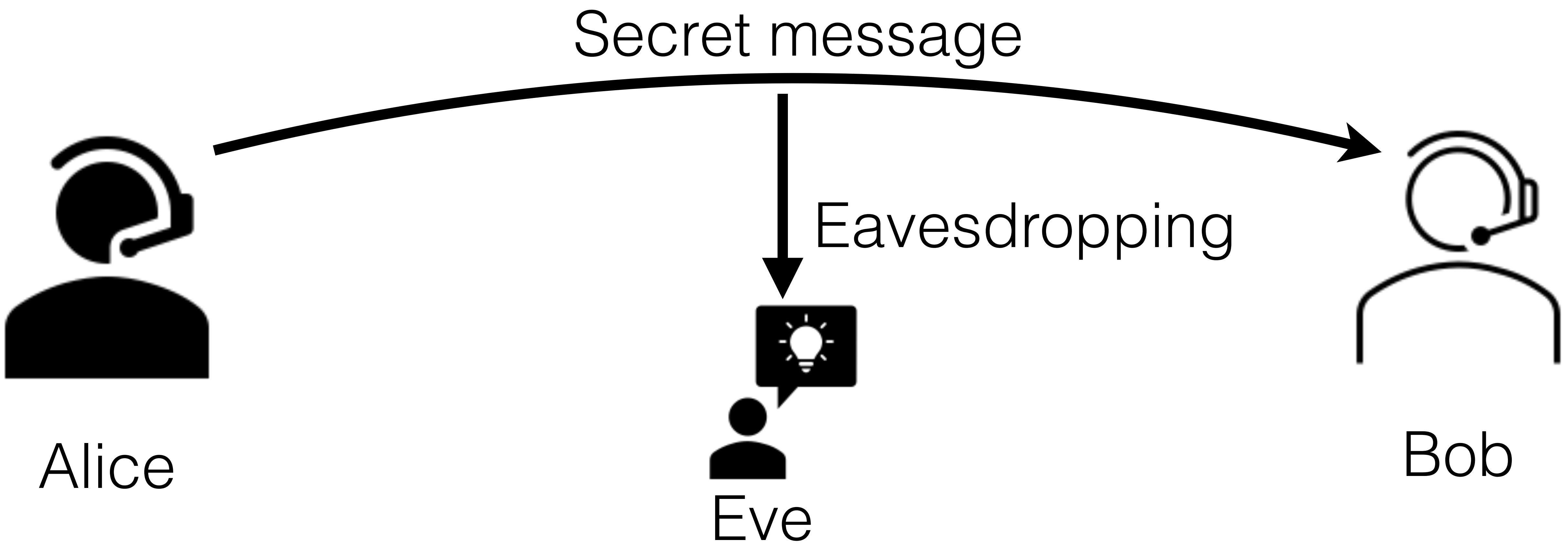
Feb. 20, 2025

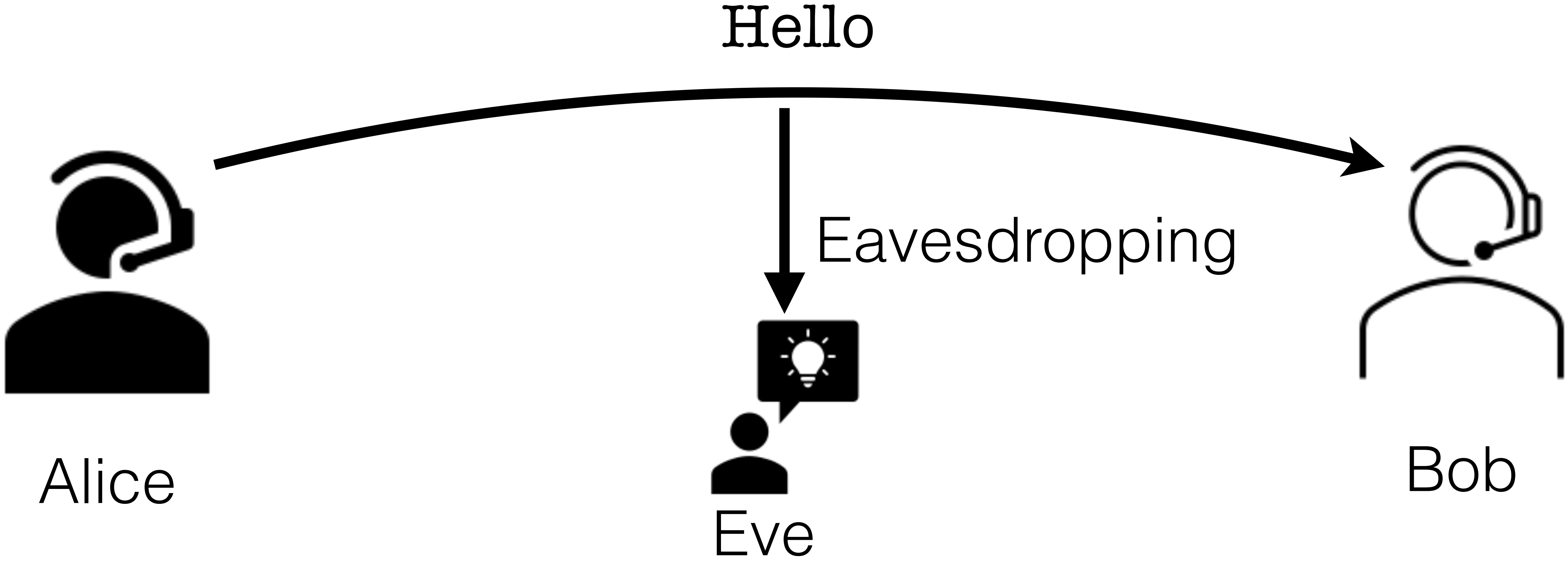
By the end of this lecture, you will be able to:

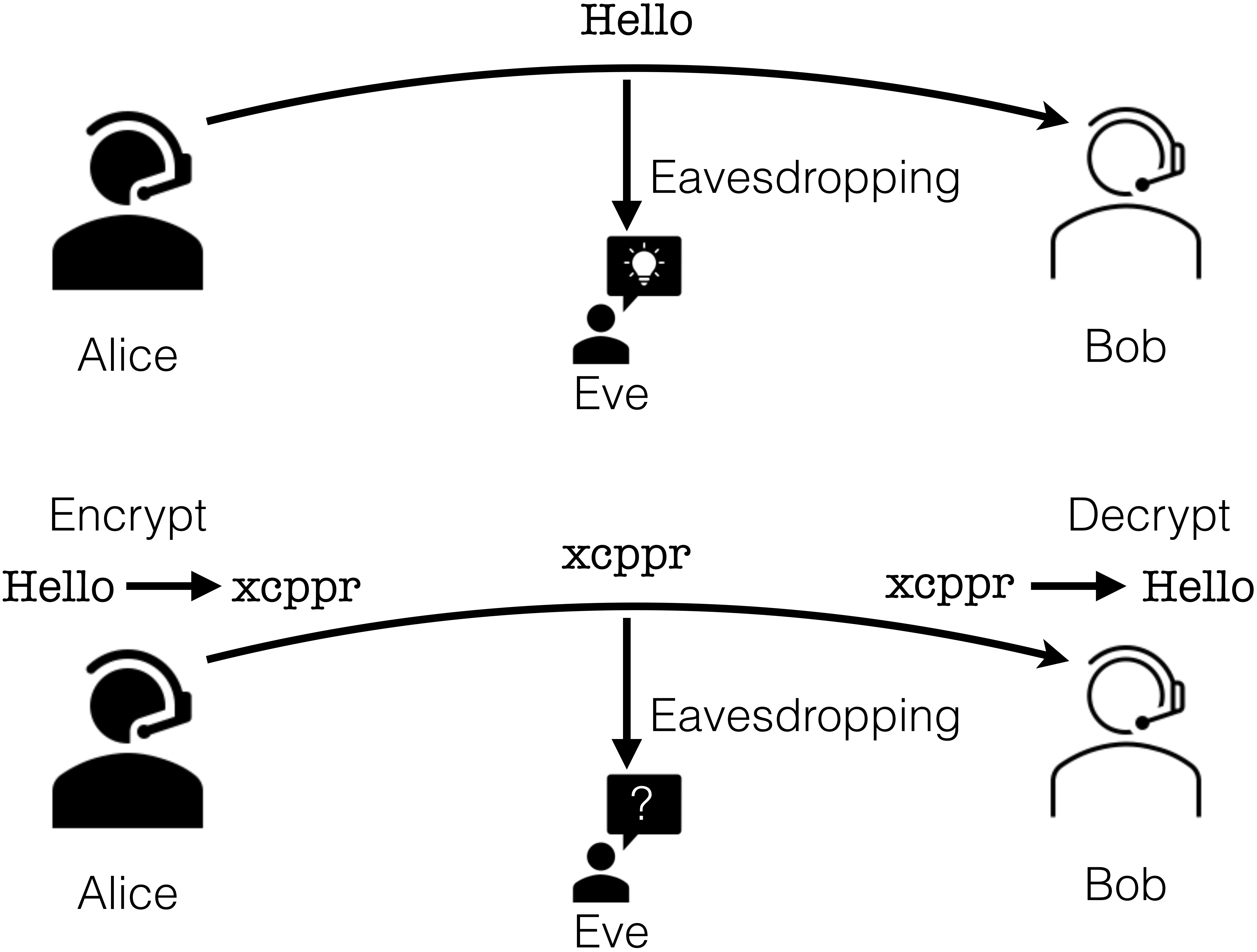
1. Define substitution ciphers and Caesar ciphers
2. Decrypt Caesar ciphers using the brute-force method
3. Decrypt substitution ciphers using frequency analysis

**Cryptography** is “the art of writing in secret characters”. A cryptographer encodes messages before they are transmitted so that even if the encrypted message is intercepted by a hostile party, its meaning will still remain secret.

**Cryptography** is “the art of writing in secret characters”. A cryptographer encodes messages before they are transmitted so that even if the encrypted message is intercepted by a hostile party, its meaning will still remain secret.




Hello
Eavesdropping
Alice
Eve
Bob

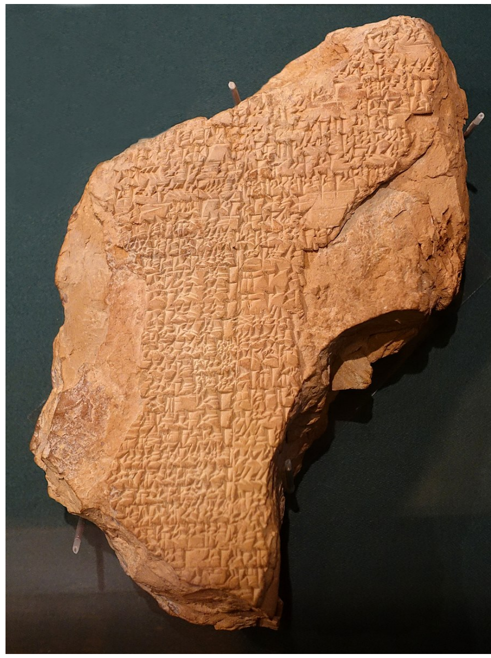

Hello
Eavesdropping
Alice
Eve
Bob
Encrypt
Decrypt
xcppr
Hello
xcppr
xcppr
Hello
Eavesdropping
?
Alice
Eve
Bob

In principle, only “friends” of the original cryptographer, who knows the secret recipe for decoding or decrypting, can decode the encrypted message to the original plain text.

A “code breaker” seeks to detect patterns in the encrypted messages that will lead to sufficient understanding of the encryption scheme to enable the discovery of a decryption method.

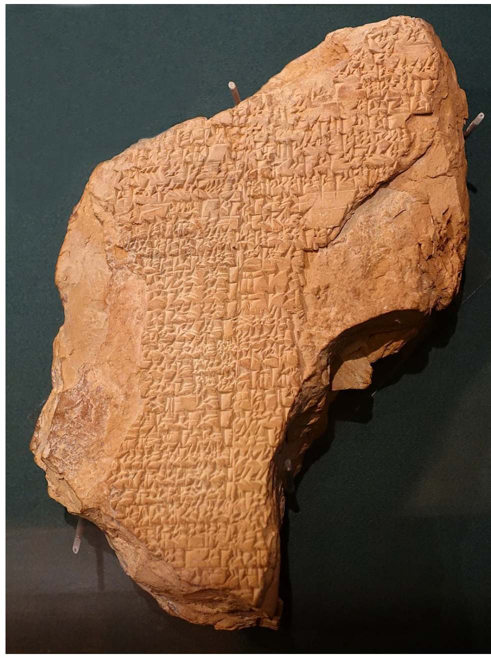
# Where is cryptography used?

# Where is cryptography used?

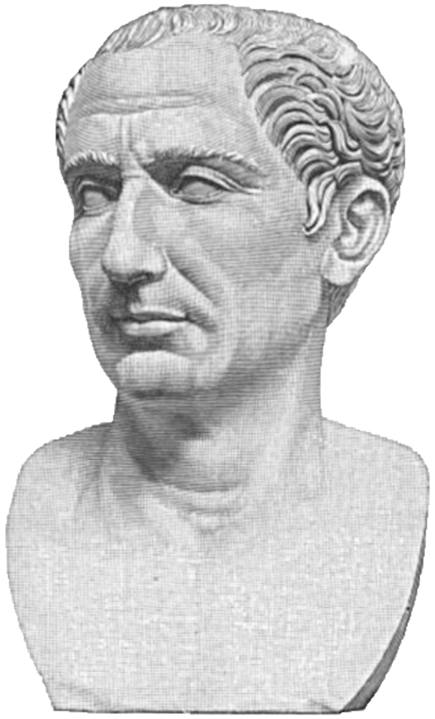


1500 BC: encrypted clay tablets to keep valuable information (recipe for pottery glaze) secret

# Where is cryptography used?

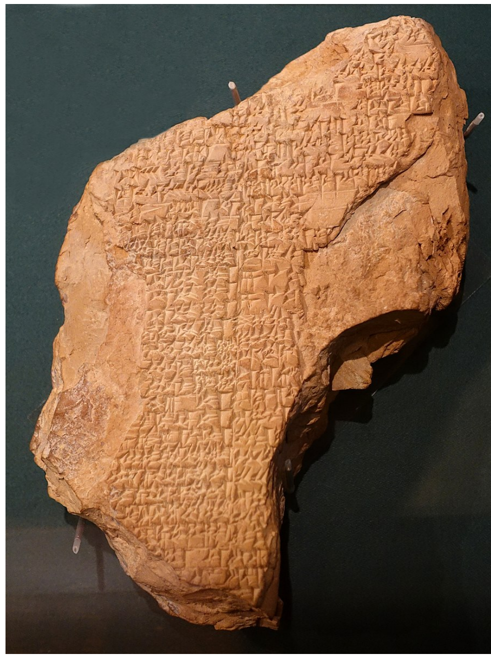


1500 BC: encrypted clay tablets to keep valuable information (recipe for pottery glaze) secret

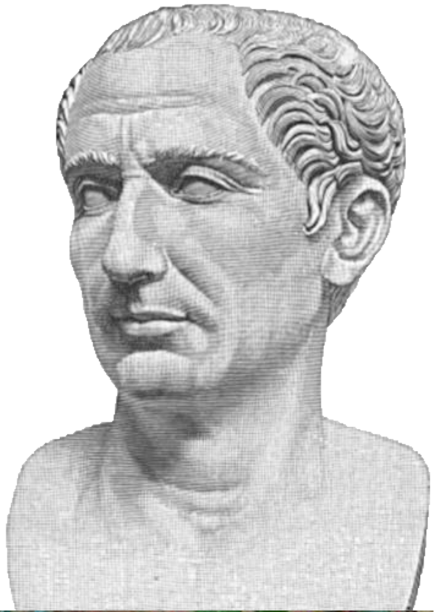


50 BC: Julius Caesar encrypted letters to generals at the frontlines

# Where is cryptography used?



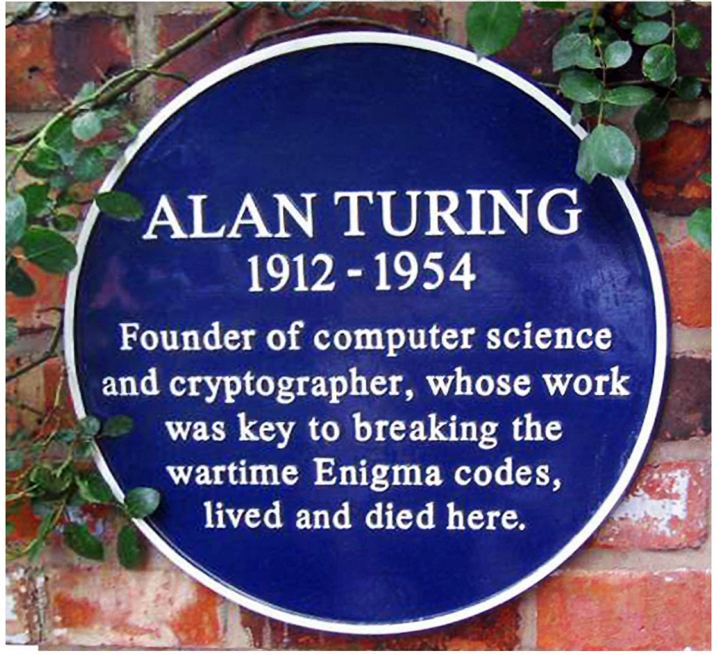
1500 BC: encrypted clay tablets to keep valuable information (recipe for pottery glaze) secret



50 BC: Julius Caesar encrypted letters to generals at the frontlines

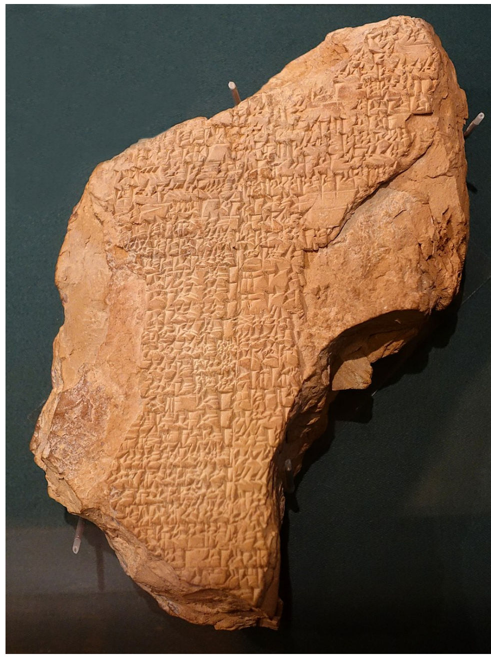
⋮

1940-1942 AD: British intelligence cracked the most secure German cipher (“Enigma”), contributing to the end of the war

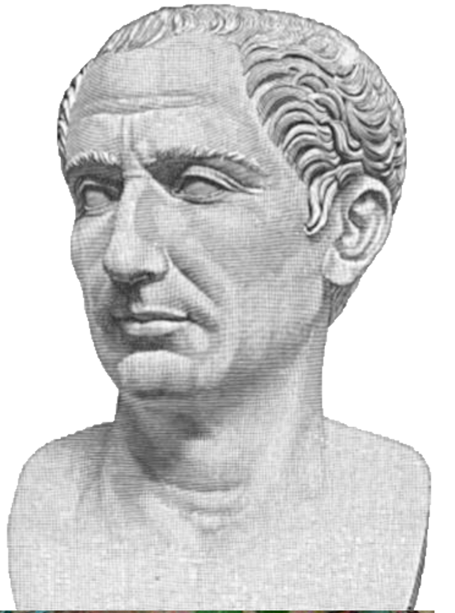


https://en.wikipedia.org/wiki/File:Turing_Plaque.jpg

# Where is cryptography used?



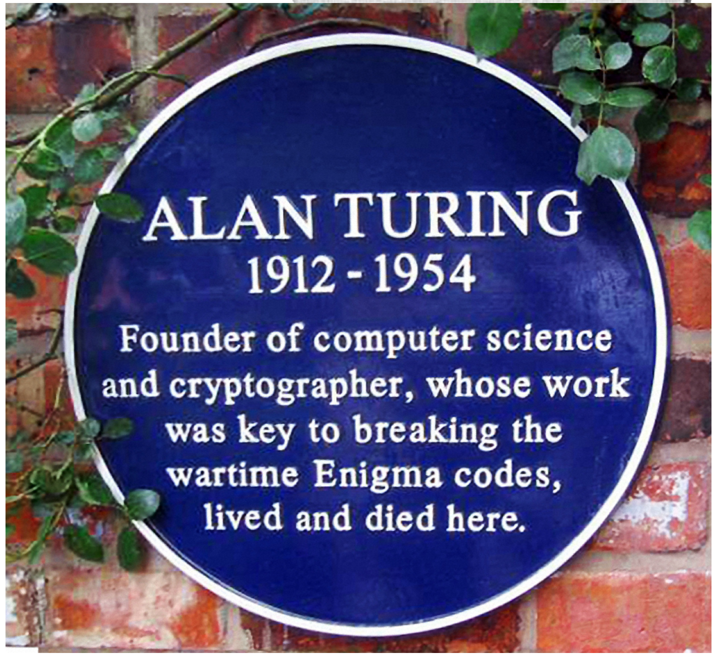
1500 BC: encrypted clay tablets to keep valuable information (recipe for pottery glaze) secret



50 BC: Julius Caesar encrypted letters to generals at the frontlines

⋮

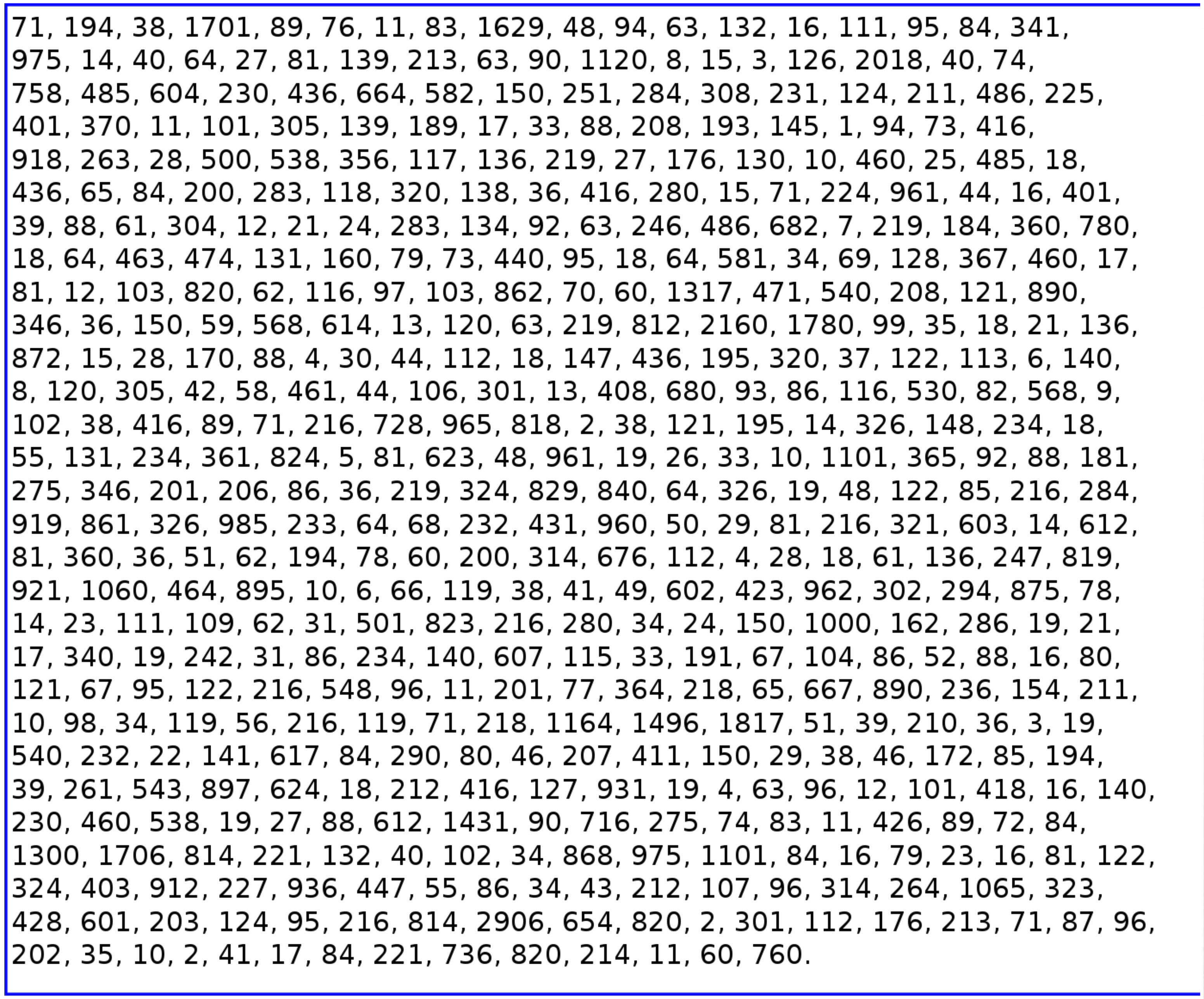
1940-1942 AD: British intelligence cracked the most secure German cipher (“Enigma”), contributing to the end of the war



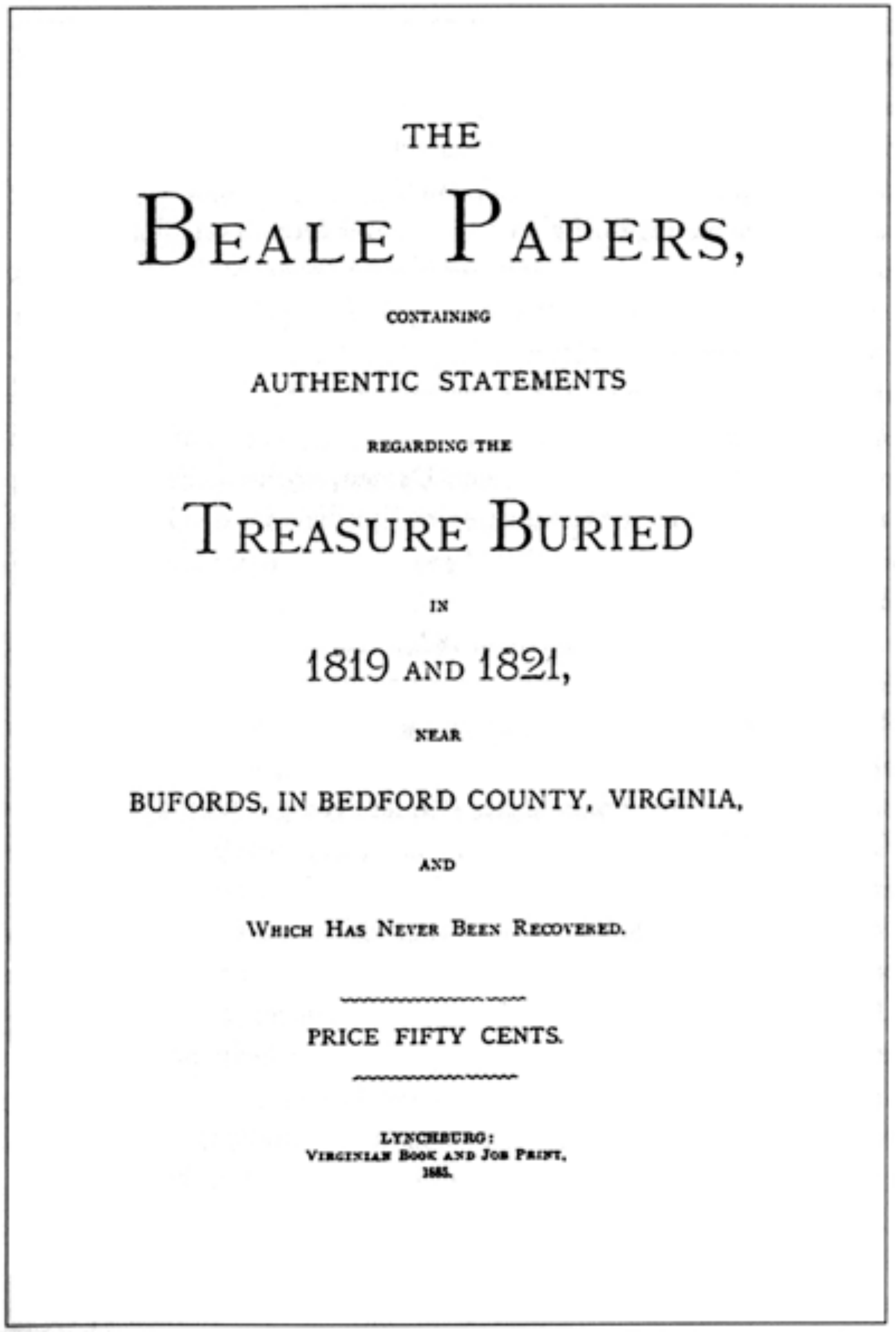
Today: logging into websites, sending emails, WhatsApp, verifying credit card information, cloud storage of pictures, …

https://en.wikipedia.org/wiki/File:Turing_Plaque.jpg

# Unsolved historical encryption techniques



71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341,
975, 14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74,
758, 485, 604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225,
401, 370, 11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416,
918, 263, 28, 500, 538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18,
436, 65, 84, 200, 283, 118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401,
39, 88, 61, 304, 12, 21, 24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780,
18, 64, 463, 474, 131, 160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17,
81, 12, 103, 820, 62, 116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890,
346, 36, 150, 59, 568, 614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136,
872, 15, 28, 170, 88, 4, 30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140,
8, 120, 305, 42, 58, 461, 44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9,
102, 38, 416, 89, 71, 216, 728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18,
55, 131, 234, 361, 824, 5, 81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181,
275, 346, 201, 206, 86, 36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284,
919, 861, 326, 985, 233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612,
81, 360, 36, 51, 62, 194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819,
921, 1060, 464, 895, 10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78,
14, 23, 111, 109, 62, 31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21,
17, 340, 19, 242, 31, 86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80,
121, 67, 95, 122, 216, 548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211,
10, 98, 34, 119, 56, 216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19,
540, 232, 22, 141, 617, 84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194,
39, 261, 543, 897, 624, 18, 212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140,
230, 460, 538, 19, 27, 88, 612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84,
1300, 1706, 814, 221, 132, 40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122,
324, 403, 912, 227, 936, 447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323,
428, 601, 203, 124, 95, 216, 814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96,
202, 35, 10, 2, 41, 17, 84, 221, 736, 820, 214, 11, 60, 760.



THE

BEALE PAPERS,

CONTAINING

AUTHENTIC STATEMENTS

REGARDING THE

TREASURE BURIED

IN

1819 AND 1821,

NEAR

BUFORDS, IN BEDFORD COUNTY, VIRGINIA,

AND

WHICH HAS NEVER BEEN RECOVERED.

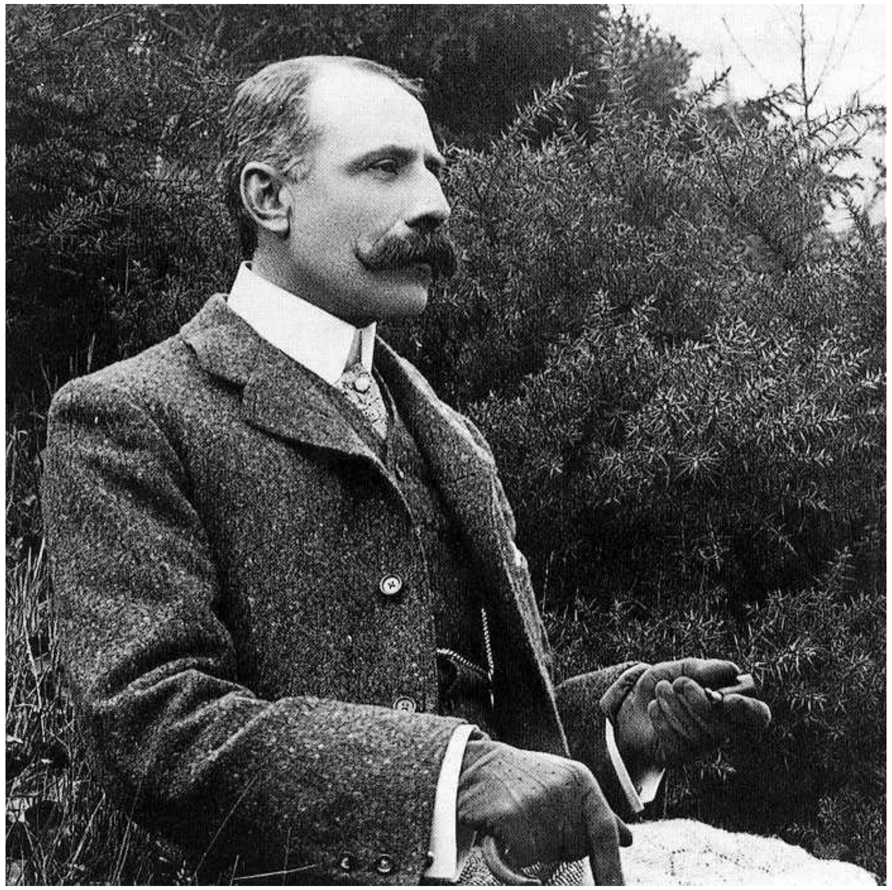
PRICE FIFTY CENTS.

LYNCHBURG:
VIRGINIAN BOOK AND JOB PRINT,
1885.

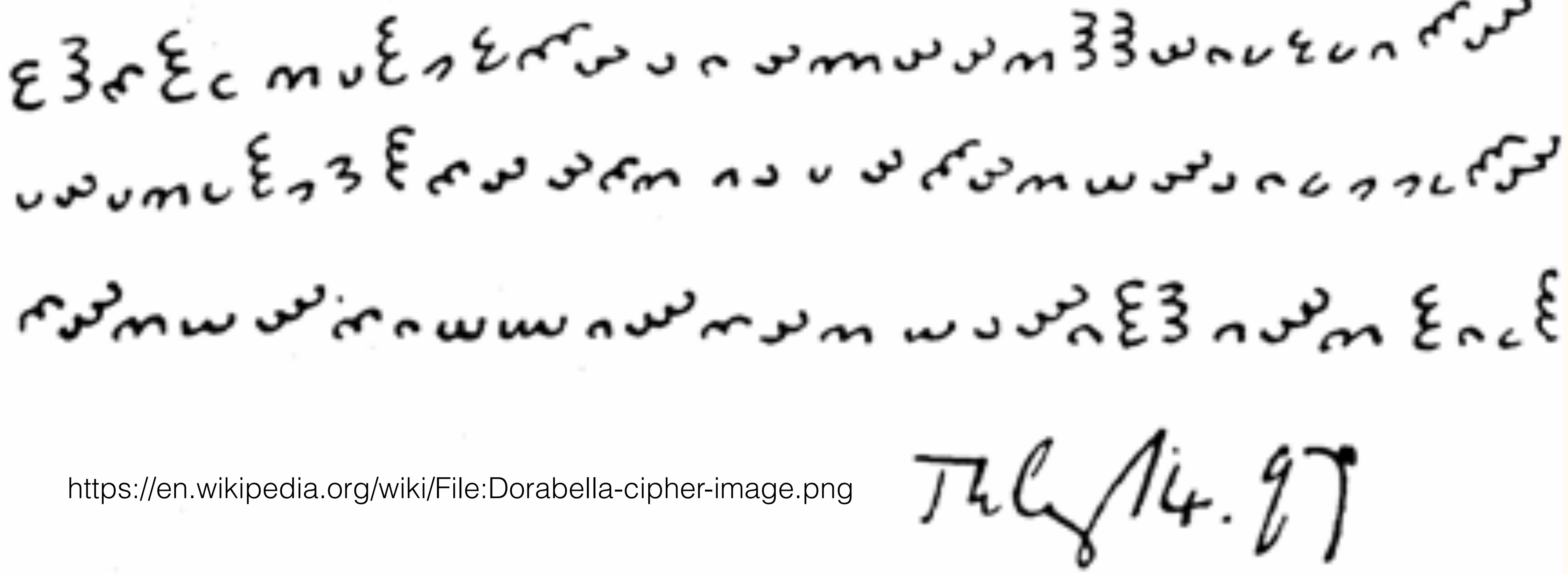
https://commons.wikimedia.org/wiki/File:Beale_1.svg

# Unsolved historical encryption techniques

Letter written by composer Edward Elgar to Dora Penny



https://commons.wikimedia.org/wiki/File:Edward_Elgar.jpg



https://en.wikipedia.org/wiki/File:Dorabella-cipher-image.png

# Some (not very good) encryption techniques:

1. Ehay isay eryvay illysay

## Some (not very good) encryption techniques:

1. Ehay isay eryvay illysay

   This is pig latin. The decrypted message is:

   "He is very silly"

**Some (not very good) encryption techniques:**

1. Ehay isay eryvay illysay

   This is pig latin. The decrypted message is:

   “He is very silly”

2. noitpyrcne eruces yreV

## Some (not very good) encryption techniques:

1. Ehay isay eryvay illysay

   This is pig latin. The decrypted message is:

   “He is very silly”

2. noitpyrcne eruces yreV

   This message is just written backwards. The decrypted message is:

   “Very secure encryption”

**Some (not very good) encryption techniques:**

1. Ehay isay eryvay illysay

   This is pig latin. The decrypted message is:

   “He is very silly”

2. noitpyrcne eruces yreV

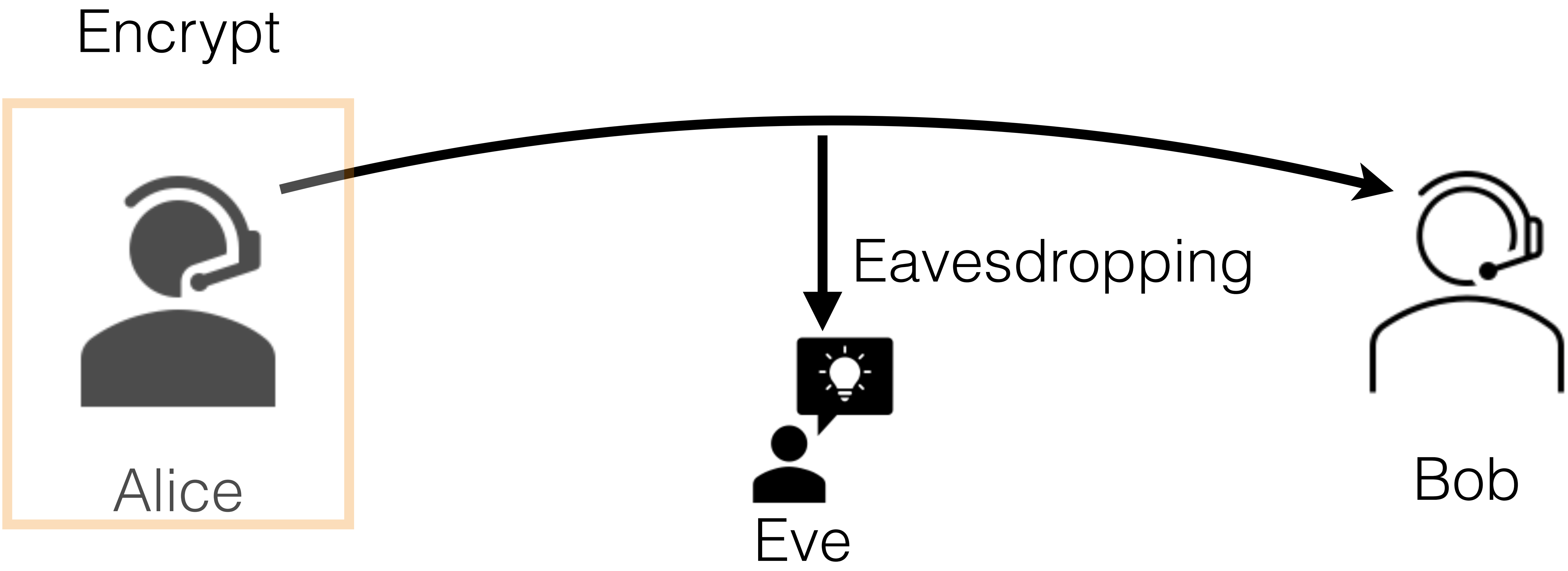
   This message is just written backwards. The decrypted message is:

   “Very secure encryption”

For the rest of today, we will discuss better techniques!

# Old standards: substitution ciphers

The oldest schemes replace the letters in the message one by one, following a fixed recipe.



# Old standards: substitution ciphers

The oldest schemes replace the letters in the message one by one, following a fixed recipe.

For example,

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

How do we encrypt “Math alive”?

# Old standards: substitution ciphers

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

Math alive

# Old standards: substitution ciphers

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

Math alive

# Old standards: substitution ciphers

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

Math alive

```
L
```

# Old standards: substitution ciphers

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

Math alive

Lg

# Old standards: substitution ciphers

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

Math alive

Lgx

# Old standards: substitution ciphers

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

Math alive

Lgxu

# Old standards: substitution ciphers

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

Math alive

Lgxu g

# Old standards: substitution ciphers

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

Math alive

Lgxu gt

# Old standards: substitution ciphers

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

Math alive

Lgxu gty

# Old standards: substitution ciphers

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

Math alive

Lgxu gtyr

# Old standards: substitution ciphers

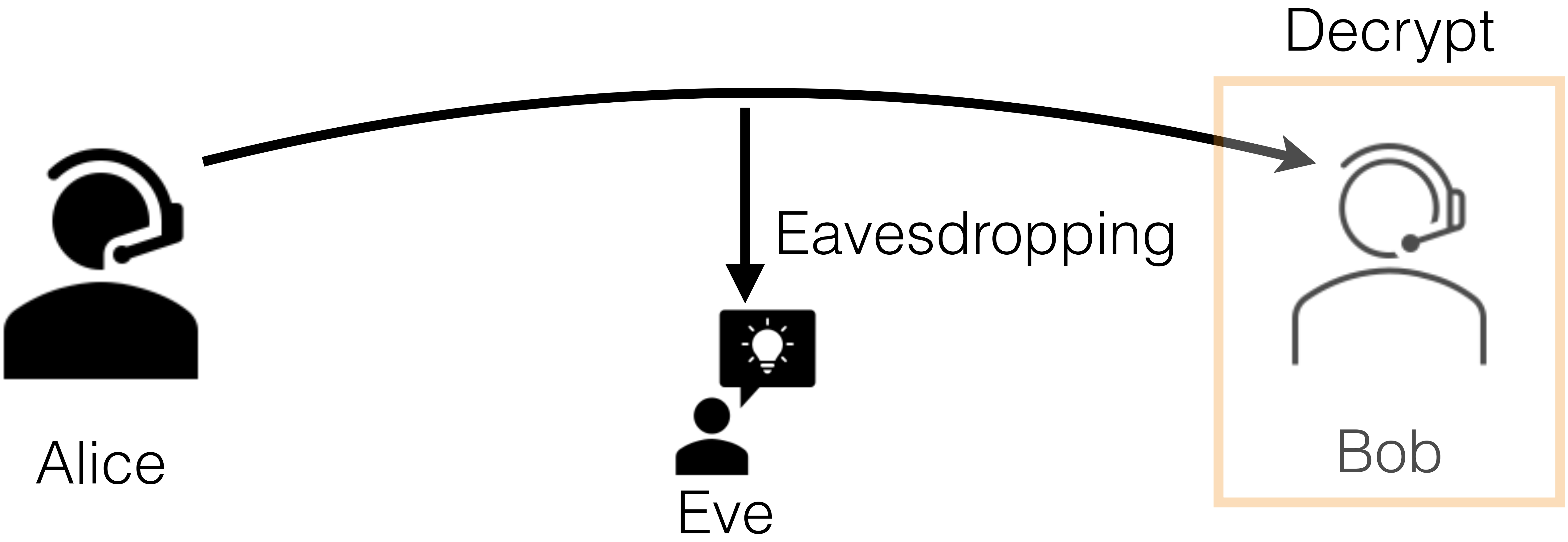
| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| G | O | K | E | A | N | Q | U | Y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

Math alive

Lgxu gtyra

# Old standards: substitution ciphers

To decrypt, go the other way!



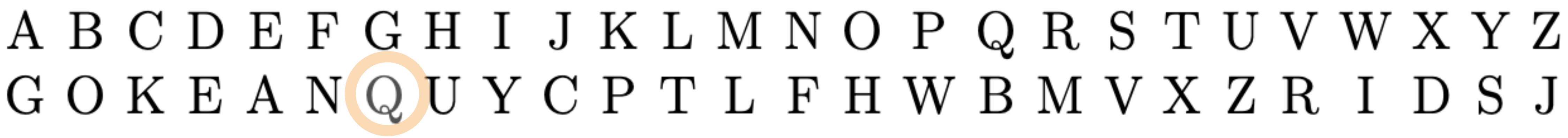
# Old standards: substitution ciphers

To decrypt, go the other way!

For example,

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

What does “QYMGNNAYVSATTHI” mean?



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

What does “QYMGNNAYVSATTHI” mean?

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

What does “QYMGNNAYVSATTHI” mean?

G

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

What does “QYMGNNAYVSATTHI” mean?

GI

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

What does “QYMGNNAYVSATTHI” mean?

GIR

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

What does “QYMGNNAYVSATTHI” mean?

GIRA

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

What does “QYMGNNAYVSATTHI” mean?

GIRAF

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

What does “QYMGNNAYVSATTHI” mean?

GIRAFF

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

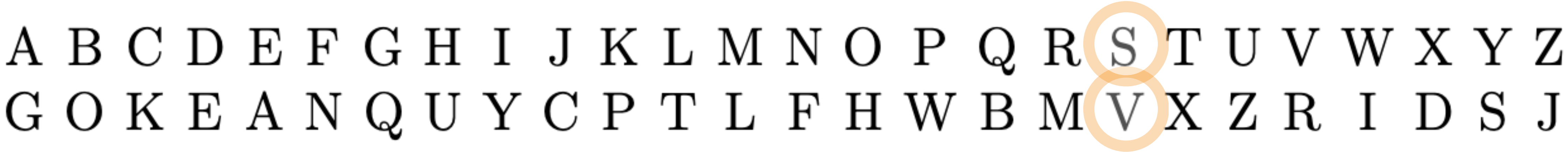
What does “QYMGNNAYVSATTHI” mean?

**GIRAFFE**

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

What does “QYMGNNAYVSATTHI” mean?

GIRAFFEI



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

What does “QYMGNNAYVSATTHI” mean?

GIRAFFEIS

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

What does “QYMGNNAYVSATTHI” mean?

GIRAFFEISY

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

What does “QYMGNNAYVSATTHI” mean?

GIRAFFEISYE

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

What does “QYMGNNAYVSATTHI” mean?

GIRAFFEISYEL

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

What does “QYMGNNAYVSATTHI” mean?

GIRAFFEISYELL

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

What does “QYMGNNAYVSATTHI” mean?

GIRAFFEISYELLO

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

What does “QYMGNNAYVSATTHI” mean?

GIRAFFEISYELLOW

# Special substitution cipher used by Julius Caesar

Caesar ciphers (circular shift of alphabets):

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | 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 |

Shift by one step

# Substitution cipher used by Julius Caesar

Caesar ciphers (circular shift of alphabets):

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | 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 |

Shift by one step

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 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 |

Shift by two steps

# Substitution cipher used by Julius Caesar

Caesar ciphers (circular shift of alphabets):

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | 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 |

Shift by one step

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 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 |

Shift by two steps

⋮

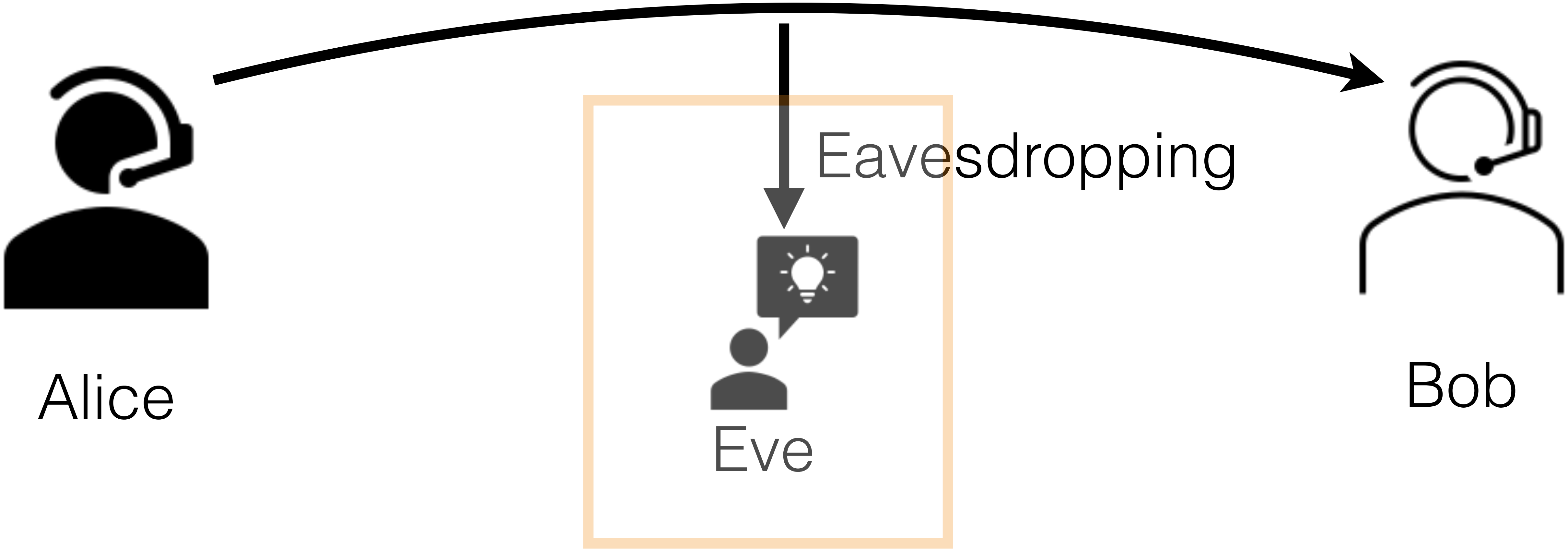
| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| Z | A | B | C | D | E | F | G | H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

Shift by 25 steps

We choose a value for the shift (the “key”) between 1 and 25 and get one cipher

**Example:** the following was encrypted with a Caesar cipher, but we do not know the key that was used. Decrypt it anyways!

```
nqpiecnewncvkqpu
```



**Example:** the following was encrypted with a Caesar cipher, but we do not know the key that was used. Decrypt it anyways!

nqpiecnewncvkqpu

Using shift 1 in the Caesar cipher:

mpohdbmdvmbujpot

**Example:** the following was encrypted with a Caesar cipher, but we do not know the key that was used. Decrypt it anyways!

nqpiecnewncvkqpu

Using shift 1 in the Caesar cipher:

mpohdbmdvmbujpot ✗

**Example:** the following was encrypted with a Caesar cipher, but we do not know the key that was used. Decrypt it anyways!

nqpiecnewncvkqpu

Using shift 1 in the Caesar cipher:

mpohdbmdvmbujpot ✗

Using shift 2 in the Caesar cipher:

longcalculations

**Example:** the following was encrypted with a Caesar cipher, but we do not know the key that was used. Decrypt it anyways!

nqpiecnewncvkqpu

Using shift 1 in the Caesar cipher:

mpohdbmdvmbujpot ✗

Using shift 2 in the Caesar cipher:

longcalculations ✓

**Brute force decryption:** try every possible key.

Feasible for Caesar cipher

**Brute force decryption:** try every possible key.

Feasible for Caesar cipher (25 possible keys),

**Brute force decryption:** try every possible key. Feasible for Caesar cipher (25 possible keys), but not for general substitution ciphers, since there are a total of

$$26 \cdot 25 \cdot \ldots \cdot 2 \cdot 1 \approx 4 \cdot 10^{26}$$

keys.

**Brute force decryption:** try every possible key. Feasible for Caesar cipher (25 possible keys), but not for general substitution ciphers, since there are a total of

$$26 \cdot 25 \cdot \ldots \cdot 2 \cdot 1 \approx 4 \cdot 10^{26}$$

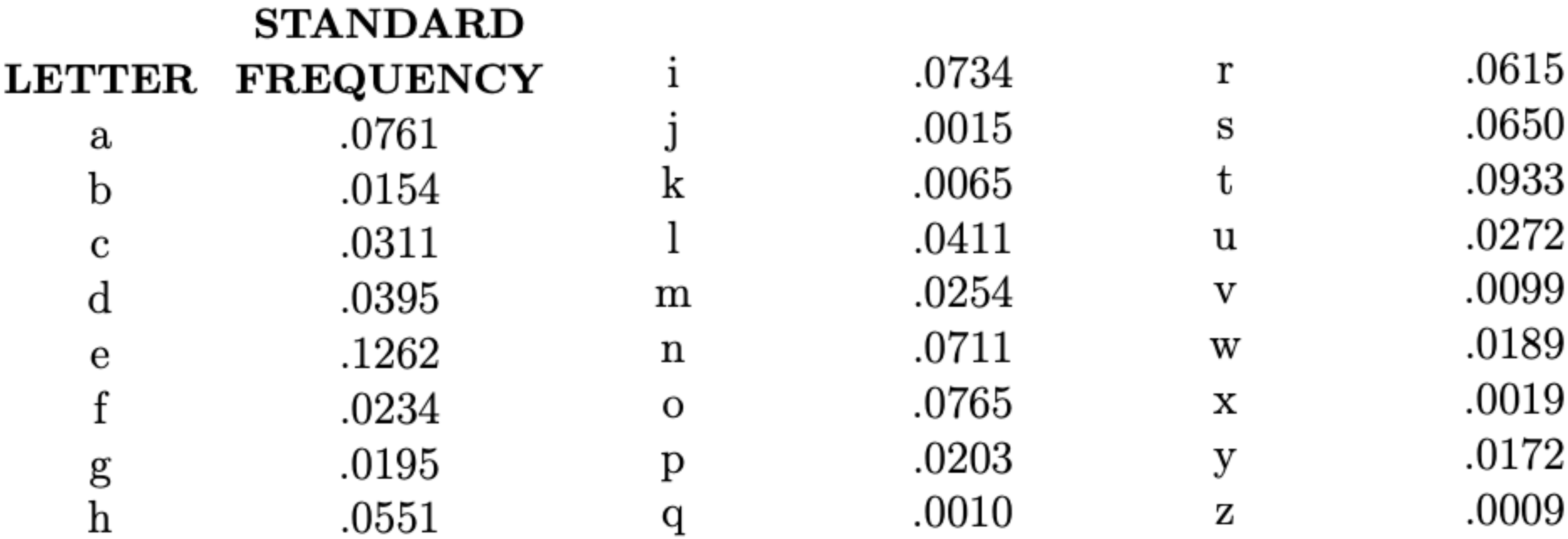
keys. Trying them all would take around 317 years on Earth's currently largest supercomputer.

zkbzkrphzkbihhwgrqwidlophqrzwdnhphwrbrxuilqlvkolqhrkpbkhduwlwe
uhdnvhyhubvwhswkdwlwdnhexwlpkrslqjwkdwwkhjdwhvwkhboowhoop
hwkdwbrxuhplqhzdonlqjwkurxjkwkhflwbvwuhhwvlvlwebplvwdnhrughv
ljqlihhovrdorqhrqdiulgdbqljkwfdqbrxpdnhlwihhoolnhkrphlilwhoobrxbrx
uhplqhlwvolnhlwrogbrxkrqhbgrqwpdnhphvdggrqwpdnhphfubvrphwlph
voryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjphodx
jkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwlphf
rphwdnhdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxol
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhb
rxdqglzhzhuheruqwrglhorvwexwqrzldpirxqglfdqvhhexwrqfhlzdveolqglz
dvvrfrqixvhgdvdolwwohfklogwulhgwrwdnhzkdwlfrxogjhwvfduhgwkdwlf
rxogqwilqgdoowkhdqvzhuvkrqhbgrqwpdnhphvdggrqwpdnhphfubvrphwl
phvoryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjpho
dxjkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwl
phfrphwdnhdzdonrqwkhzlogvlghfrphnlvvphkduglqwkhsrxulqjudlqbrxol
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhb
rxdqglzhzhuheruqwrglhzhzhuheruqwrglhzhzhuheruqwrglhfrphdqgwdn
hdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxolnhbrxuj
luovlqvdqhgrqwpdnhphvdggrqwpdnhphfubvrphwlphvoryhlvqrwhqrxjkd
qgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjphodxjkohwvjrjhwkljkwk
hurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwlphfrphwdnhdzdonrqw
khzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxolnhbrxujluovlqvdqh
fkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhbrxdqglzhzhuheruqwrg
lhzhzhuheruqwrglh

zkbzkrphzkbihhwgrqwidlophqrzwdnhphwrbrxuilqlvkolqhrkpbkhduwlwe
uhdnvhyhubvwhswkdwlwdnhexwlpkrslqjwkdwwkhjdwhvwkhboowhoop
hwkdwbrxuhplqhzdonlqjwkurxjkwkhflwbvwuhhwvlvlwebplvwdnhrughv
ljqlihhovrdorqhrqdiulgdbqljkwfdqbrxpdnhlwihhoolnhkrphlilwhoobrxbrx
uhplqhlwvolnhlwrogbrxkrqhbgrqwpdnhphvdggrqwpdnhphfubvrphwlph
voryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjphodx
jkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwlphf
rphwdnhdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxol
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhb
rxdqglzhzhuheruqwrglhorvwexwqrzldpirxqglfdqvhhexwrqfhlzdveolqglz
dvvrfrqixvhgdvdolwwohfklogwulhgwrwdnhzkdwlfrxogjhwvfduhgwkdwlf
rxogqwilqgdoowkhdqvzhuvkrqhbgrqwpdnhphvdggrqwpdnhphfubvrphwl
phvoryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjpho
dxjkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwl
phfrphwdnhdzdonrqwkhzlogvlghfrphnlvvphkduglqwkhsrxulqjudlqbrxol
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhb
rxdqglzhzhuheruqwrglhzhzhuheruqwrglhzhzhuheruqwrglhfrphdqgwdn
hdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxolnhbrxuj
luovlqvdqhgrqwpdnhphvdggrqwpdnhphfubvrphwlphvoryhlvqrwhqrxjkd
qgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjphodxjkohwvjrjhwkljkwk
hurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwlphfrphwdnhdzdonrqw
khzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxolnhbrxujluovlqvdqh
fkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhbrxdqglzhzhuheruqwrg
lhzhzhuheruqwrglh

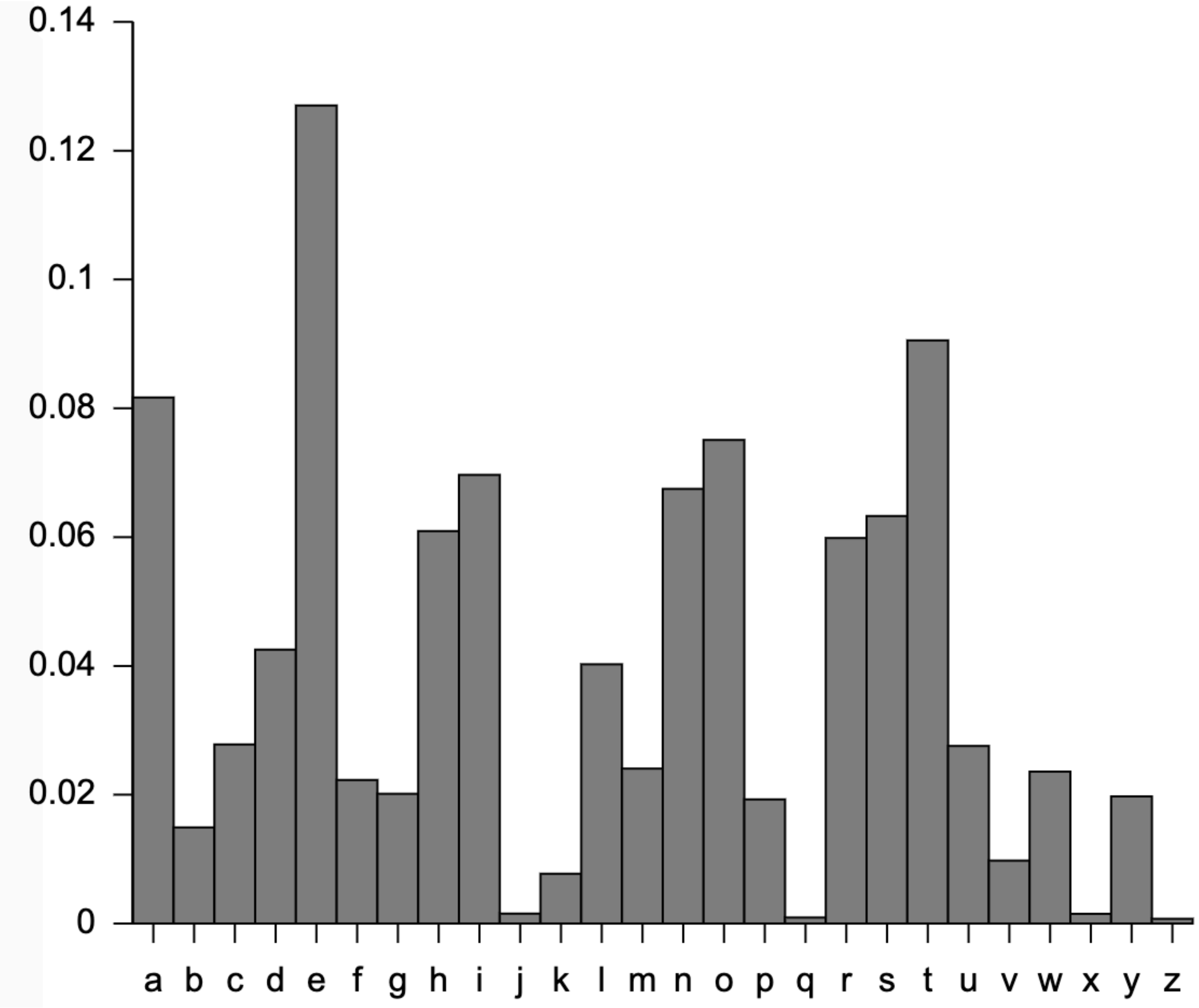
zkbzkrphzkbihhwgrqwidlophqrzwdnhphwrbrxuilqlvkolqhrkpbkhduwlwe
uhdnvhyhubvwhswkdwlwdnhexwlpkrslqjwkdwwkhjdwhvwkhboowhoop
hwkdwbrxuhplqhzdonlqjwkurxjkwkhflwbvwuhhwvlvlwebplvwdnhrughv
ljqlihhovrdorqhrqdiulgdbqljkwfdqbrxpdnhlwihhoolnhkrphlilwhoobrxbrx
uhplqhlwvolnhlwrogbrxkrqhbgrqwpdnhphvdggrqwpdnhphfubvrphwlph
voryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjphodx
jkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwlphf
rphwdnhdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxol
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhb
rxdqglzhzhuheruqwrglhorvwexwqrzldpirxqglfdqvhhexwrqfhlzdveolqglz
dvvrfrqixvhgdvdolwwohfklogwulhgwrwdnhzkdwlfrxogjhwvfduhgwkdwlf
rxogqwilqgdoowkhdqvzhuvkrqhbgrqwpdnhphvdggrqwpdnhphfubvrphwl
phvoryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjpho
dxjkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwl
phfrphwdnhdzdonrqwkhzlogvlghfrphnlvvphkduglqwkhsrxulqjudlqbrxol
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhb
rxdqglzhzhuheruqwrglhzhzhuheruqwrglhzhzhuheruqwrglhfrphdqgwdn
hdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxolnhbrxuj
luovlqvdqhgrqwpdnhphvdggrqwpdnhphfubvrphwlphvoryhlvqrwhqrxjkd
qgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjphodxjkohwvjrjhwkljkwk
hurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwlphfrphwdnhdzdonrqw
khzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxolnhbrxujluovlqvdqh
fkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhbrxdqglzhzhuheruqwrg
lhzhzhuheruqwrglh

If the language in which the plain text is written is known to the code-breaker, and if the messages contain a few sentences of text,



| LETTER | STANDARD FREQUENCY |
|---|---|
| a | .0761 |
| b | .0154 |
| c | .0311 |
| d | .0395 |
| e | .1262 |
| f | .0234 |
| g | .0195 |
| h | .0551 |
| i | .0734 |
| j | .0015 |
| k | .0065 |
| l | .0411 |
| m | .0254 |
| n | .0711 |
| o | .0765 |
| p | .0203 |
| q | .0010 |
| r | .0615 |
| s | .0650 |
| t | .0933 |
| u | .0272 |
| v | .0099 |
| w | .0189 |
| x | .0019 |
| y | .0172 |
| z | .0009 |

If the language in which the plain text is written is known sages contair



**ST**

**LETTER** **FR**

a
b
c
d
e
f
g
h

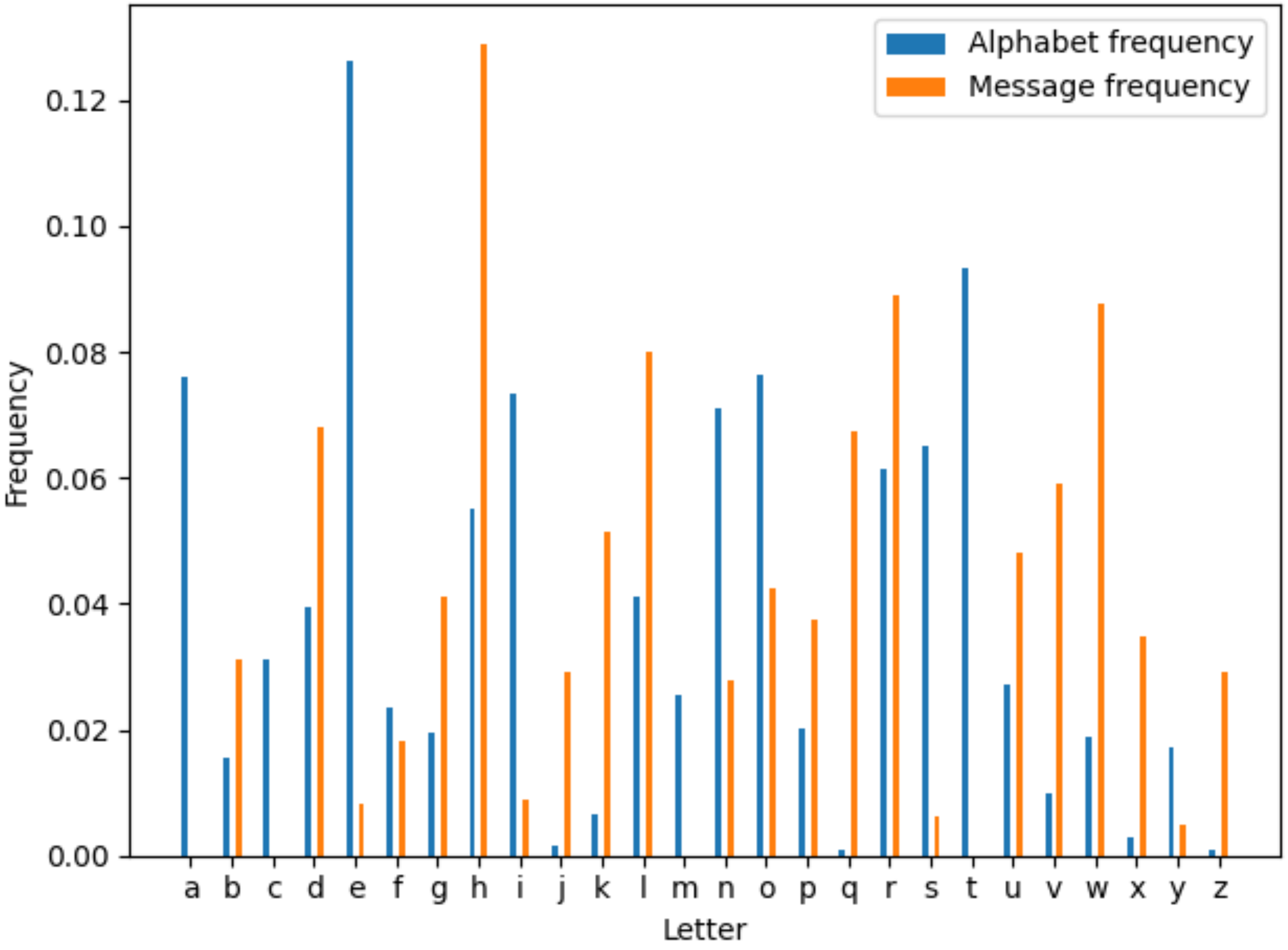
.0615
.0650
.0933
.0272
.0099
.0189
.0019
.0172
.0009

# Decryption example using frequency analysis:

zkbzkrphzkbihhwgrqwidlophqrzwdnhphwrbrxuilqlvkolqhrkpbkhduwlwe
uhdnvhyhubvwhswkdwlwdnhexwlpkrslqjwkdwwkhjdwhvwkhboowhoop
hwkdwbrxuhplqhzdonlqjwkurxjkwkhflwbvwuhhwvlvlwebplvwdnhrughv
ljqlihhovrdorqhrqdiulgdbqljkwfdqbrxpdnhlwihhoolnhkrphlilwhoobrxbrx
uhplqhlwvolnhlwrogbrxkrqhbgrqwpdnhphvdggrqwpdnhphfubvrphwlph
voryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjphodx
jkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwlphf
rphwdnhdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxol
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhb
rxdqglzhzhuheruqwrglhorvwexwqrzldpirxqglfdqvhhexwrqfhlzdveolqglz
dvvrfrqixvhgdvdolwwohfklogwulhgwrwdnhzkdwlfrxogjhwvfduhgwkdwlf
rxogqwilqgdoowkhdqvzhuvkrqhbgrqwpdnhphvdggrqwpdnhphfubvrphwl
phvoryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjpho
dxjkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwl
phfrphwdnhdzdonrqwkhzlogvlghfrphnlvvphkduglqwkhsrxulqjudlqbrxol
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhb
rxdqglzhzhuheruqwrglhzhzhuheruqwrglhzhzhuheruqwrglhfrphdqgwdn
hdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxolnhbrxuj
luovlqvdqhgrqwpdnhphvdggrqwpdnhphfubvrphwlphvoryhlvqrwhqrxjkd
qgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjphodxjkohwvjrjhwkljkwk
hurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwlphfrphwdnhdzdonrqw
khzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxolnhbrxujluovlqvdqh
fkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhbrxdqglzhzhuheruqwrg
lhzhzhuheruqwrglh

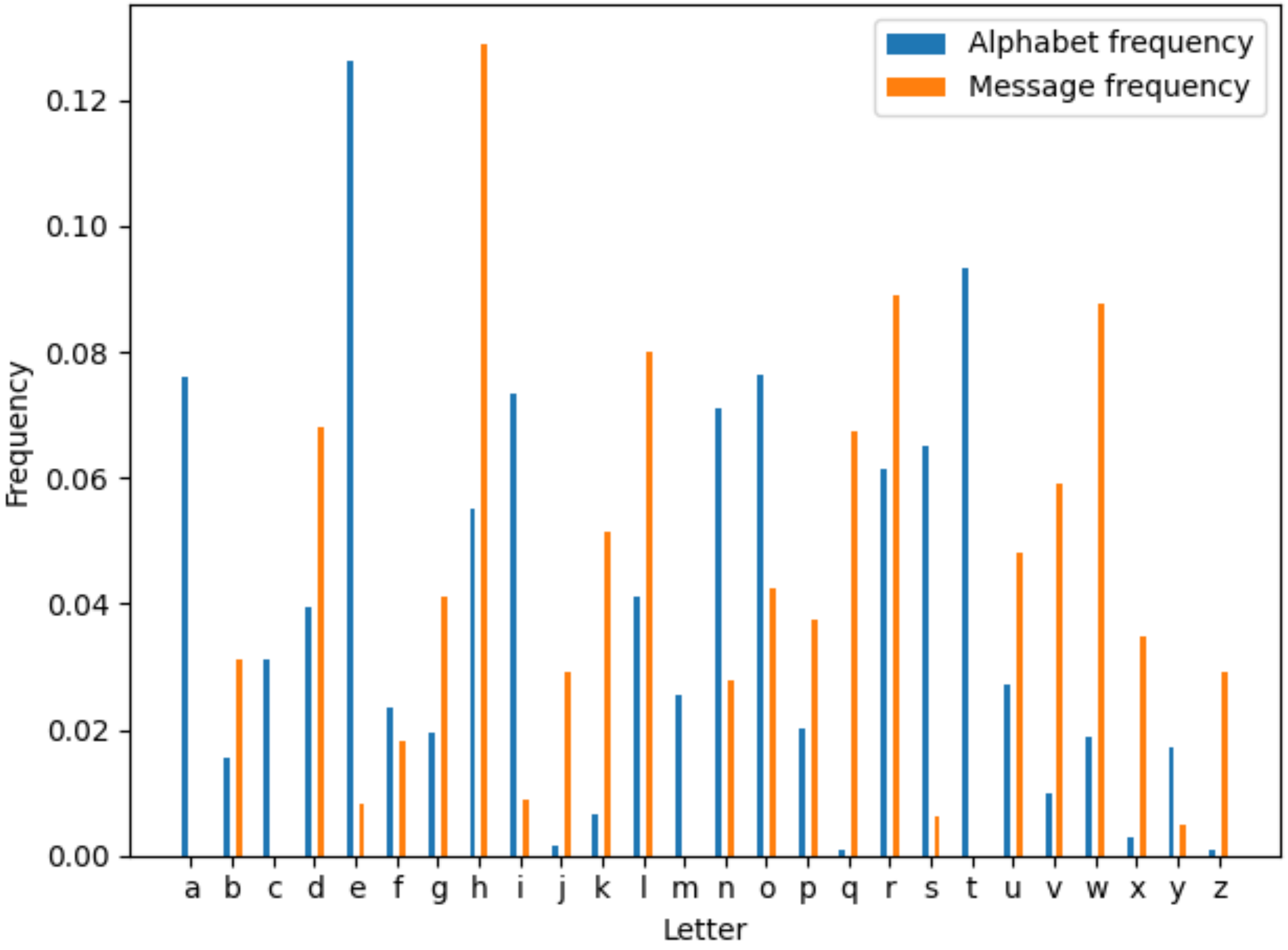
# Decryption example using frequency analysis:

zkbzkrphzkbihhwgrqwidlophqrzwdnhphwrbrxuilqlvkolqhrkp
uhdnvhyhubvwhswkdwlwdnhexwlpkrslqjwkdwwkhjdwhvwkh
hwkdwbrxuhplqhzdonlqjwkurxjkwkhflwbvwuhhwvlvlwebplvv
ljqlihhovrdorqhrqdiulgdbqljkwfdqbrxpdnhlwihhoolnhkrphlilw
uhplqhlwvolnhlwrogbrxkrqhbgrqwpdnhphvdggrqwpdnhphful
voryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhsp
jkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlqwkh
rphwdnhdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxulq
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvww
rxdqglzhzhuheruqwrglhorvwexwqrzldpirxqglfdqvhhexwrqfh
dvvrfrqixvhgdvdolwwohfklogwulhgwrwdnhzkdwlfrxogjhwvfd
rxogqwilqgdoowkhdqvzhuvkrqhbgrqwpdnhphvdggrqwpdnhph
phvoryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnhh
dxjkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlqw
phfrphwdnhdzdonrqwkhzlogvlghfrphnlvvphkduglqwkhsrxulq
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvww
rxdqglzhzhuheruqwrglhzhzhuheruqwrglhzhzhuheruqwrglhfr
hdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbr
luovlqvdqhgrqwpdnhphvdggrqwpdnhphfubvrphwlphvoryhlvq
qgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjphodxjkohwvj
hurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwlphfrphwdn
khzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxolnhbrxuj
fkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhbrxdqglzhzh
lhzhzhuheruqwrglh



# Decryption example using frequency analysis:

zkbzkrphzkbihhwgrqwidlophqrzwdnhphwrbrxuilqlvkolqhrkp
uhdnvhyhubvwhswkdwlwdnhexwlpkrslqjwkdwwkhjdwhvwk
hwkdwbrxuhplqhzdonlqjwkurxjkwkhflwbvwuhhwvlvlwebplv
ljqlihhovrdorqhrqdiulgdbqljkwfdqbrxpdnhlwihhoolnhkrphlilw
uhplqhlwvolnhlwrogbrxkrqhbgrqwpdnhphvdggrqwpdnhphfu
voryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhs
jkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlqwk
rphwdnhdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxul
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvww
rxdqglzhzhuheruqwrglhorvwexwqrzldpirxqglfdqvhhexwrqfh
dvvrfrqixvhgdvdolwwohfklogwulhgwrwdnhzkdwlfrxogjhwvf
rxogqwilqgdoowkhdqvzhuvkrqhbgrqwpdnhphvdggrqwpdnhp
phvoryhlvqrwhqrxjkdqgwkhurdgjhwvwrxjklgrqwnqrzzkbnh
dxjkohwvjrjhwkljkwkhurdglvorqjzhfduubrqwubwrkdyhixqlq
phfrphwdnhdzdonrqwkhzlogvlghfrphnlvvphkduglqwkhsrxul
nhbrxujluovlqvdqhvrfkrrvhbrxuodvwzrugvwklvlvwkhodvww
rxdqglzhzhuheruqwrglhzhzhuheruqwrglhzhzhuheruqwrglhf
hdzdonrqwkhzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbr
luovlqvdqhgrqwpdnhphvdggrqwpdnhphfubvrphwlphvoryhlv
qgwkhurdgjhwvwrxjklgrqwnqrzzkbnhhspdnlqjphodxjkohwvj
hurdglvorqjzhfduubrqwubwrkdyhixqlqwkhphdqwlphfrphwdn
khzlogvlghohwphnlvvbrxkduglqwkhsrxulqjudlqbrxolnhbrxuj
fkrrvhbrxuodvwzrugvwklvlvwkhodvwwlphfdxvhbrxdqglzhz
lhzhzhuheruqwrglh



whywhomewhyfeetdontfailmenowtakemetoyourfinishlineohmyheartitbreakseverystepthatitake...
— Lana Del Rey

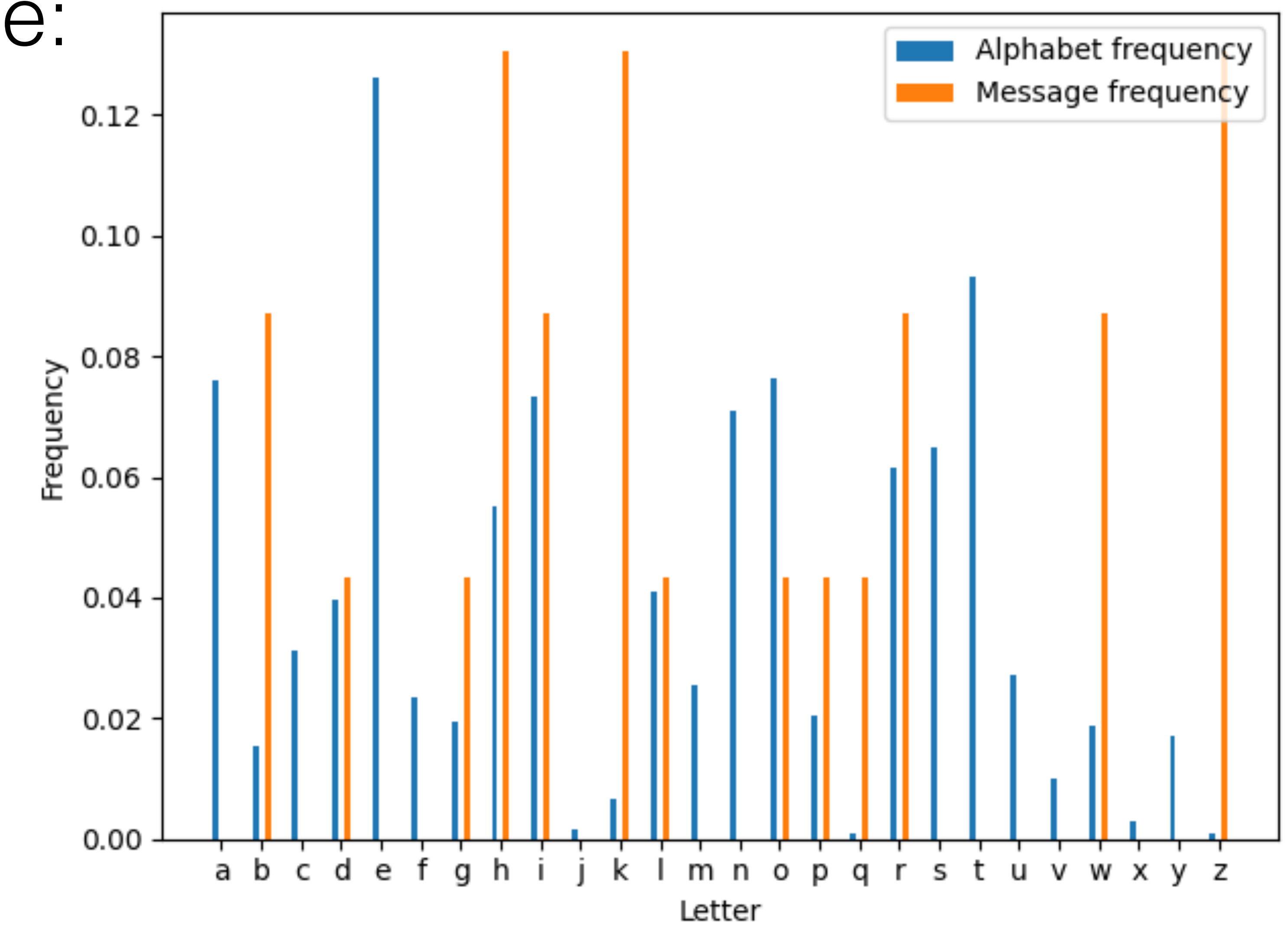
# Decryption example using frequency analysis:

The first part of the message:

zkbzkrphzkbihhwgrqwidlo

"decrypts" to:

etoetihaetonaasridsnlcu



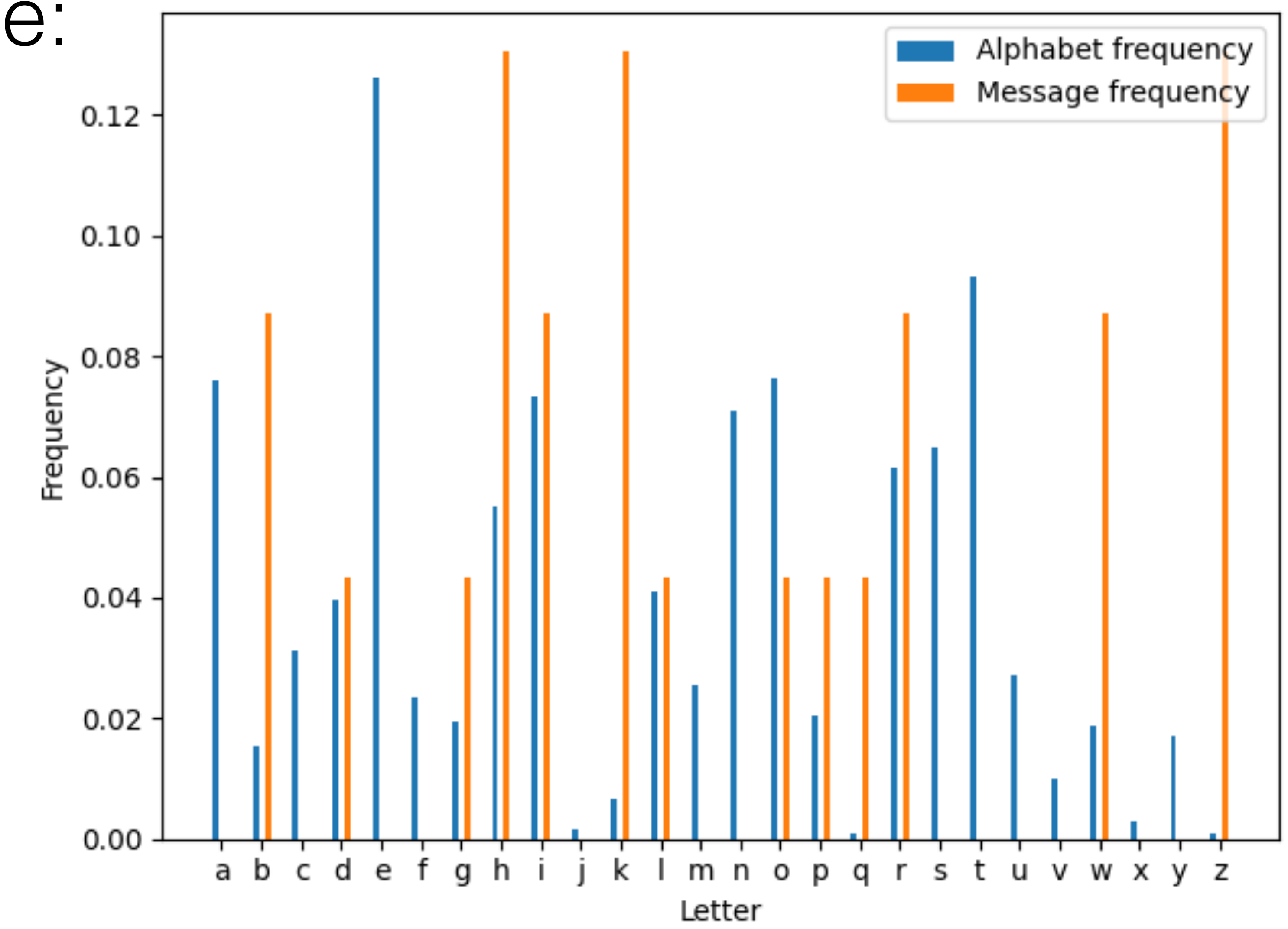
# Decryption example using frequency analysis:

The first part of the message:

zkbzkrphzkbihhwgrqwidlo

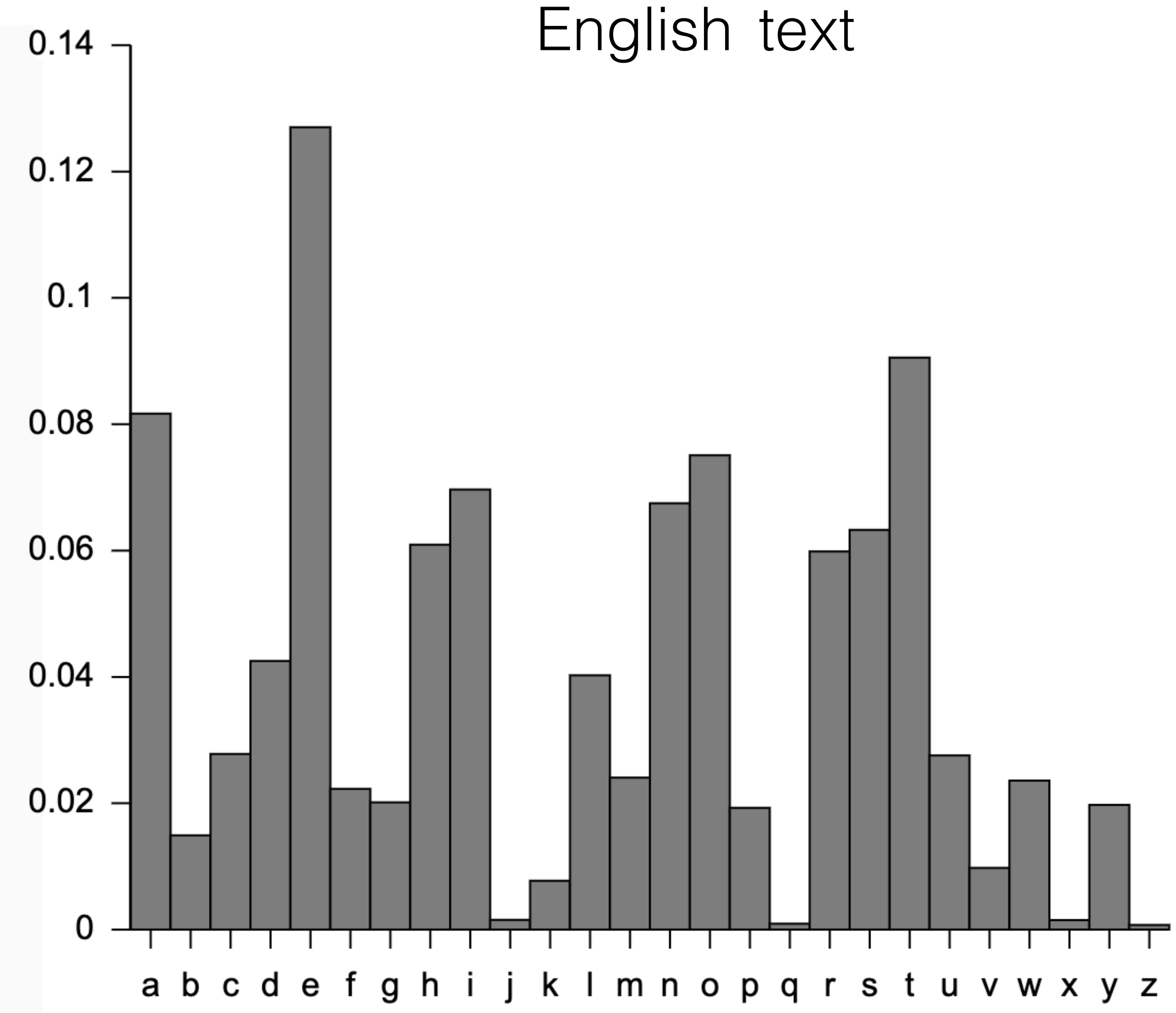
“decrypts” to:

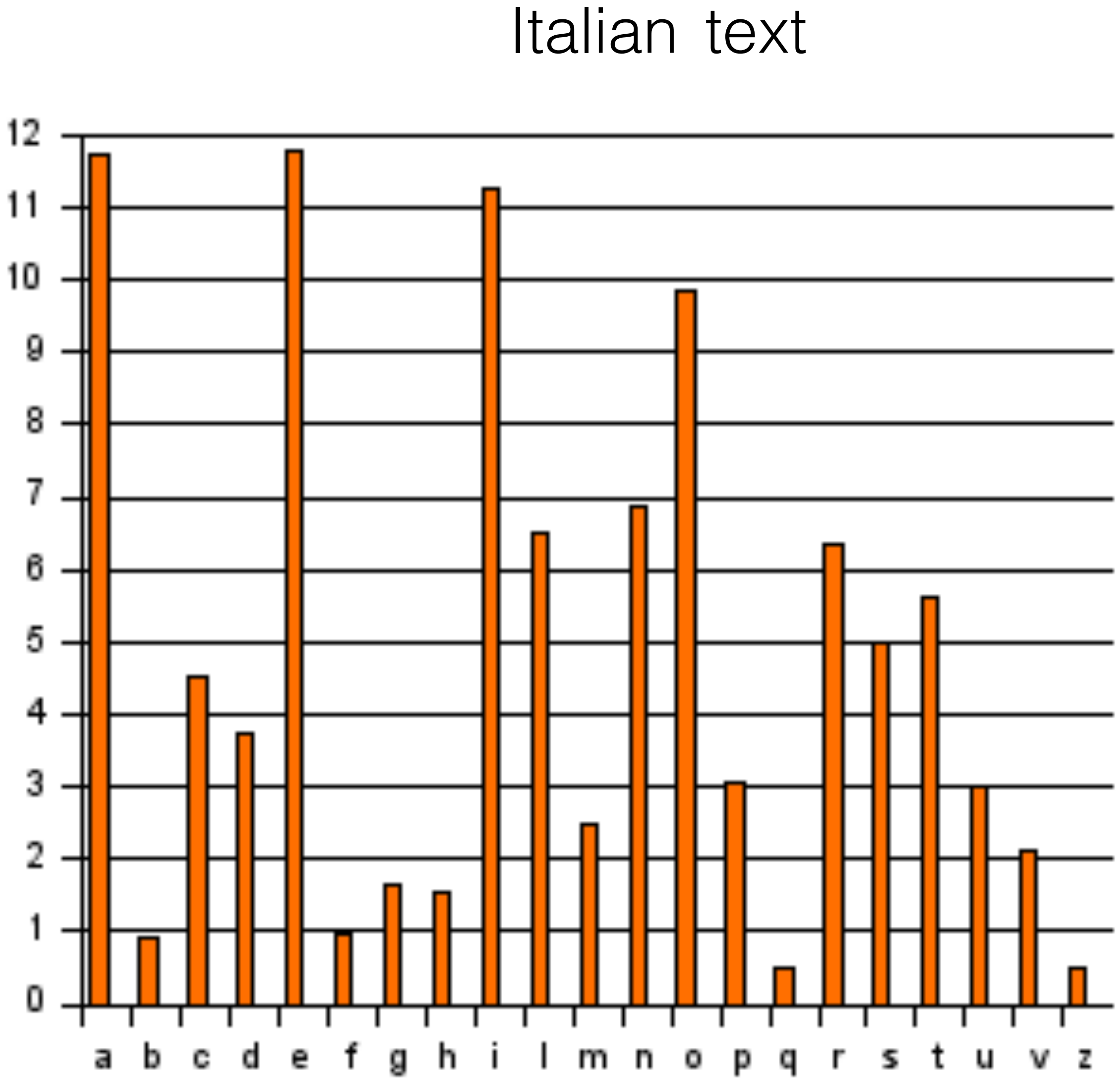
etoetihaetonaasridsnlcu



Does not work when message is too short!

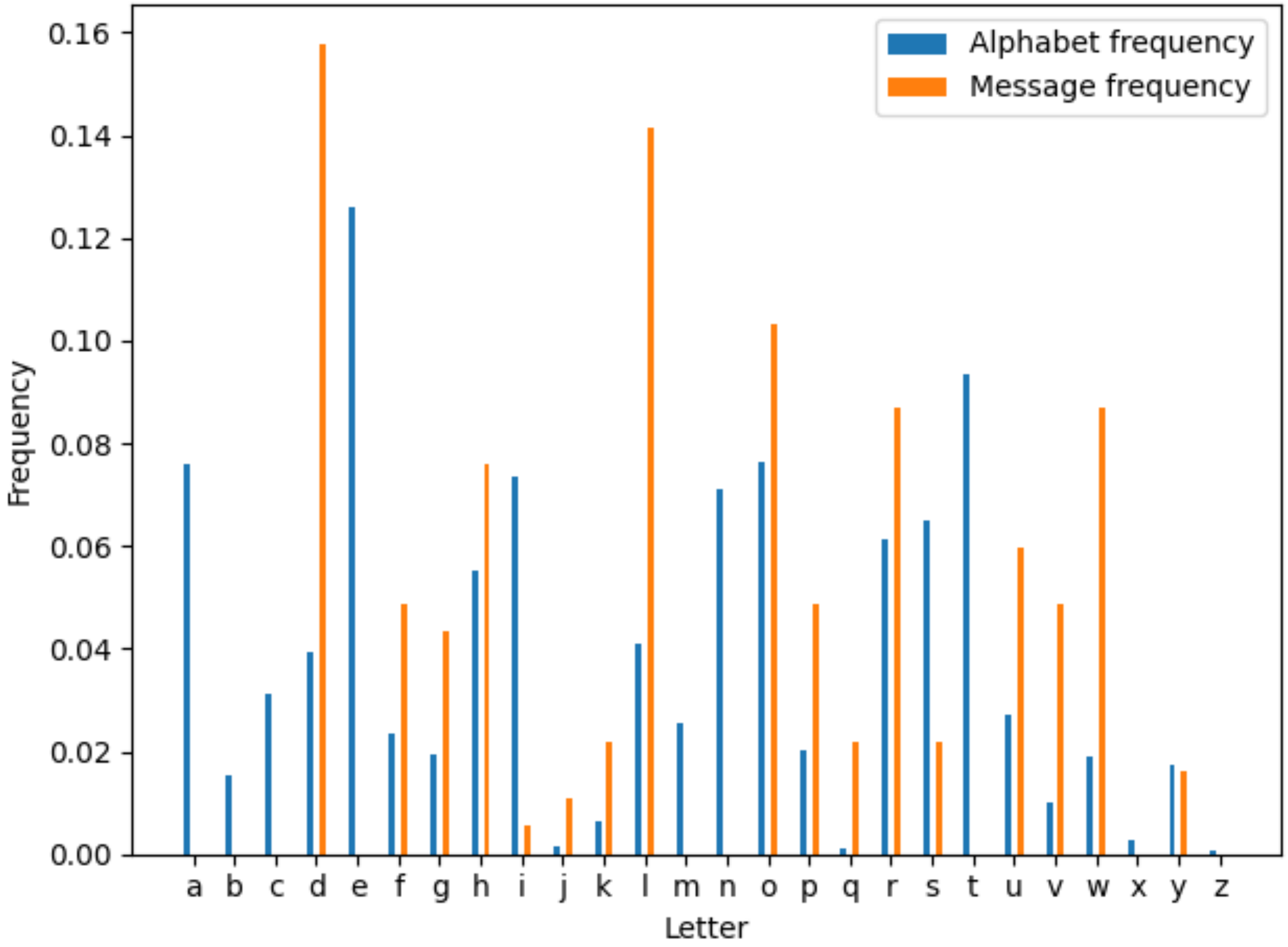
# Decryption example using frequency analysis:



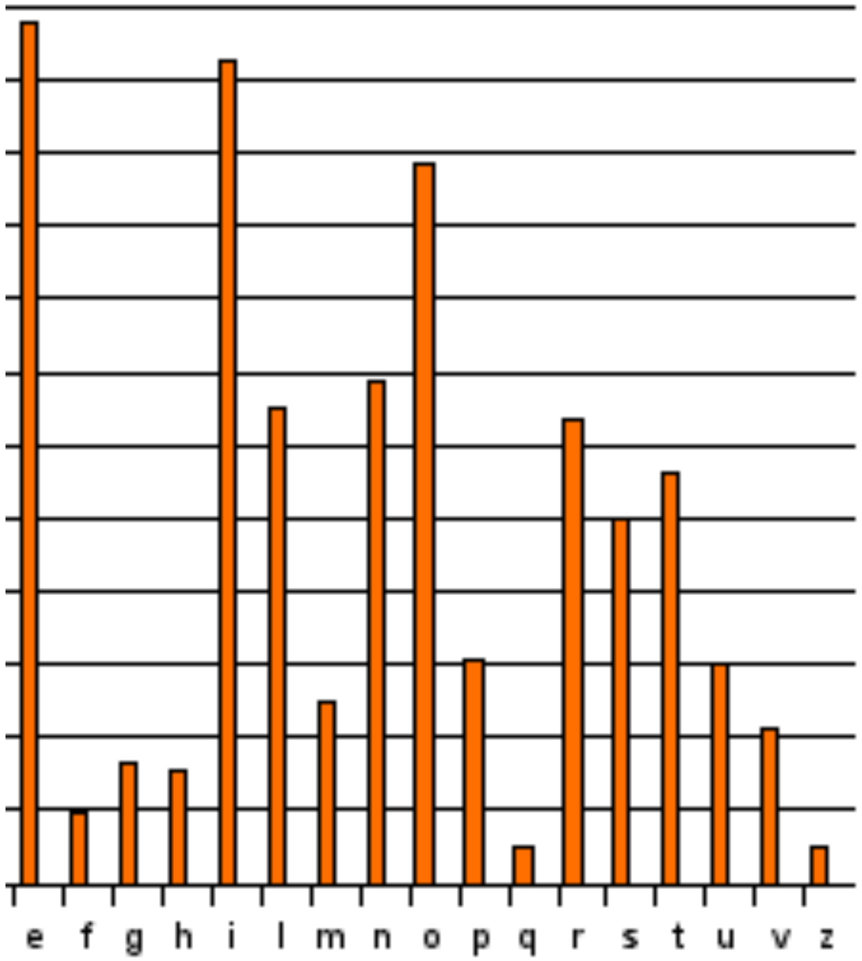


https://commons.wikimedia.org/wiki/File:Frequenze-alf_it.png

# Decryption example using frequency analysis:



Italian text



https://commons.wikimedia.org/wiki/File:Frequenze-alf_it.png

Does not work if message is in the wrong language!