# Lecture 1 – Introduction to cryptography

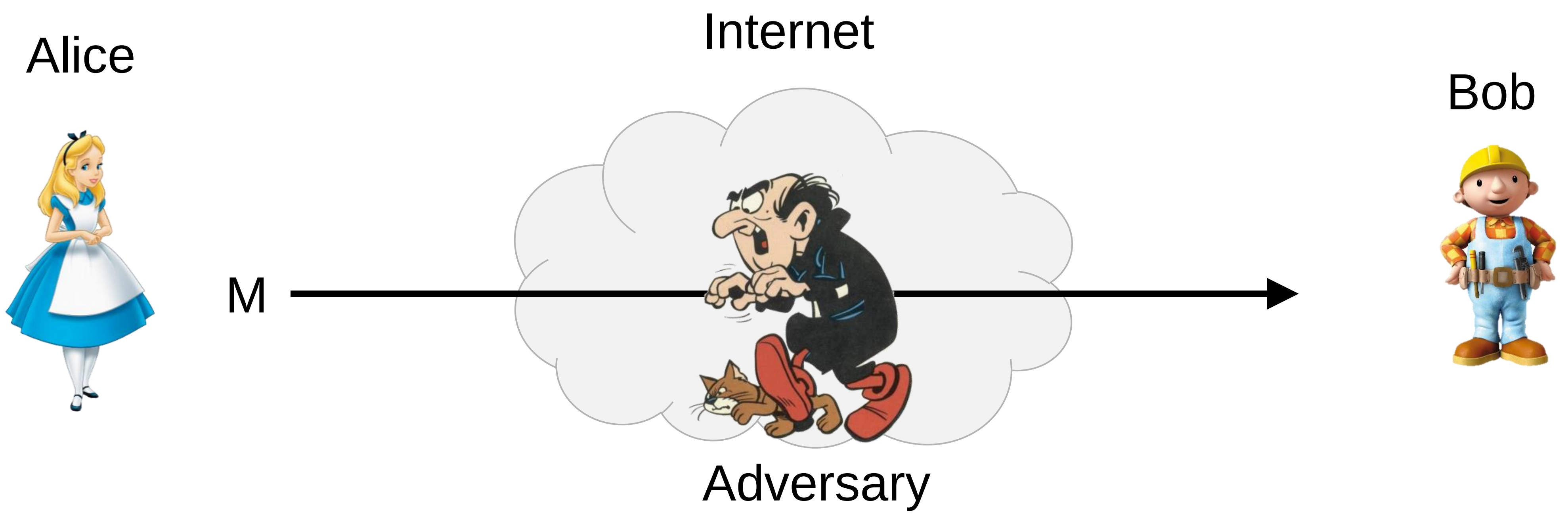
**TEK4500**

25.08.2021

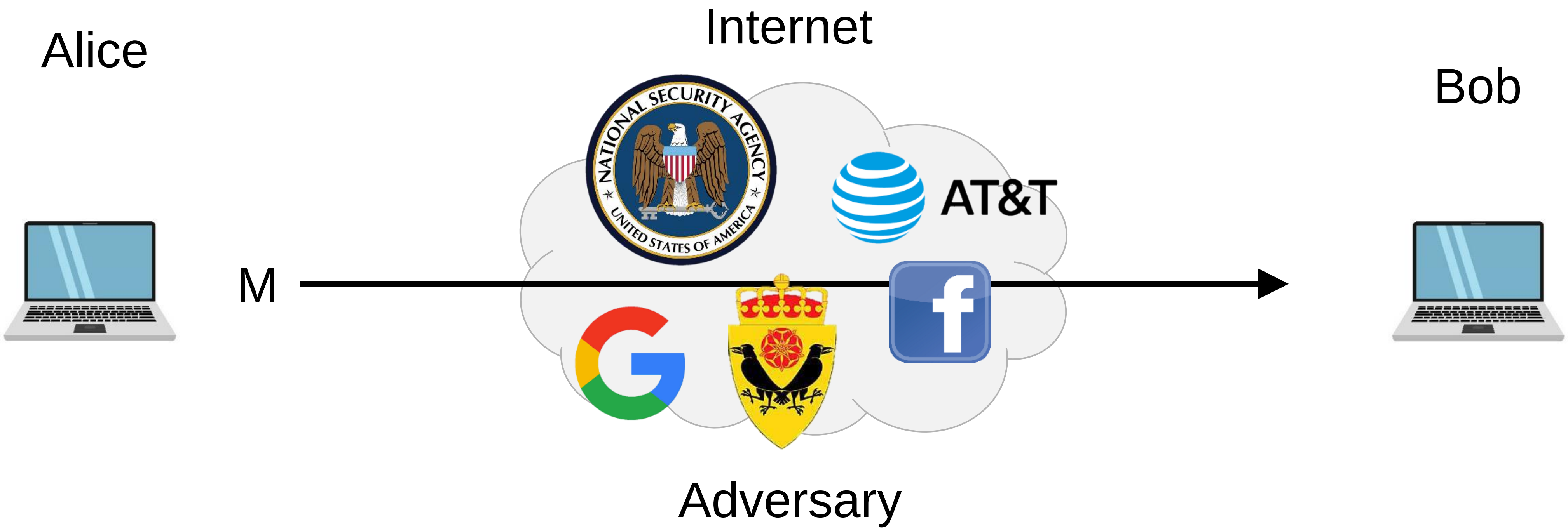
Håkon Jacobsen

hakon.jacobsen@its.uio.no

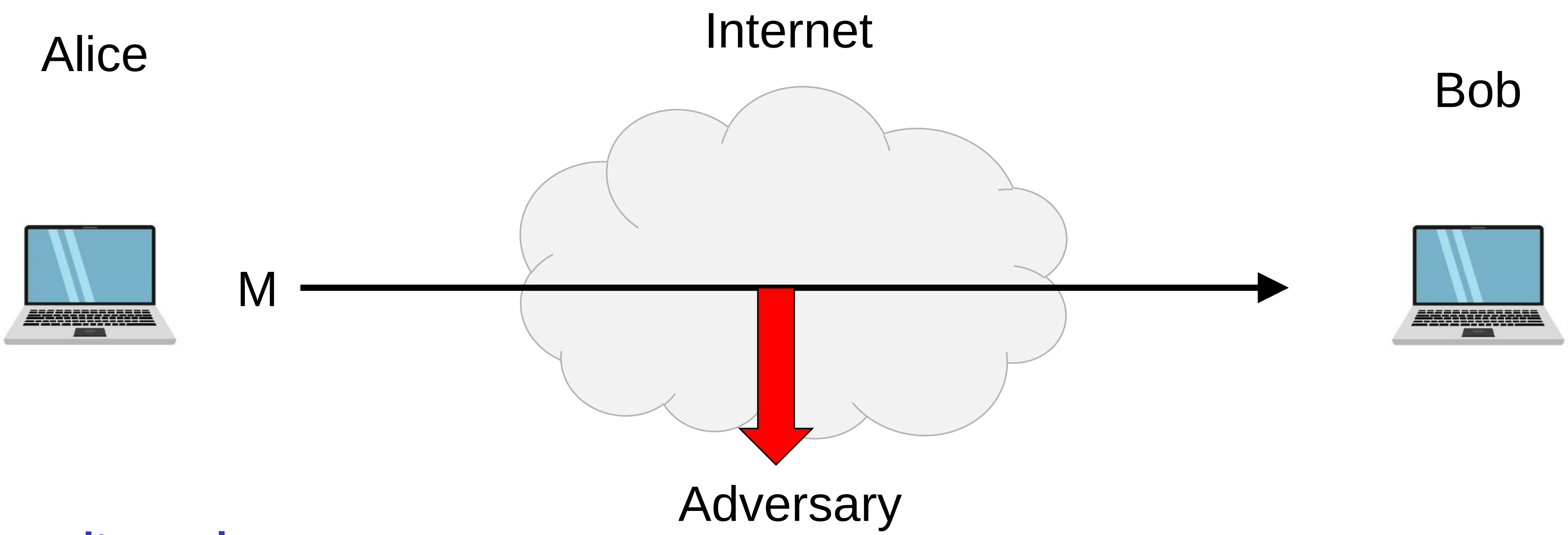
# What is cryptography?



# What is cryptography?



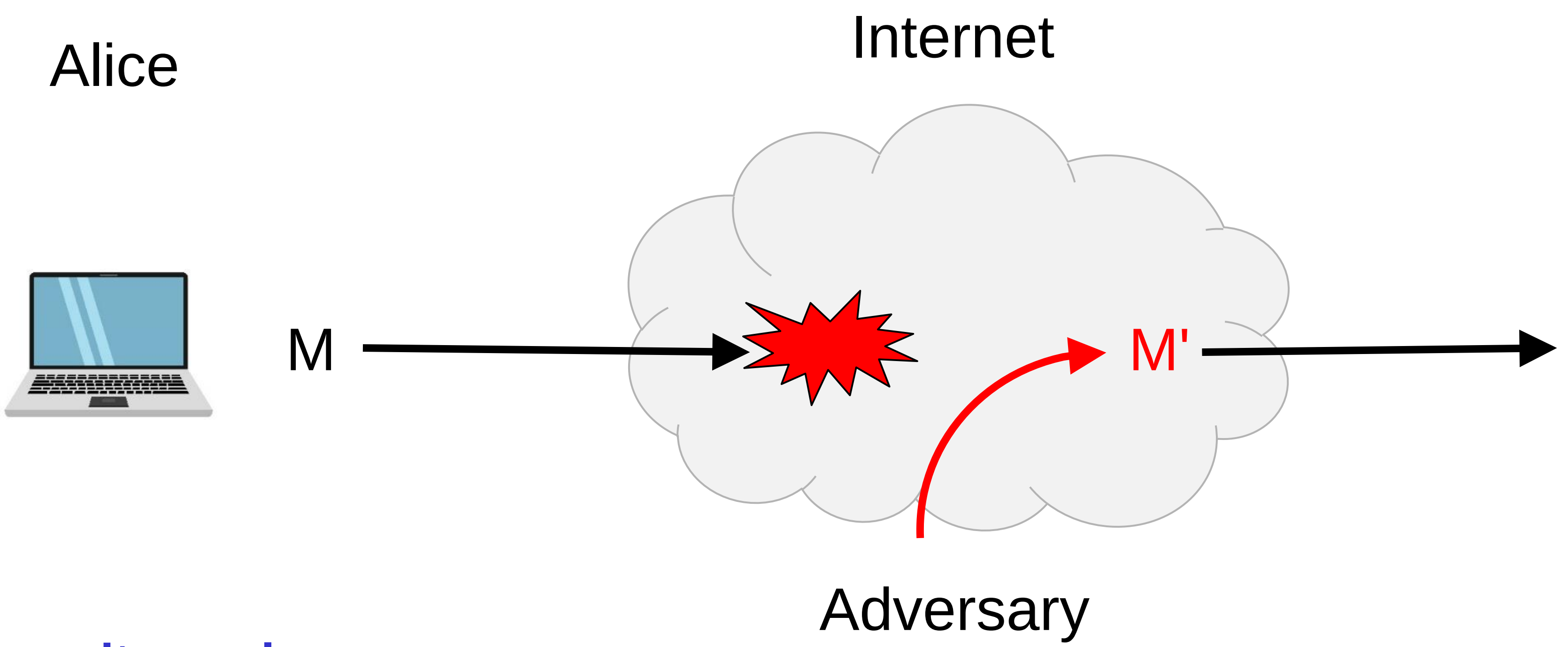
# What is cryptography?




**Security goals:**

- **Data privacy:** adversary should not be able to read message M

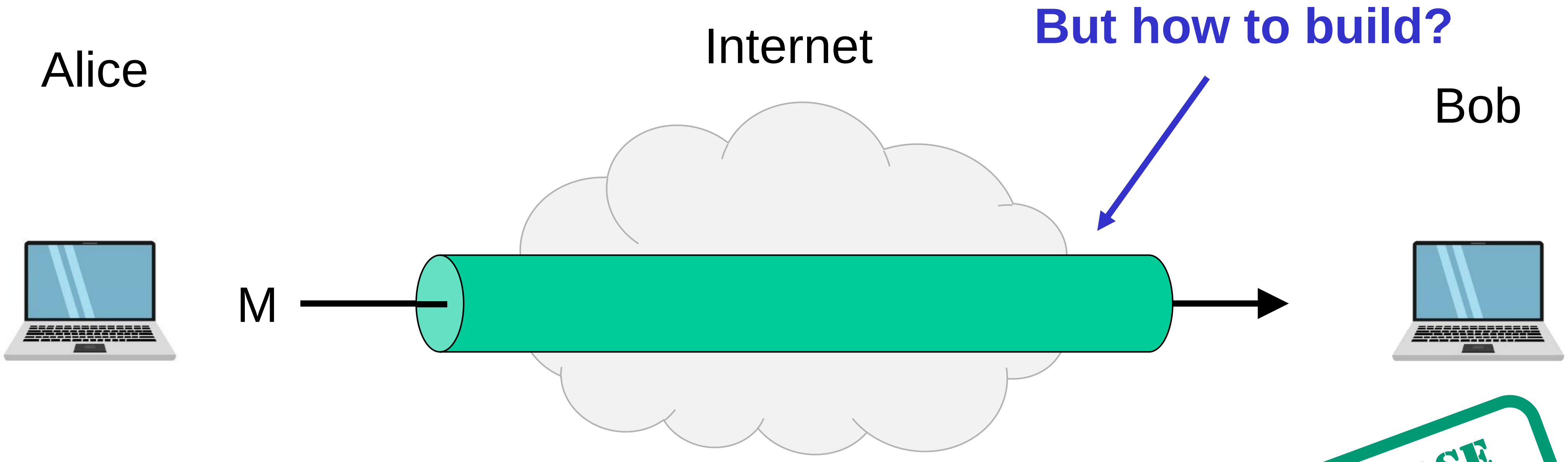
# What is cryptography?




**Security goals:**

- **Data privacy:** adversary should not be able to read message M
- **Data integrity:** adversary should not be able to modify message M
- **Data authenticity:** message M really originated from Alice

# Ideal solution: secure channels

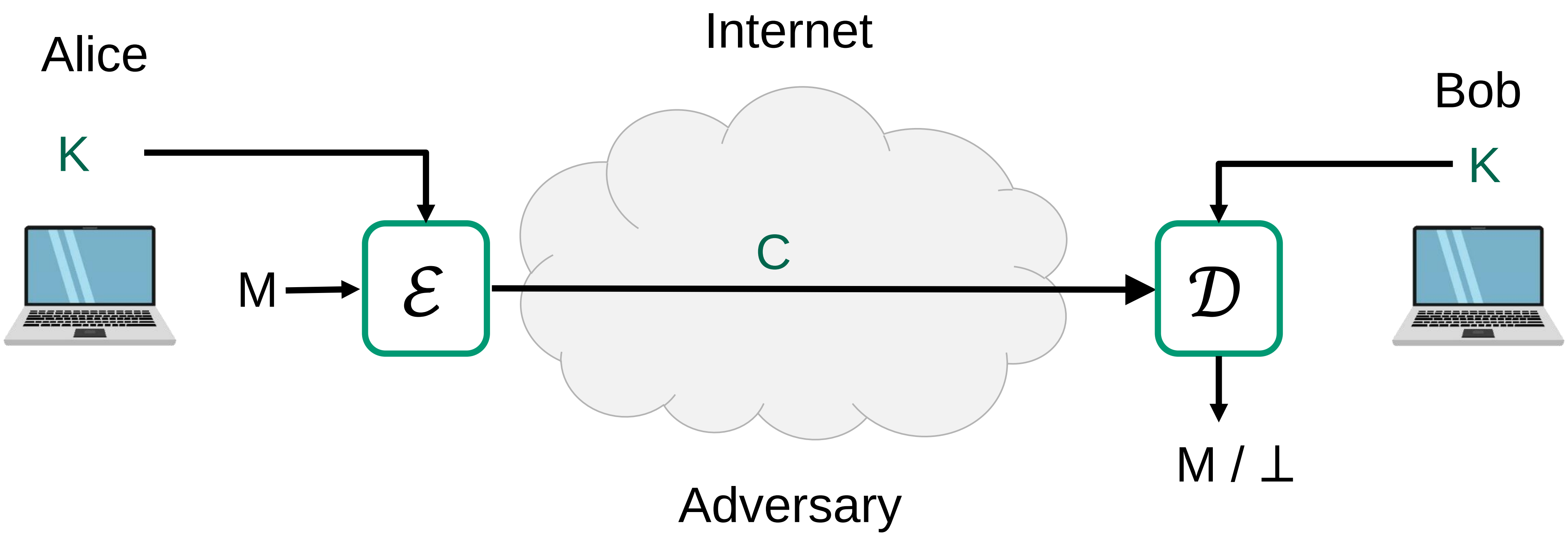




**Security goals:**

- **Data privacy:** adversary should not be able to read message M ✓
- **Data integrity:** adversary should not be able to modify message M ✓
- **Data authenticity:** message M really originated from Alice ✓

# Creating secure channels: encryption schemes

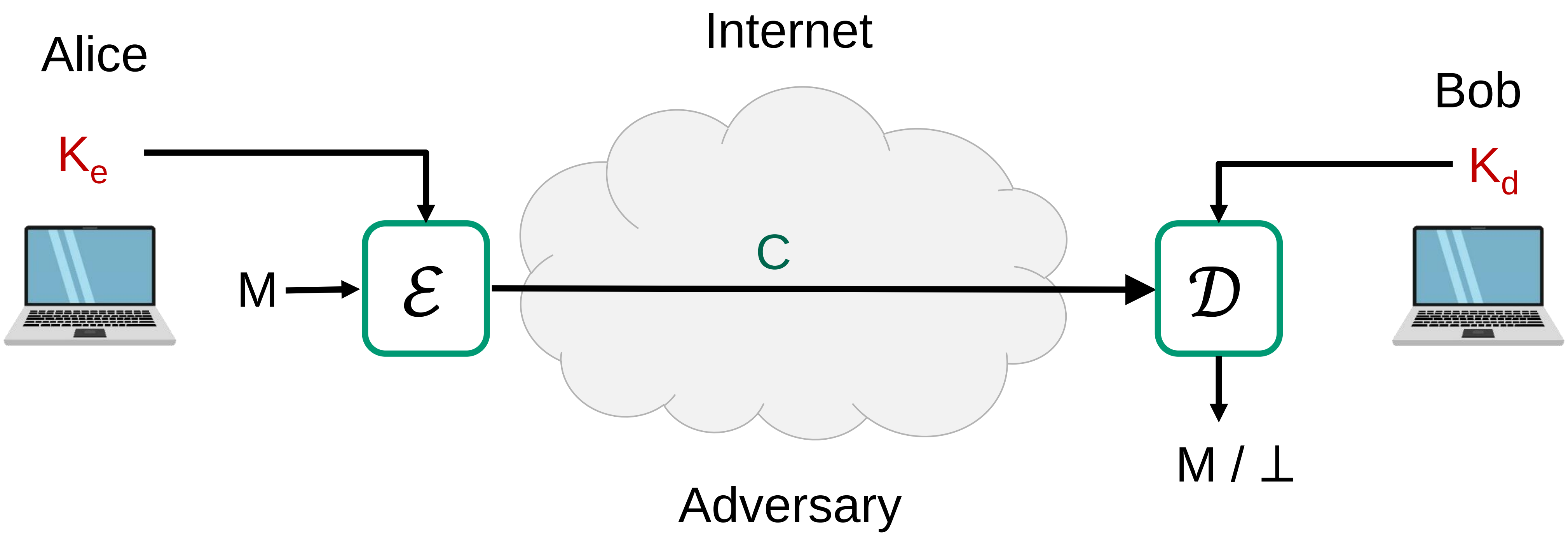



$\mathcal{E}$ **:** encryption algorithm (public)

**K :** encryption / decryption key (secret)

$\mathcal{D}$ **:** decryption algorithm (public)

# Creating secure channels: encryption schemes

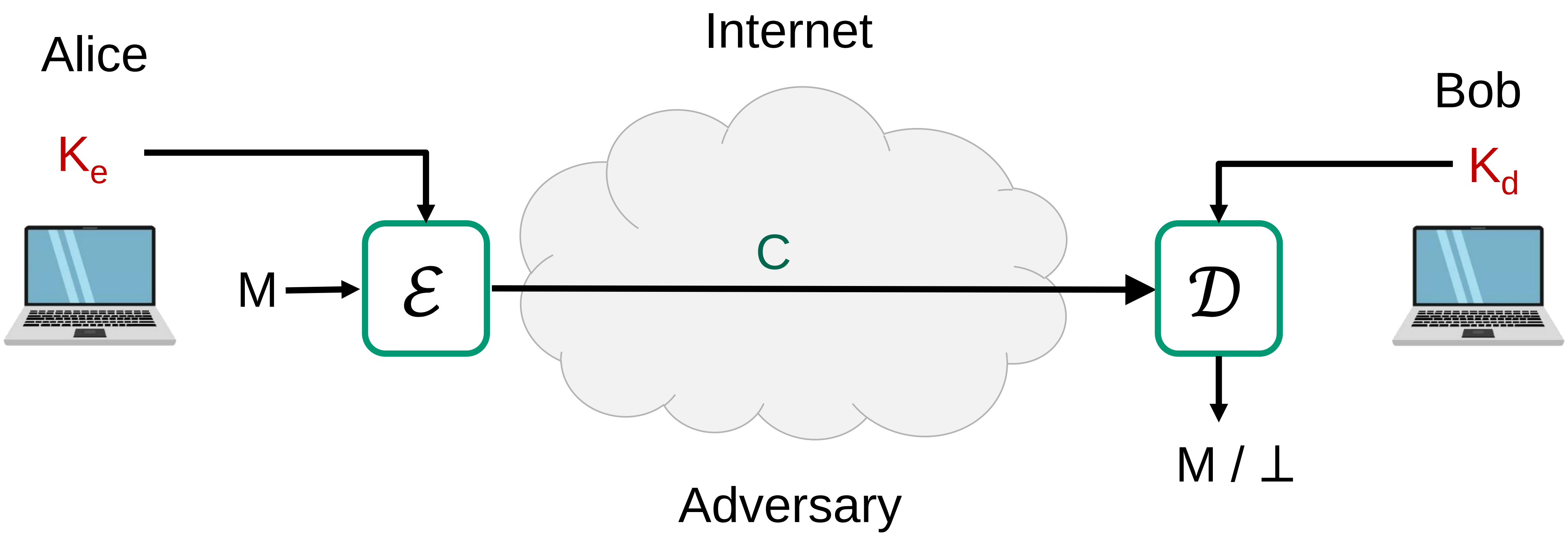



$\mathcal{E}$ **:** encryption algorithm (public)

$\mathcal{D}$ **:** decryption algorithm (public)

**K :** encryption / decryption key (secret)

# Creating secure channels: encryption schemes




$\mathcal{E}$ **:** encryption algorithm (public)

$\mathcal{D}$ **:** decryption algorithm (public)

$\mathbf{K_e}$ **:** encryption key (public)

$\mathbf{K_d}$ **:** decryption key (secret)

# Basic goals of cryptography

| | Message privacy | Message integrity / authentication |
|---|---|---|
| **Symmetric keys** | Symmetric encryption | Message authentication codes (MAC) |
| **Asymmetric keys** | Asymmetric encryption (a.k.a. public-key encryption) | Digital signatures |

# Basic goals of cryptography

| | **Message privacy** | **Message integrity / authentication** |
|---|---|---|
| **Symmetric keys** | Symmetric encryption | Message authentication codes (MAC) |
| **Asymmetric keys** | Asymmetric encryption (a.k.a. public-key encryption) | Digital signatures |

# Some notation

- $\in$ – "element in"
  - $3 \in \{1,2,3,4,5\}$
  - $7 \notin \{1,2,3,4,5\}$
- $\{0,1\}^n$ – set of all bitstrings of length $n$
  - $011 \in \{0,1\}^3$
  - $011 \notin \{0,1\}^5$
- $\{0,1\}^*$ – set of all bitstrings of *finite* length
  - $1, 1001, 10, 10001101000001 \in \{0,1\}^*$
- $F : \mathcal{X} \to \mathcal{Y}$ – function from set $\mathcal{X}$ to set $\mathcal{Y}$
  - $F : \{0,1\}^5 \to \{0,1\}^3$
  - $G : \{A, B, C, D\} \to \{0,1,2, \ldots\}$

- $\forall$ – "for all"
  - "$\forall X \in \{0,1\}^4$ … " = "for all bitstrings of length 4…"
- $\exists$ – "there exists"
  - "$\exists X \in \{0,1,2, \ldots\}$ such that $X > 13$"
- $\mathcal{X} \times \mathcal{Y}$ – set of pairs $(X, Y)$ with $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$
- $X \leftarrow 5$ – "assign value 5 to $X$"
- $X \stackrel{\$}{\leftarrow} \mathcal{X}$ – "assign $X$ a *random* value from set $\mathcal{X}$"

…**independent**, and **uniformly** distributed…

# Symmetric encryption – syntax

$\Pi = (\mathcal{E}, \mathcal{D})$

$\mathcal{E} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$

$\mathcal{E}(K, M) = \mathcal{E}_K(M) = C$

$\mathcal{D}: \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$

$\mathcal{D}(K, C) = \mathcal{D}_K(C) = M$

**Examples:**

| | | |
|---|---|---|
| $\mathcal{K} = \{0,1\}^{128}$ | $\mathcal{M} = \{0,1\}^*$ | $\mathcal{C} = \{0,1\}^*$ |
| $\mathcal{K} = \{0,1\}^{128}$ | $\mathcal{M} = \{A, B, \ldots, Z\}$ | $\mathcal{C} = \{A, B, \ldots, Z\}$ |
| $\mathcal{K} = \{0,1\}^{128}$ | $\mathcal{M} = \{\text{YES}, \text{NO}\}$ | $\mathcal{C} = \{0,1\}^*$ |
| $\mathcal{K} = \{1, \ldots, p\}$ | $\mathcal{M} = \{A, B, \ldots, Z\}$ | $\mathcal{C} = \{0,1\}^*$ |

**Correctness requirement:**

$\forall K \in \mathcal{K}, \forall M \in \mathcal{M}$:

$$\mathcal{D}\big(K, \mathcal{E}(K, M)\big) = M$$

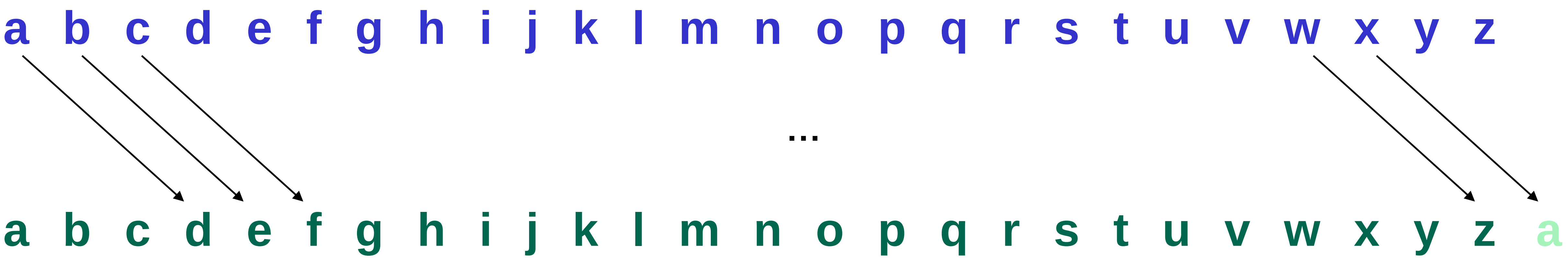
**Possible privacy security goals:**

- Hard to recover $K$ from $C$
- Hard to recover $M$ from $C$
- Hard to learn one bit of $M$ from $C$
- Hard to learn parity of $M$ from $C$
- …

| | 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 |

# Historical encryption algorithms

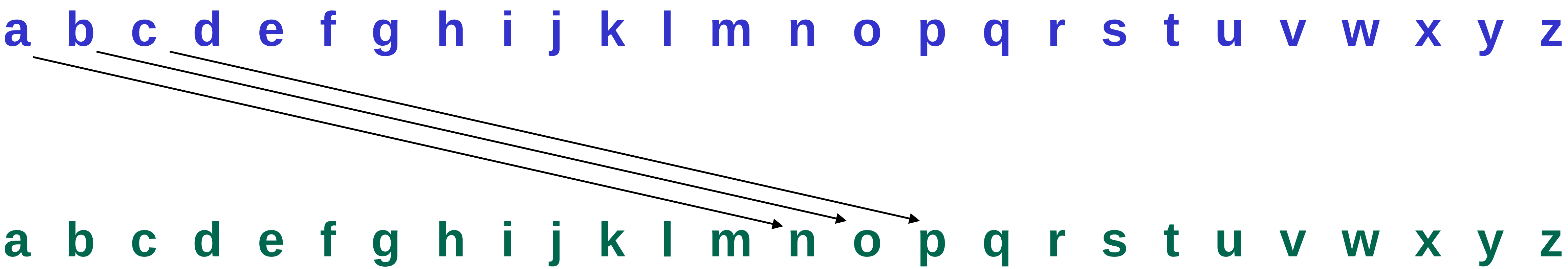
# Ceasar cipher




```
in the far distance a helicopter skimmed down between
the roofs, hovered for an instant like a bluebottle,
and darted away again with a curving flight. It was
the police patrol, snooping into people's windows
```

```
lq wkh idu glvwdqfh d kholfrswhu vnlpphg grzq ehwzhhq
wkh urriv, kryhuhg iru dq lqvwdqw olnh d eoxherwwoh,
dqg gduwhg dzdb djdlq zlwk d fxuylqj ioljkw. Lw zdv
wkh srolfh sdwuro, vqrrslqj lqwr shrsoh'v zlqgrzv
```

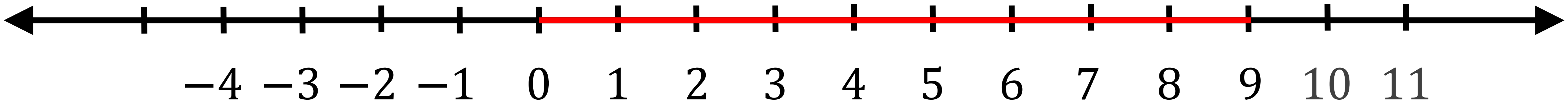
# Ceasar cipher (ROT-13)



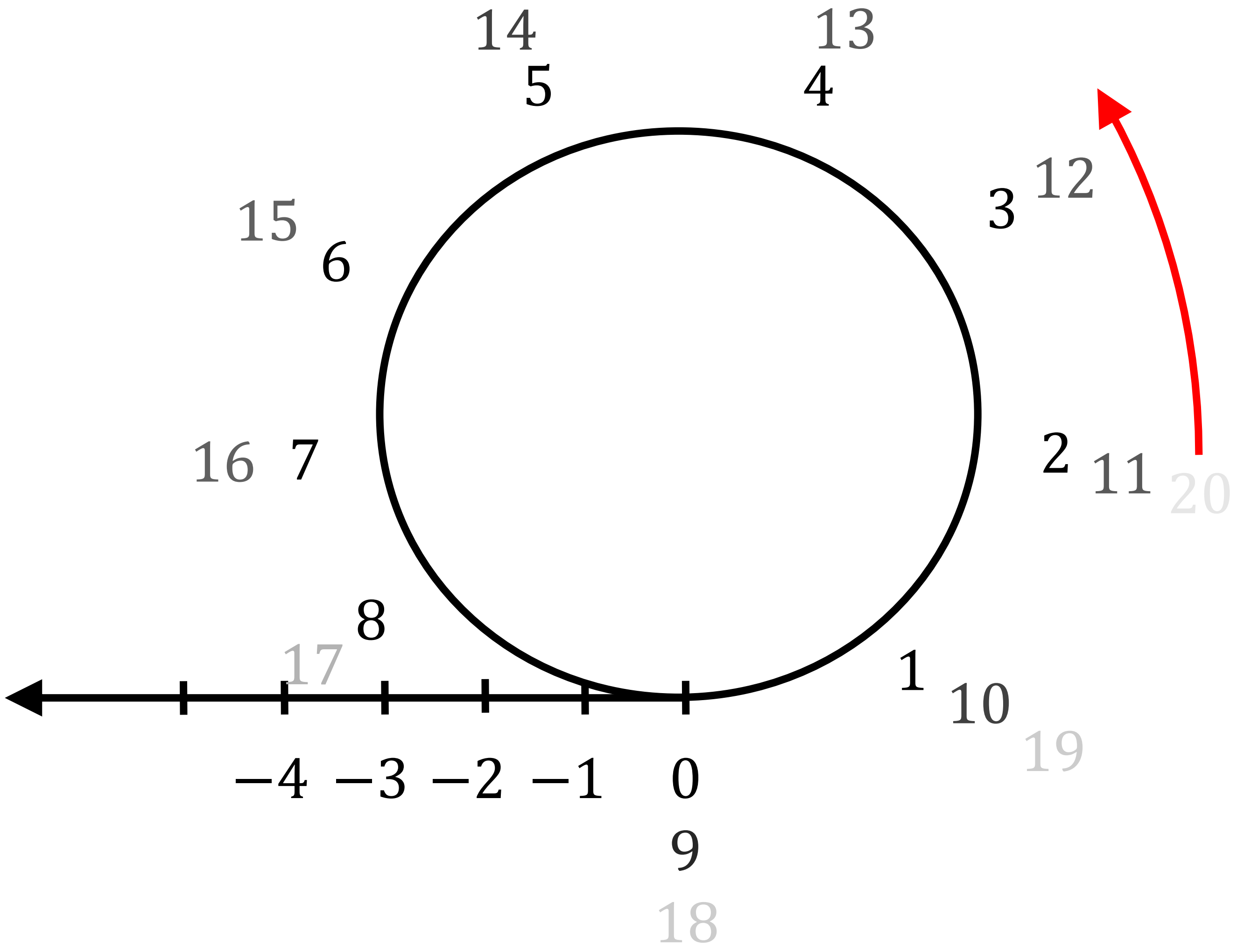

```
in the far distance a helicopter skimmed down between
the roofs, hovered for an instant like a bluebottle,
and darted away again with a curving flight. It was
the police patrol, snooping into people's windows
```

```
va gur sne qvfgnapr n uryvpbcgre fxvzzrq qbja orgjrra
gur ebbsf, ubirerq sbe na vafgnag yvxr n oyhrobggyr,
naq qnegrq njnl ntnva jvgu n pheivat syvtug. Vg jnf
gur cbyvpr cngeby, fabbcvat vagb crbcyr'f jvaqbjf
```

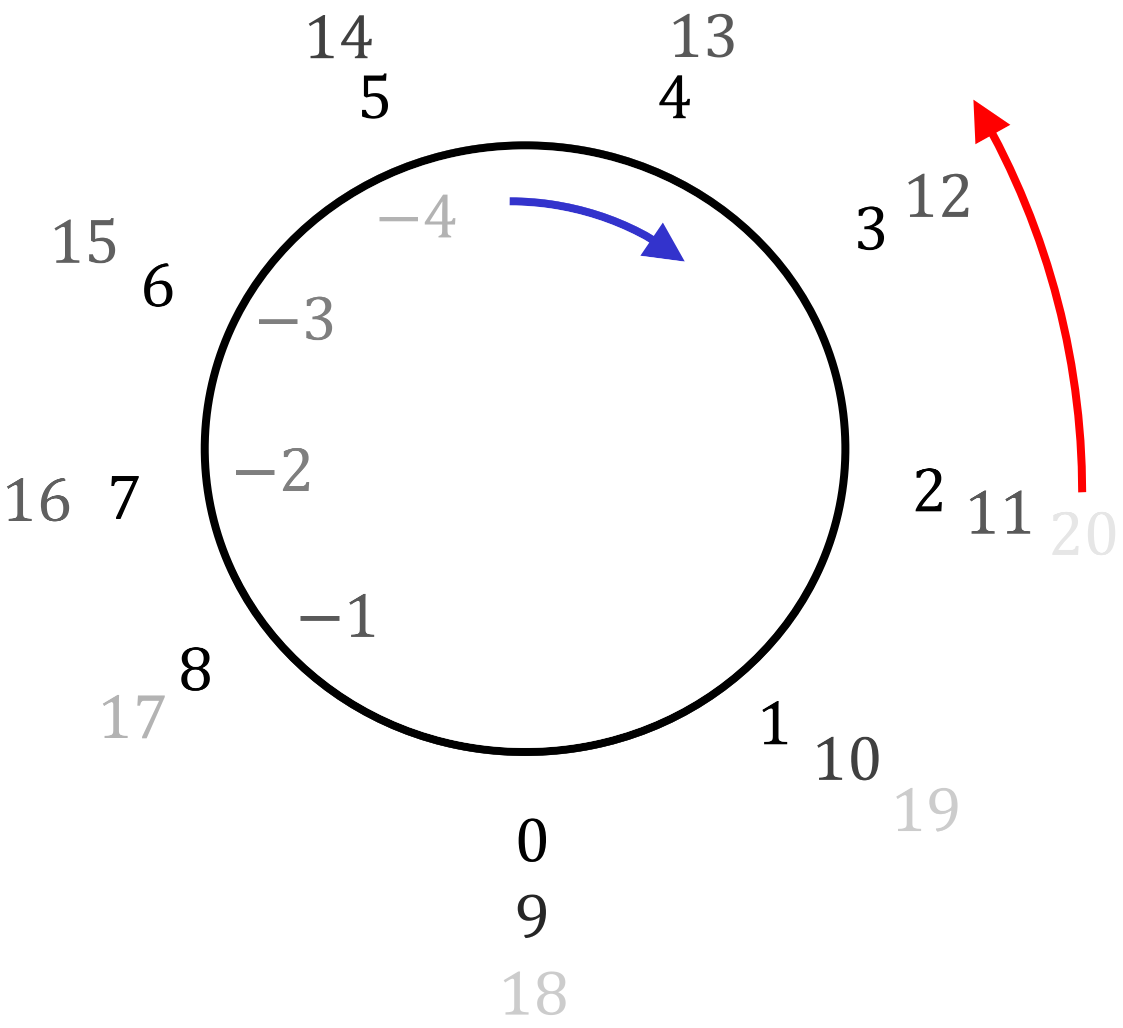
# Modular arithmetic



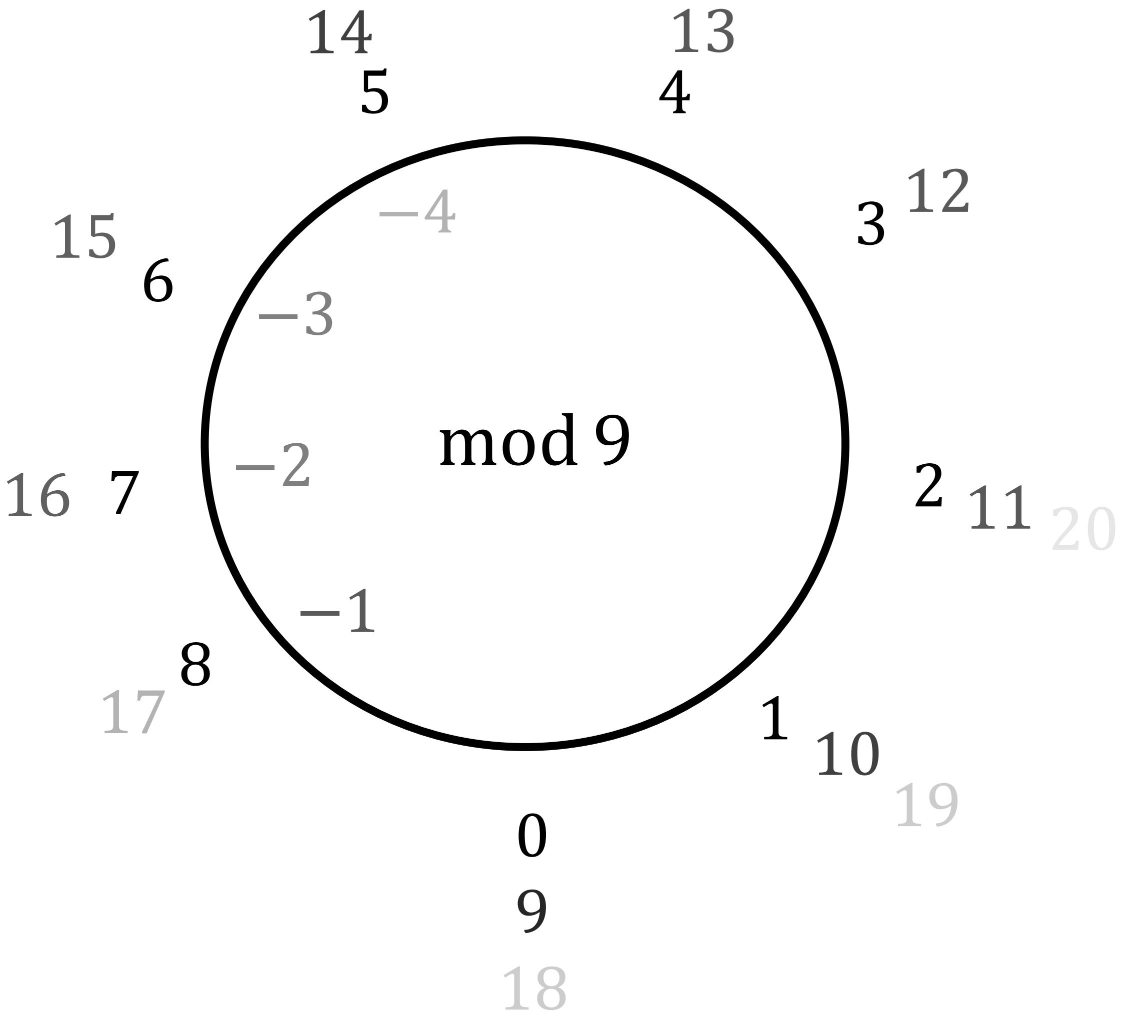
# Modular arithmetic



# Modular arithmetic



# Modular arithmetic




$$1 + 3 = 4$$

$$5 + 8 = 13 \equiv 4 \bmod 9$$

$$5 \cdot 4 = 20 \equiv 2 \bmod 9$$

$$2 - 5 = -3 \equiv 6 \bmod 9$$

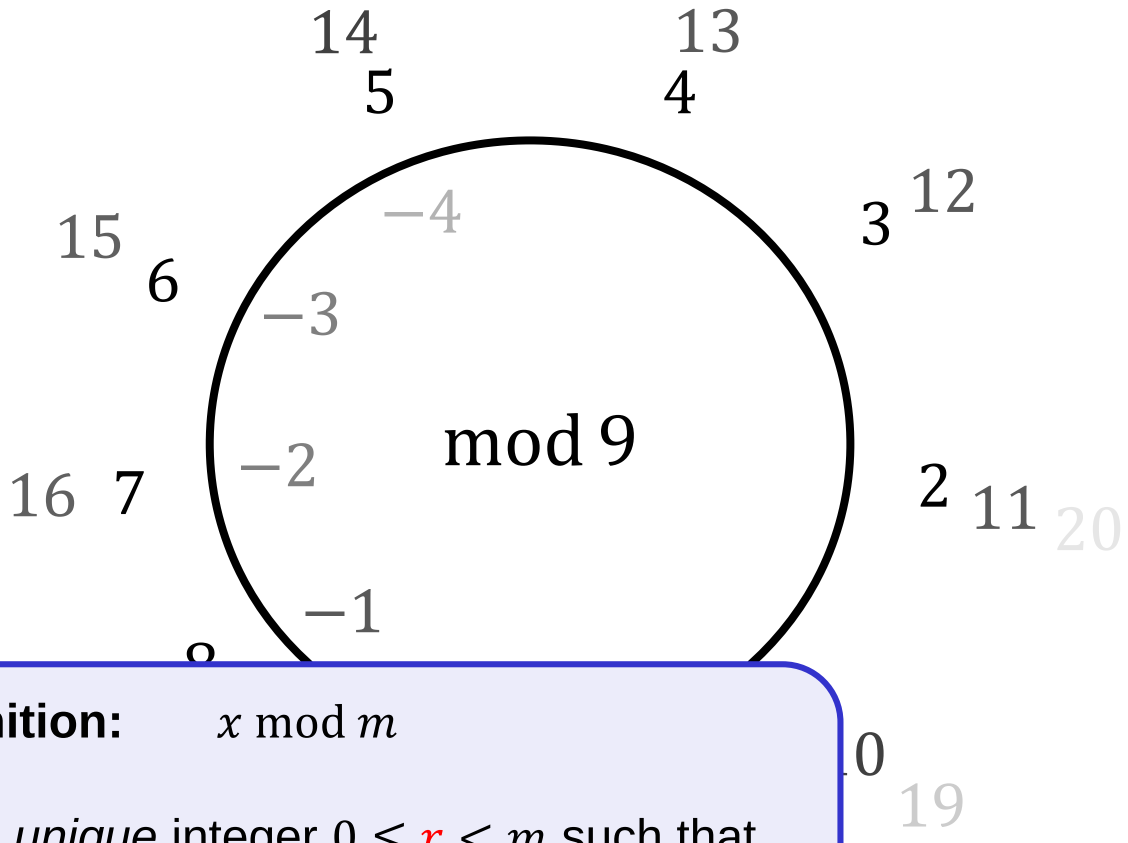
$$2^{10} = 1024 \equiv 7 \bmod 9$$

$$158 \quad = 153 + {\color{red} r} \quad \equiv {\color{red} r} \bmod 9 \equiv 5 \bmod 9$$

$${\color{red} r} < 9$$

$$9 \to 18 \to 27 \to 36 \to \cdots \to \mathbf{153} \to 162$$

# Modular arithmetic




**Definition:** $x \bmod m$

is the *unique* integer $0 \leq r < m$ such that

$$x = q \cdot m + r$$

$$1 + 3 = 4$$

$$5 + 8 = 13 \quad \equiv 4 \bmod 9$$

$$5 \cdot 4 = 20 \equiv 2 \bmod 9$$

$$2 - 5 = -3 \equiv 6 \bmod 9$$

$$2^{10} = 1024 \equiv 7 \bmod 9$$

$$158 \quad = 153 + r \quad \equiv r \bmod 9 \equiv 5 \bmod 9$$

$$r < 9$$

$$9 \rightarrow 18 \rightarrow 27 \rightarrow 36 \rightarrow \cdots \rightarrow \mathbf{153} \rightarrow 162$$

More details: https://en.wikibooks.org/wiki/High_School_Mathematics_Extensions/Primes/Modular_Arithmetic

# Ceasar cipher

- a $\leftrightarrow$ 0
- b $\leftrightarrow$ 1
- c $\leftrightarrow$ 2
- d $\leftrightarrow$ 3
- e $\leftrightarrow$ 4

$$C \leftarrow M + 3 \pmod{26}$$

⋮

- z $\leftrightarrow$ 25

# ROT-13

- a ↔ 0
- b ↔ 1
- c ↔ 2
- d ↔ 3
- e ↔ 4

⋮

- z ↔ 25

$$C \leftarrow M + 13 \pmod{26}$$

$$M \leftarrow C - 13 \pmod{26}$$

$$\mathcal{E} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$$

$$\mathcal{D} : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$$

$$\mathcal{K} = \{\ \}$$

$$\mathcal{M} = \{0,1,2, \ldots, 25\}$$

$$\mathcal{C} = \{0,1,2, \ldots, 25\}$$

# ROT-K

- a ↔ 0
- b ↔ 1
- c ↔ 2
- d ↔ 3
- e ↔ 4

⋮

- z ↔ 25

$$C \leftarrow M + K \pmod{26}$$

$$M \leftarrow C - K \pmod{26}$$

$$\mathcal{E} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$$

$$\mathcal{D} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$$

$$\mathcal{K} = \{0,1,2,\ldots,25\}$$

$$\mathcal{M} = \{0,1,2,\ldots,25\}$$

$$\mathcal{C} = \{0,1,2,\ldots,25\}$$

# Attacking ROT-K

$|\mathcal{K}| = 26$

| $K$ | $M$ |
|---|---|
| 0 | va gur sne qvfgnapr n uryvpbcgre.… |

$C$ = va gur sne qvfgnapr n uryvpbcgre…

**Conclusion:** key space must be large enough!

# Substitution cipher

$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| ↕ | ↕ | ↕ | ↕ | | | | | | | | | … | | | | | | | | | | | | | ↕ |
| s | x | d | y | w | q | f | m | j | k | o | i | l | g | z | b | e | n | t | u | c | p | a | r | v | h |

```
in the far distance a helicopter skimmed down between the roofs,
hovered for an instant like a bluebottle, and darted away again
with a curving flight. It was the police patrol, snooping into
people's windows
```

```
jg umw qsn yjtusgdw s mwijdzbuwn tojllwy yzag xwuawwg umw nzzqt,
mzpwnwy qzn sg jgtusgu ijow s xicwxzuuiw, sgy ysnuwy sasv sfsjg
ajum s dcnpjgf qijfmu. ju ast umw bzijdw bsunzi, tgzzbjgf jguz
bwzbiw't ajgyzat
```

# Substitution cipher – formal syntax

- $\Sigma = \{a, b, c, \dots, z\}$
- $\mathcal{M} = \Sigma^*$
- $\mathcal{C} = \Sigma^*$
- $\mathcal{K} =$ all permutations on $\Sigma$ $= \{\pi : \Sigma \to \Sigma \mid \pi \text{ a permutation}\}$
- $\pi \in \mathcal{K}$

$\mathcal{E} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$

$\mathcal{D} : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$

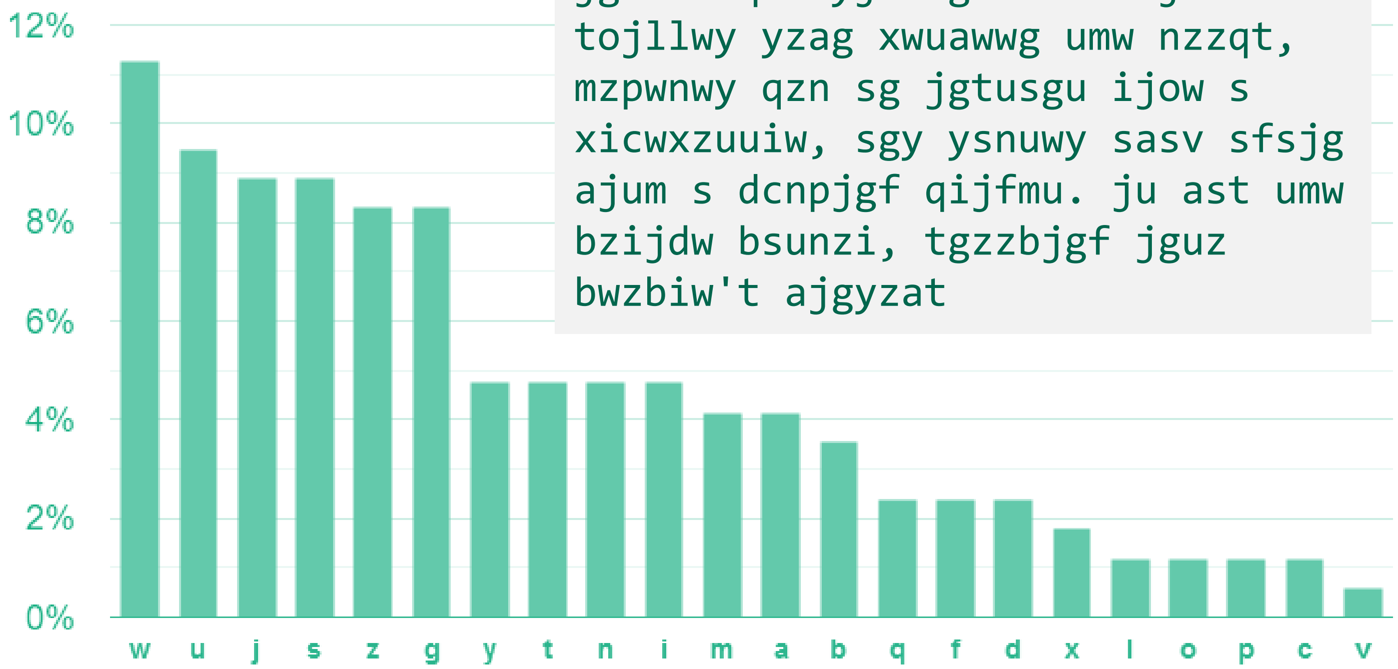
| $\sigma$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | … |
|---|---|---|---|---|---|---|---|---|---|
| $\pi(\sigma)$ | $o$ | $y$ | $e$ | $z$ | $p$ | $u$ | $g$ | $t$ | … |

- $M = feed$
- $C = \mathcal{E}(\pi, M) = \pi(f)\pi(e)\pi(e)\pi(d) = uppz$
- $\mathcal{D}(\pi, C) = \pi^{-1}(u)\pi^{-1}(p)\pi^{-1}(p)\pi^{-1}(z) = feed$

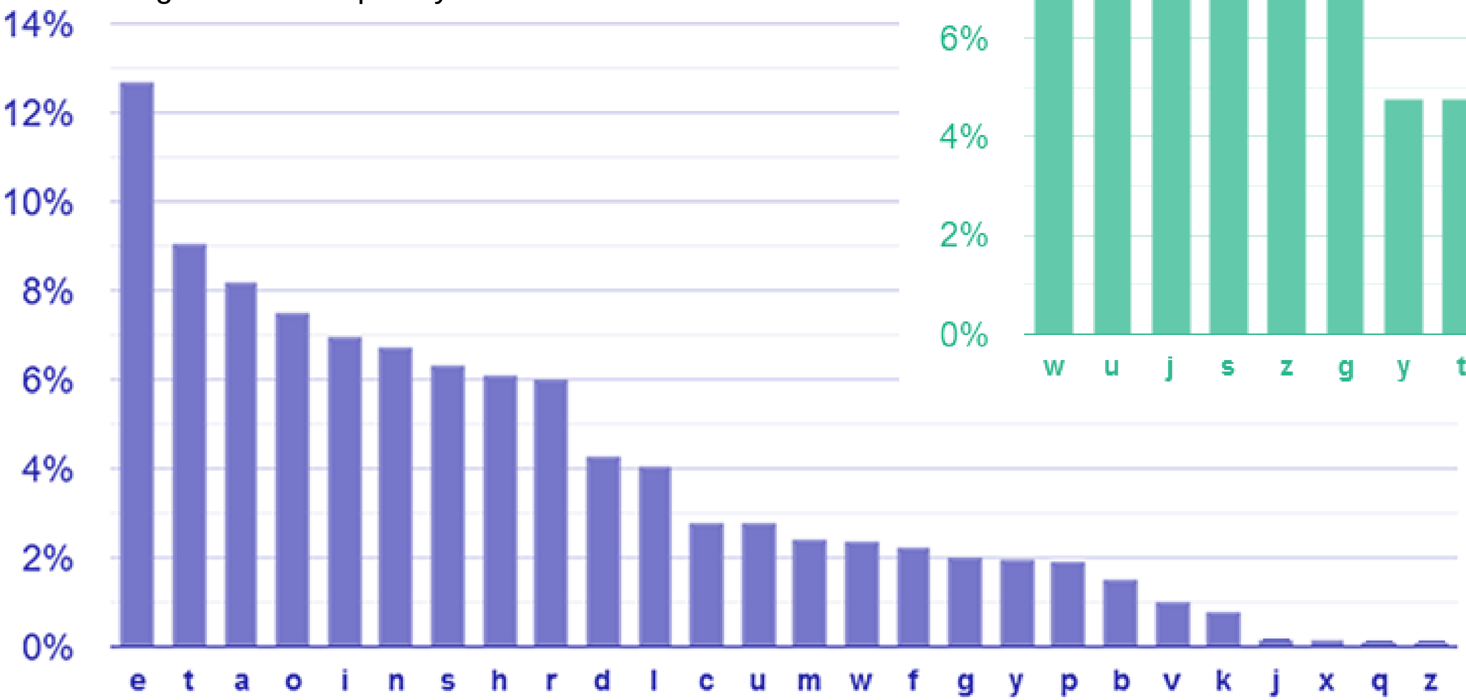
# Attacking the substitution cipher

$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$

```
jg umw qsn yjtusgdw s mwijdzbuwn
tojllwy yzag xwuawwg umw nzzqt,
mzpwnwy qzn sg jgtusgu ijow s
xicwxzuuiw, sgy ysnuwy sasv sfsjg
ajum s dcnpjgf qijfmu. ju ast umw
bzijdw bsunzi, tgzzbjgf jguz
bwzbiw't ajgyzat
```



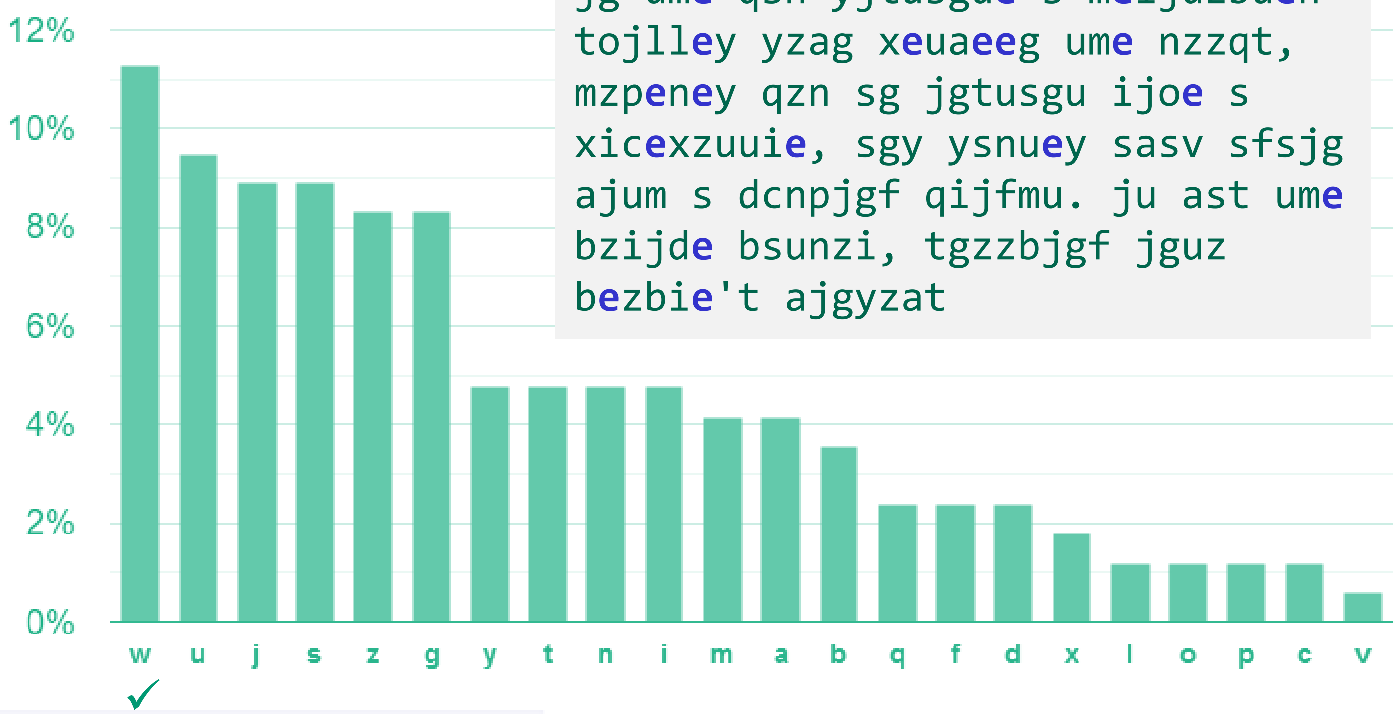

English letter frequency

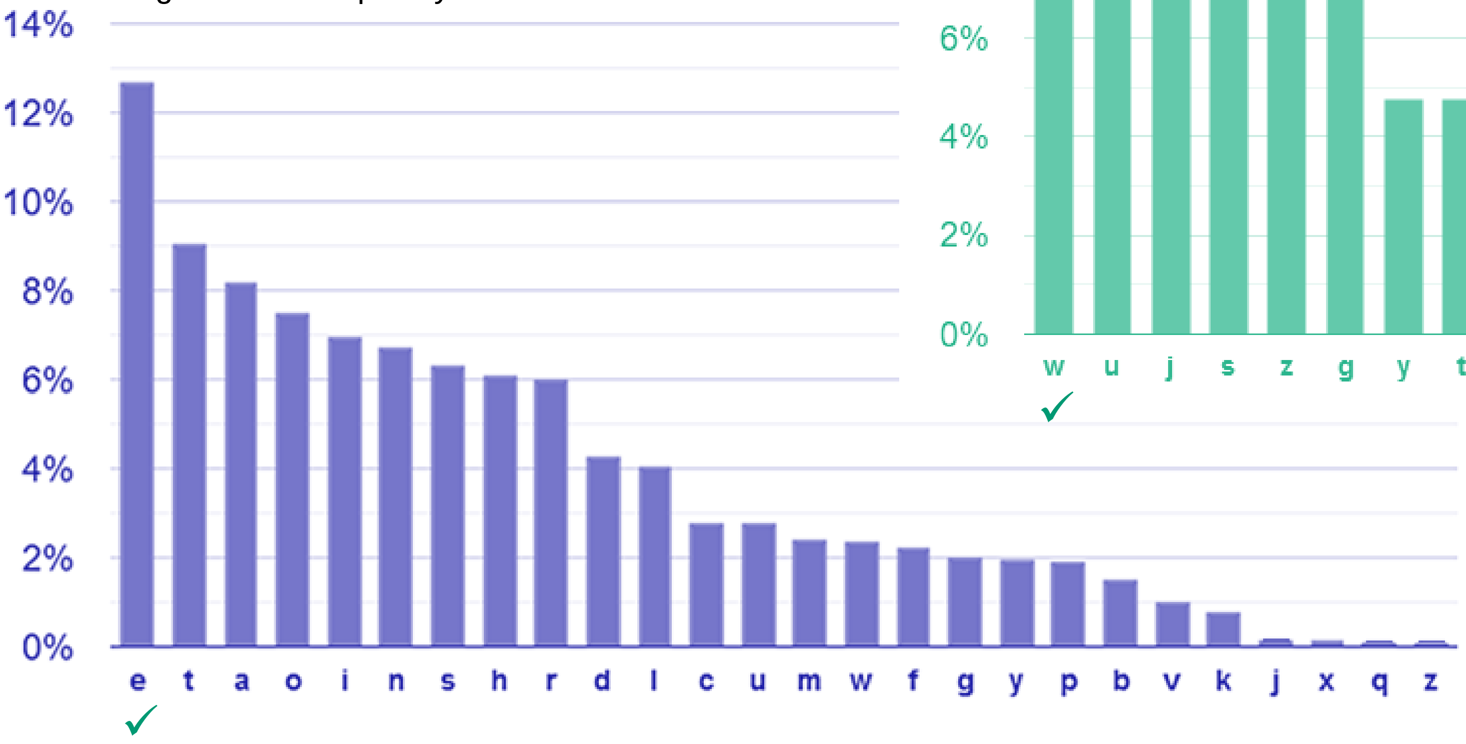


# Attacking the substitution cipher

$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$

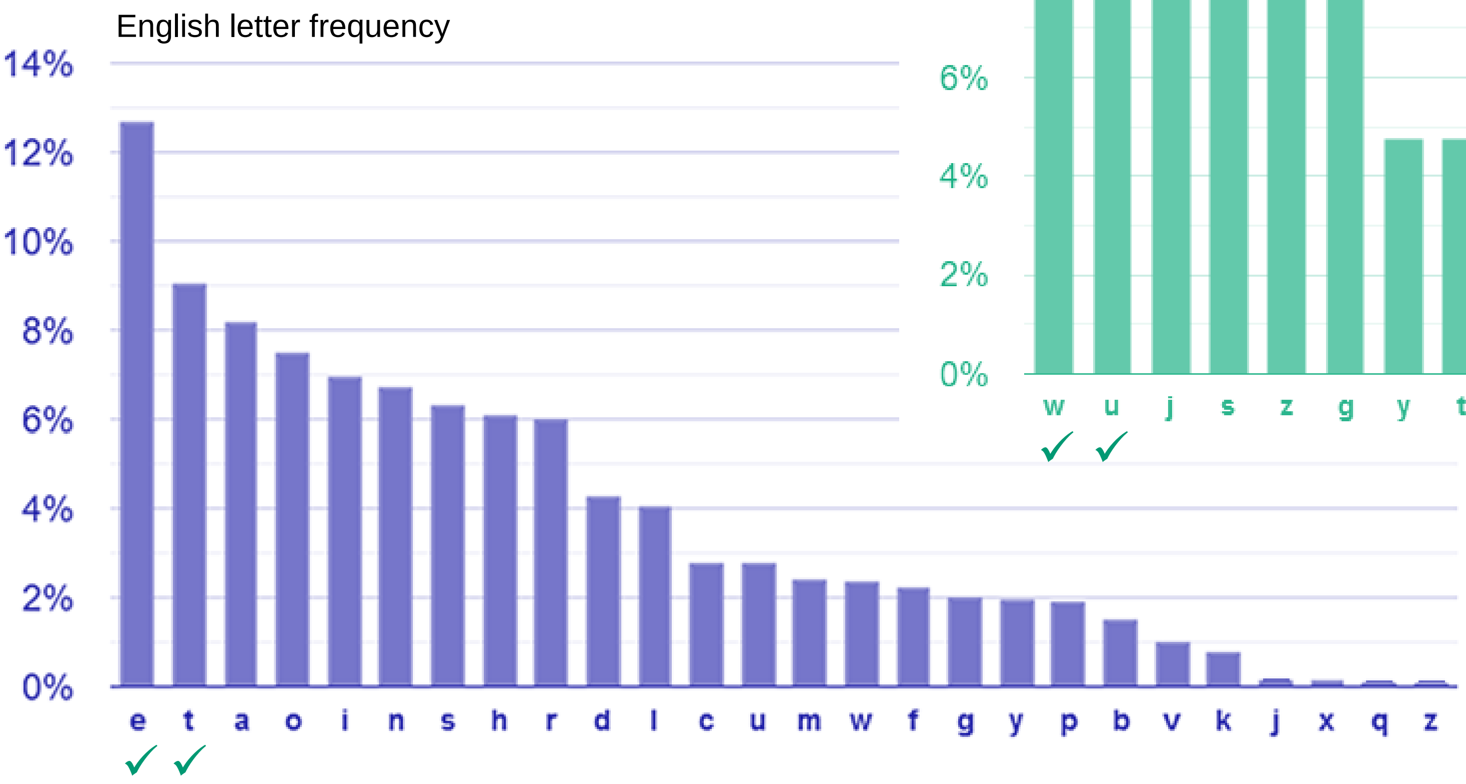
```
jg ume qsn yjtusgde s meijdzbuen
tojlley yzag xeuaeeg ume nzzqt,
mzpeney qzn sg jgtusgu ijoe s
xicexzuuie, sgy ysnuey sasv sfsjg
ajum s dcnpjgf qijfmu. ju ast ume
bzijde bsunzi, tgzzbjgf jguz
bezbie't ajgyzat
```

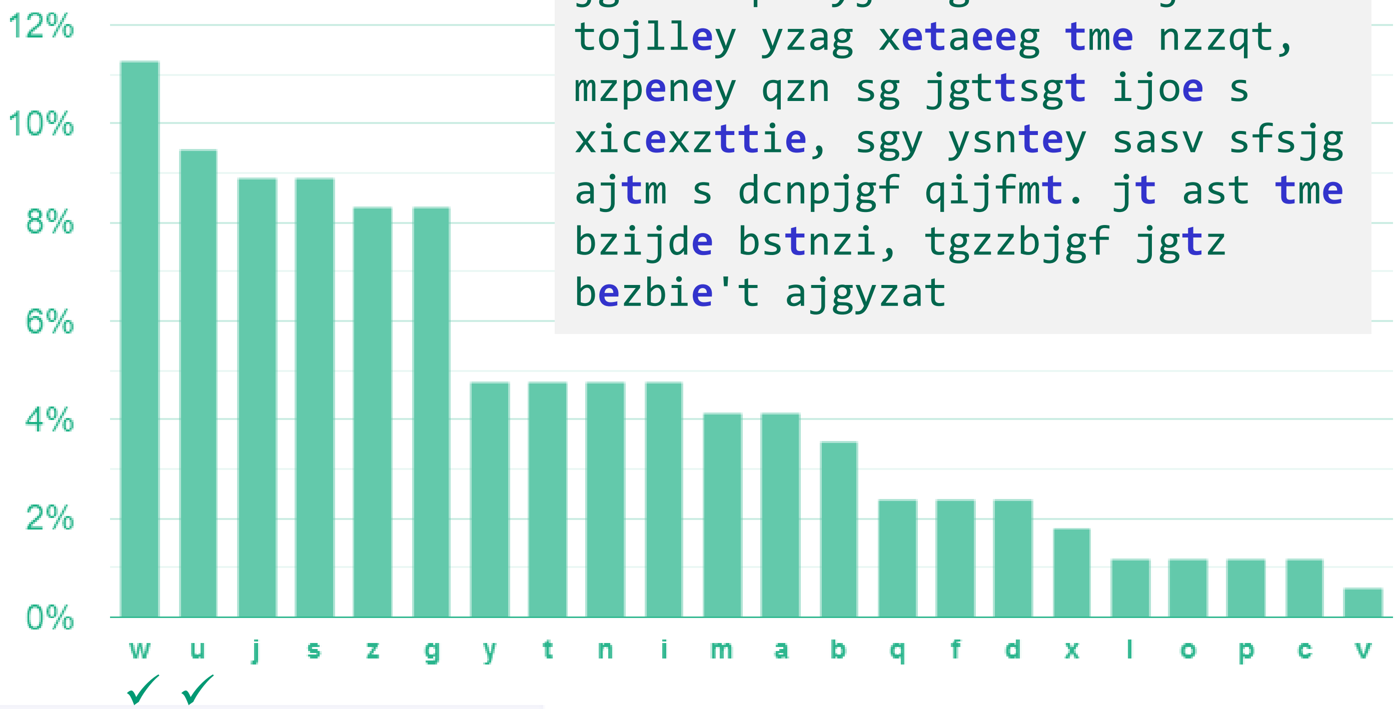


# Attacking the substitution cipher

$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$

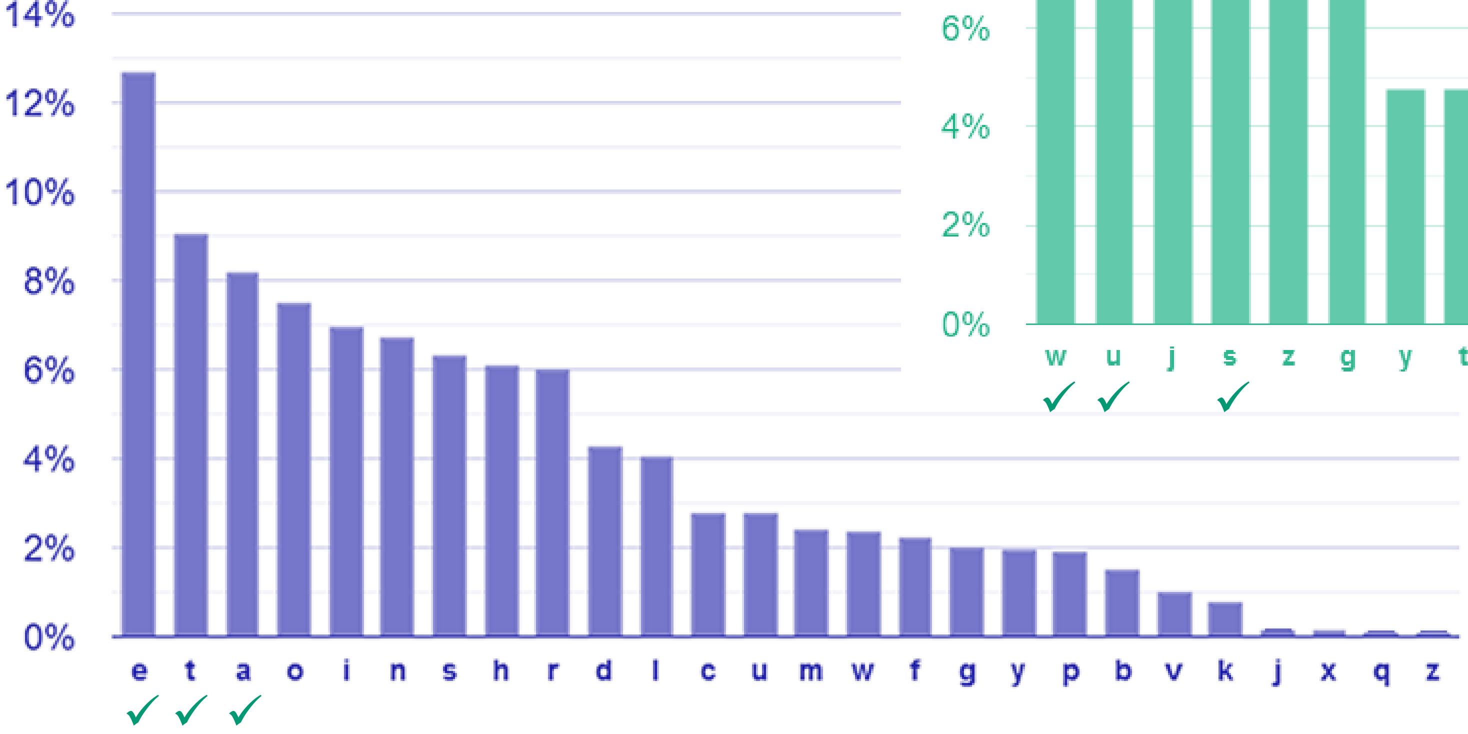


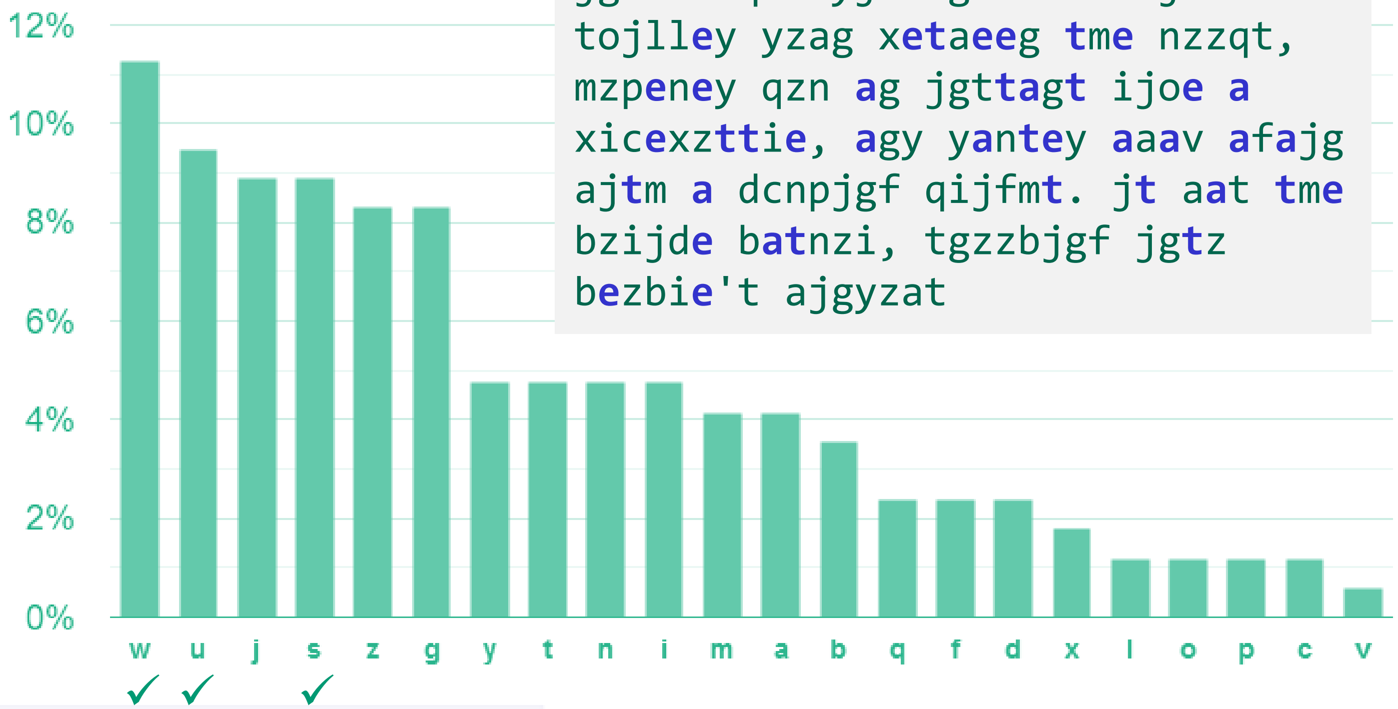




```
jg tme qsn yjttsgde s meijdzbten
tojlley yzag xetaeeg tme nzzqt,
mzpeney qzn sg jgttsgt ijoe s
xicexzttie, sgy ysntey sasv sfsjg
ajtm s dcnpjgf qijfmt. jt ast tme
bzijde bstnzi, tgzzbjgf jgtz
bezbie't ajgyzat
```

# Attacking the substitution cipher

$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$



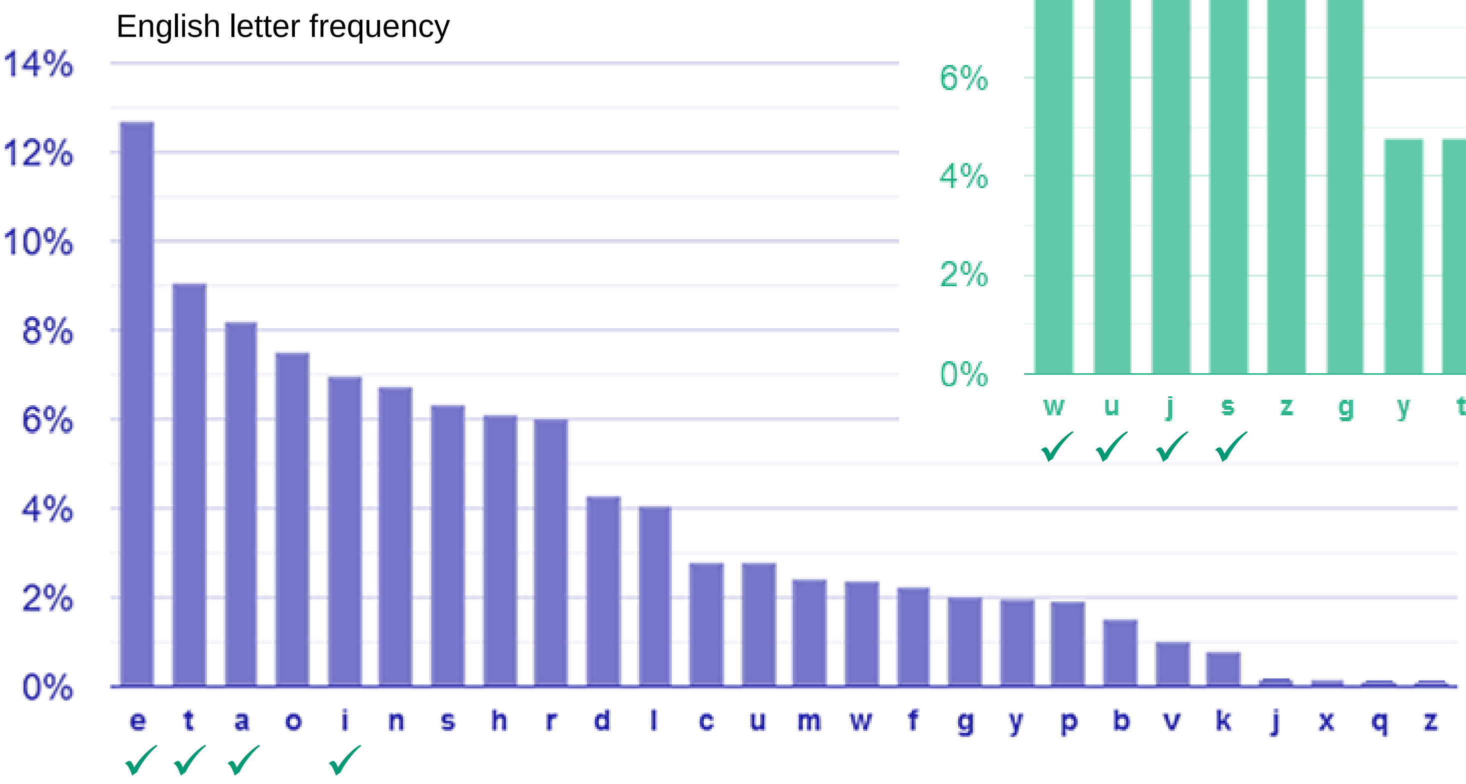



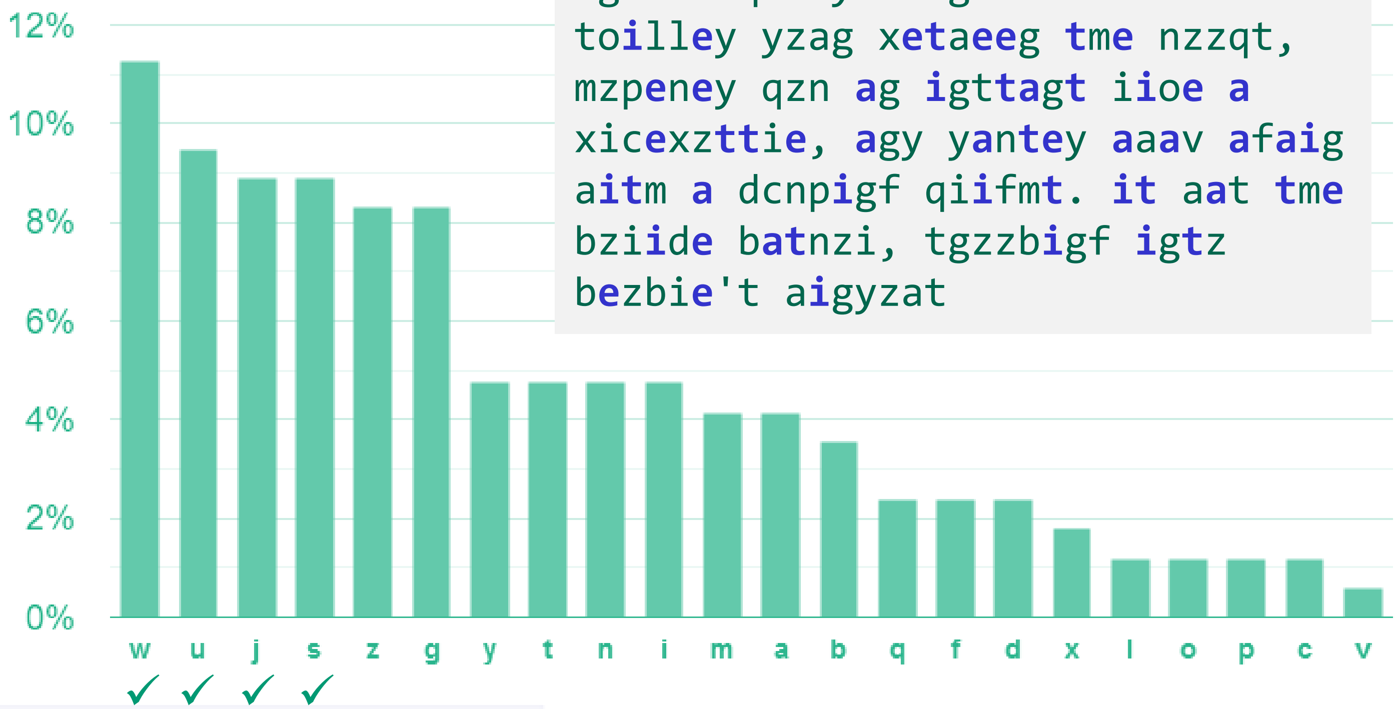

jg tme qan yjttagde a meijdzbten
tojlley yzag xetaeeg tme nzzqt,
mzpeney qzn ag jgttagt ijoe a
xicexzttie, agy yantey aaav afajg
ajtm a dcnpjgf qijfmt. jt aat tme
bzijde batnzi, tgzzbjgf jgtz
bezbie't ajgyzat

# Attacking the substitution cipher

$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$

ig tme qan yittagde a meiidzbten
toilley yzag xetaeeg tme nzzqt,
mzpeney qzn ag igttagt iioe a
xicexzttie, agy yantey aaav afaig
aitm a dcnpigf qiifmt. it aat tme
bziide batnzi, tgzzbigf igtz
bezbie't aigyzat

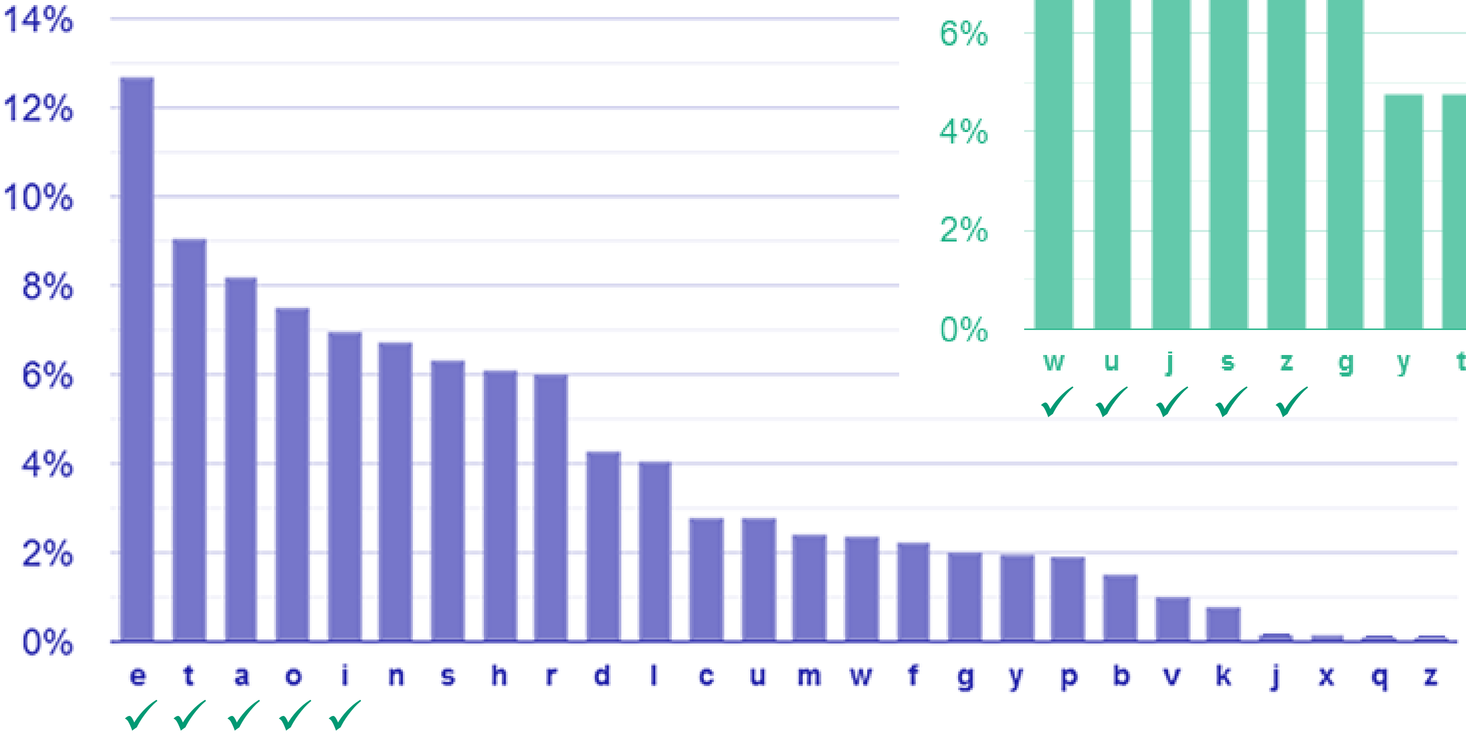


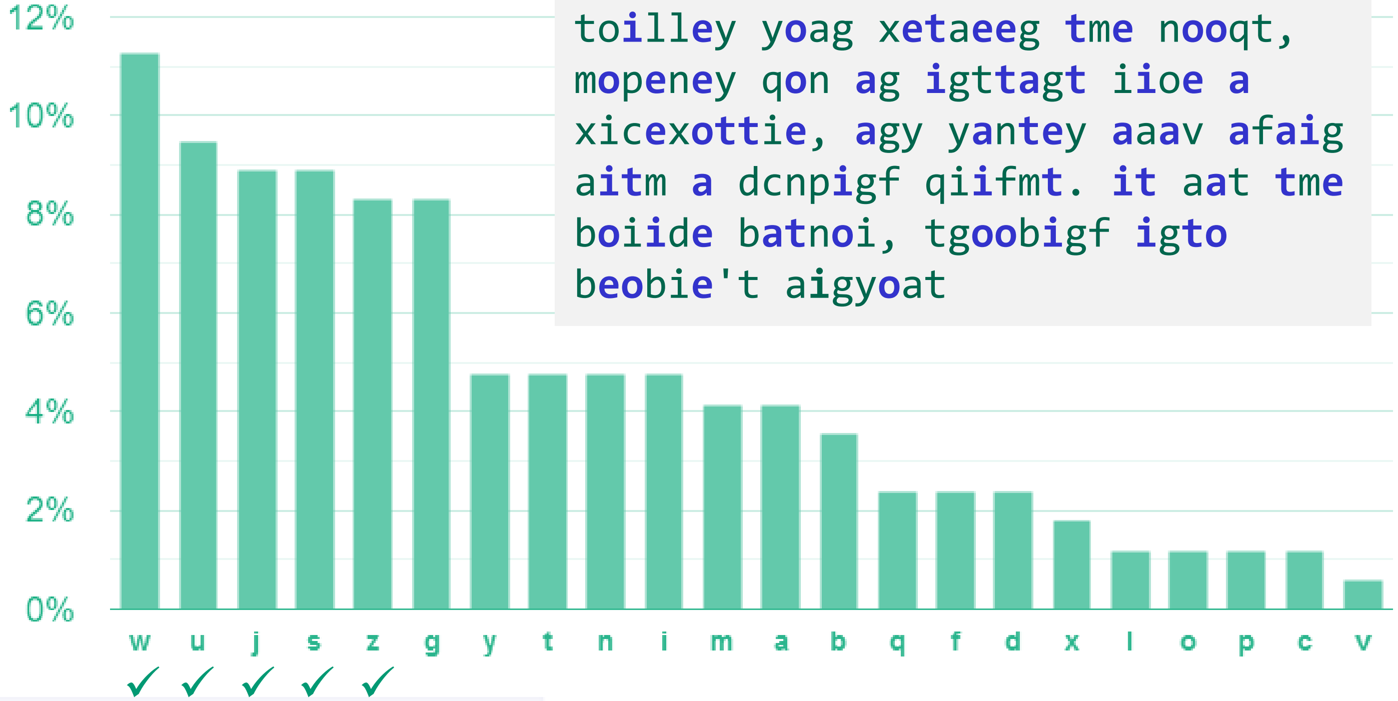



# Attacking the substitution cipher

$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$

English letter frequency



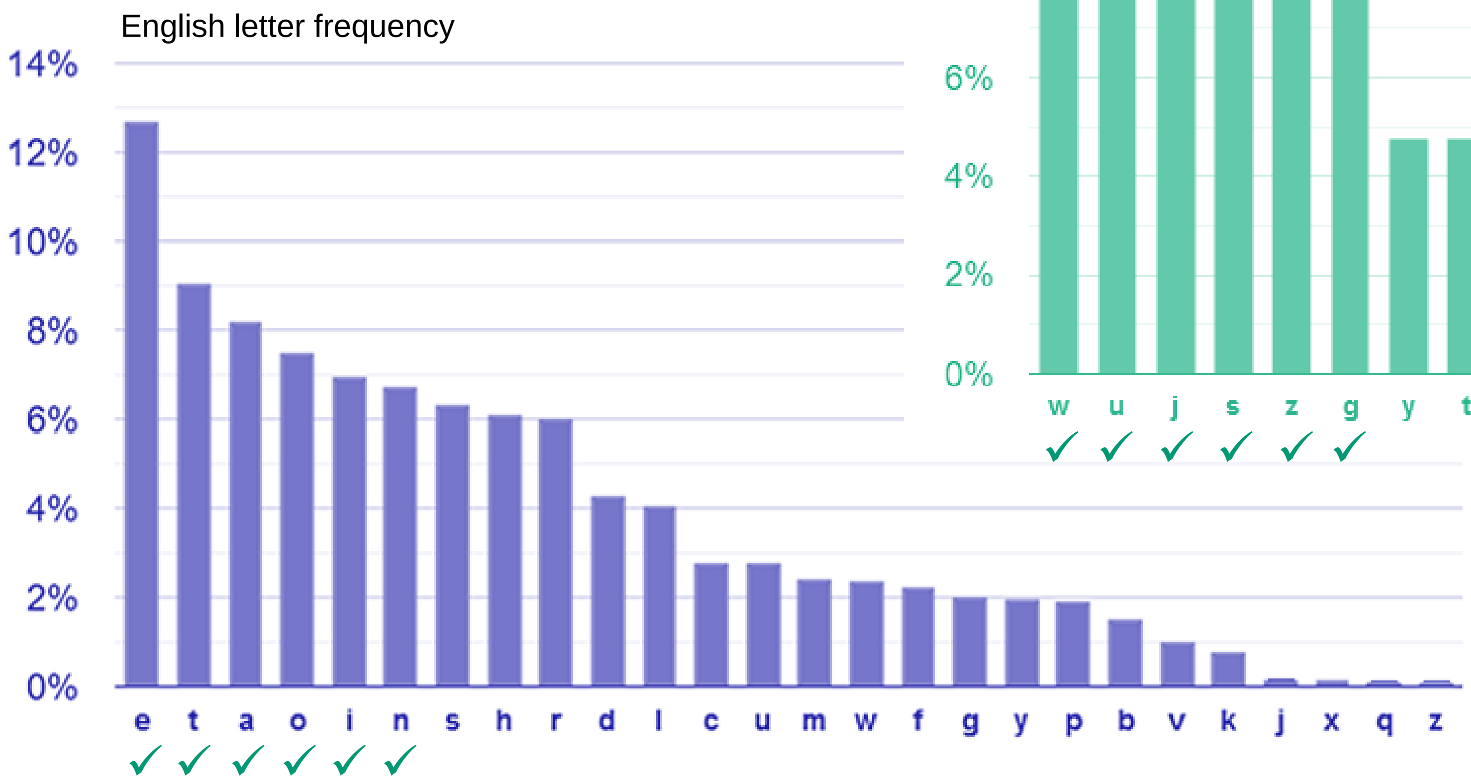



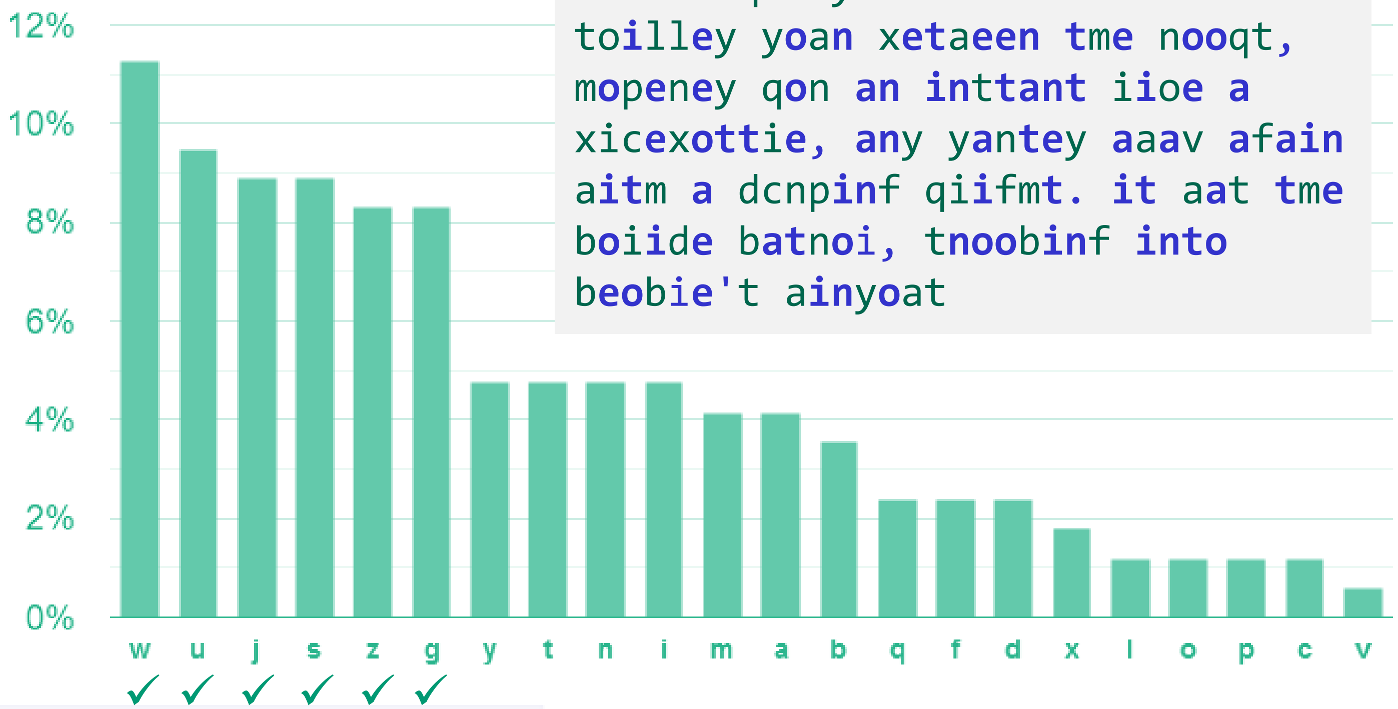

```
ig tme qan yittagde a meiidobten
toilley yoag xetaeeg tme nooqt,
mopeney qon ag igttagt iioe a
xicexottie, agy yantey aaav afaig
aitm a dcnpigf qiifmt. it aat tme
boiide batnoi, tgoobigf igto
beobie't aigyoat
```

# Attacking the substitution cipher

$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$

```
in tme qan yittande a meiidobten
toilley yoan xetaeen tme nooqt,
mopeney qon an inttant iioe a
xicexottie, any yantey aaav afain
aitm a dcnpinf qiifmt. it aat tme
boiide batnoi, tnoobinf into
beobie't ainyoat
```



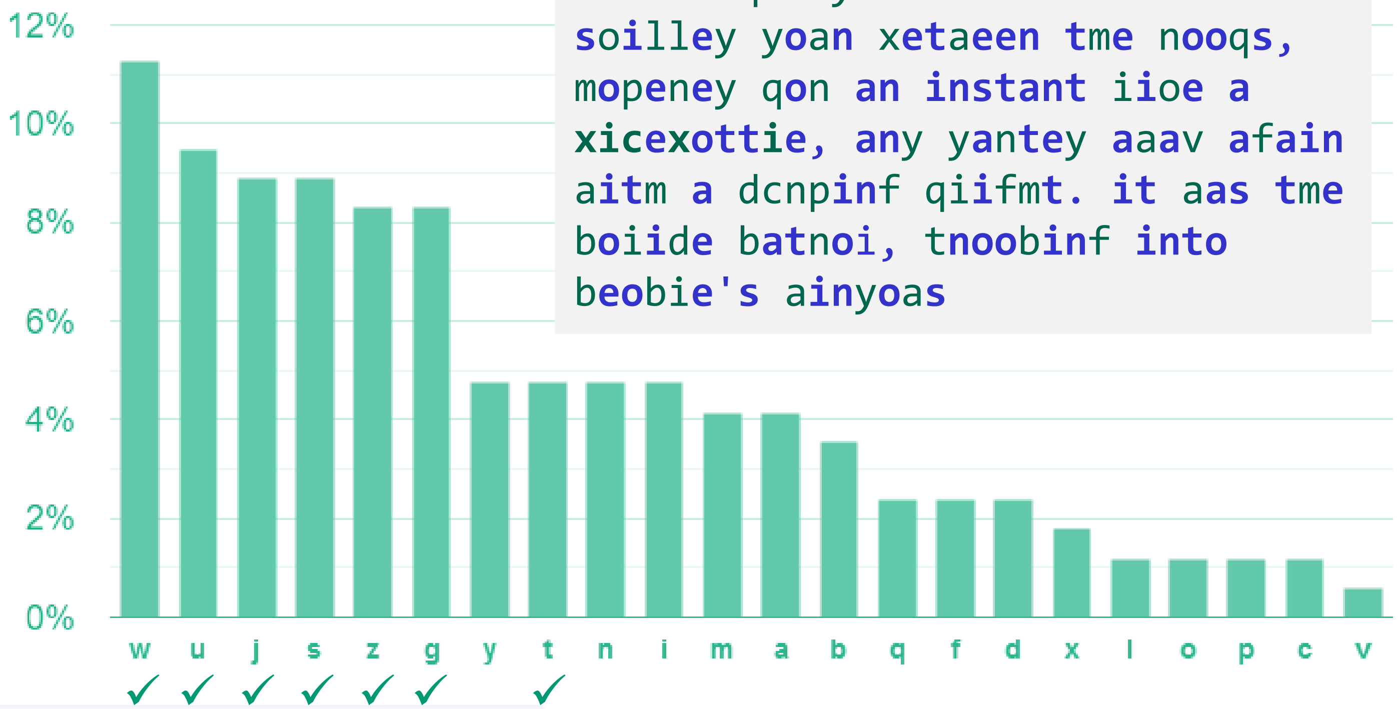



# Attacking the substitution cipher

$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$

```
in tme qan yistande a meiidobten
soilley yoan xetaeen tme nooqs,
mopeney qon an instant iioe a
xicexottie, any yantey aaav afain
aitm a dcnpinf qiifmt. it aas tme
boiide batnoi, tnoobinf into
beobie's ainyoas
```

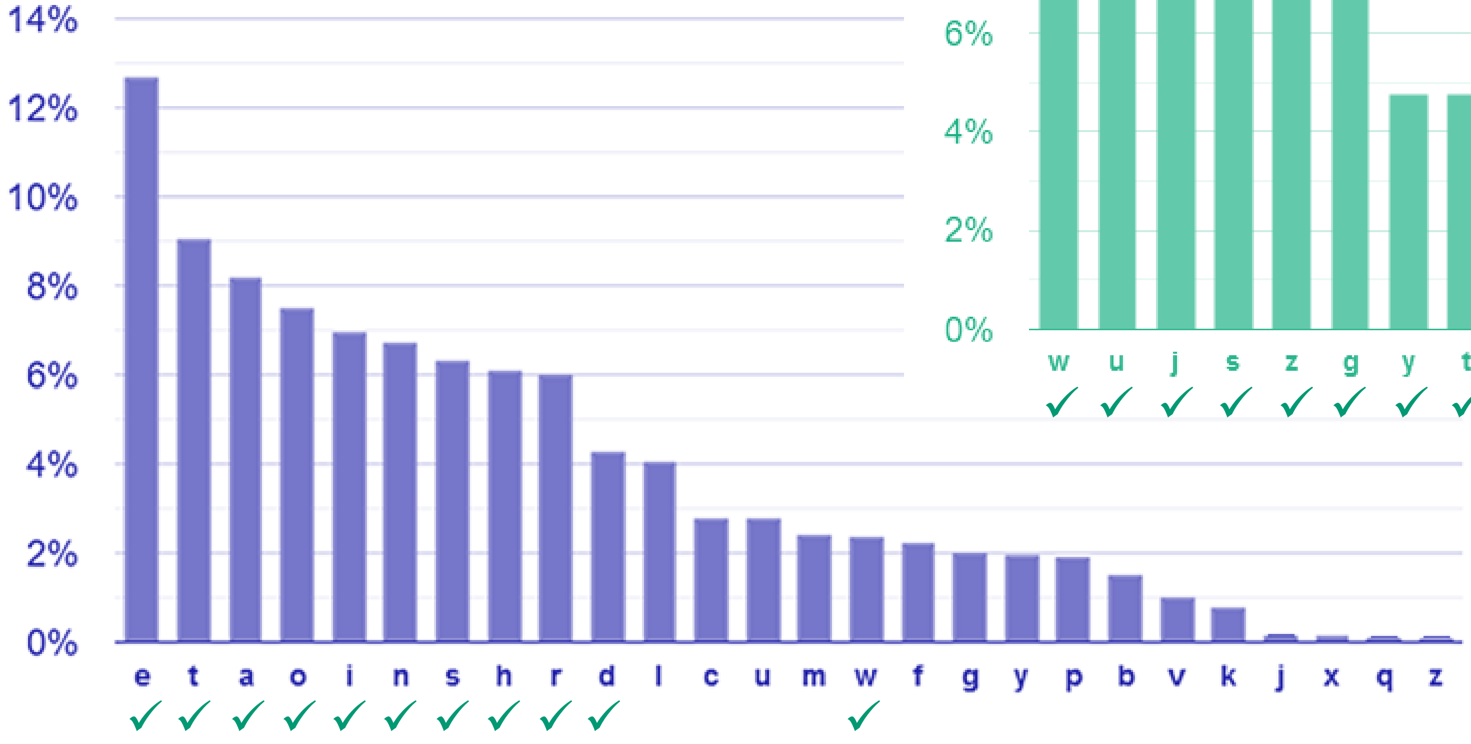
English letter frequency

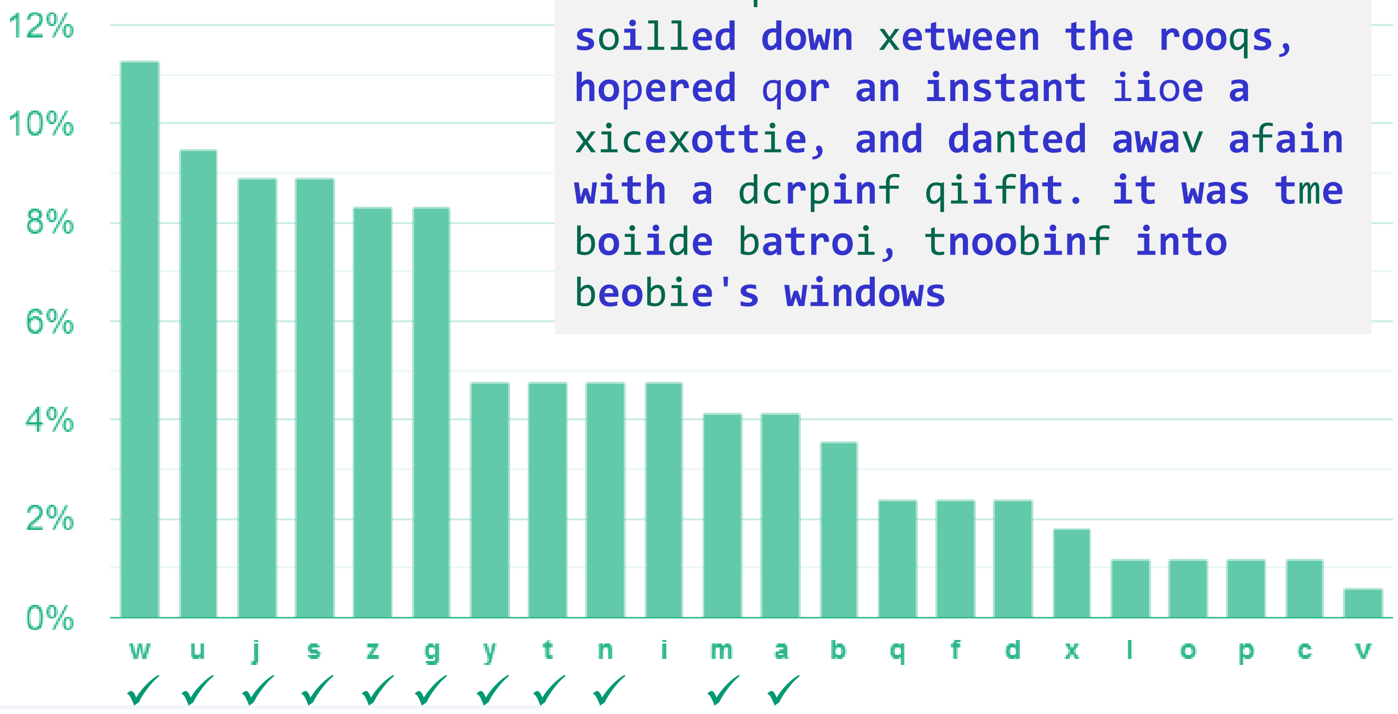



# Attacking the substitution cipher

$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$

English letter frequency



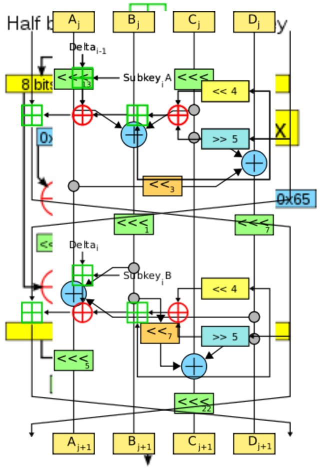




in the qan distande a heiidobter soilled down xetween the rooqs, hopered qor an instant iioe a xicexottie, and danted awav afain with a dcrpinf qiifht. it was tme boiide batroi, tnoobinf into beobie's windows

# Conclusions

- Key space must be large enough
- Ciphertext should not reveal letter frequency of the message
- Is this enough?

# Historical approach to crypto development




build → break → fix → break → fix → break → fix ...    secure?

# Modern approach

- Trying to make cryptography more a **science** than an **art**
- Focus on **formal definitions** of security (and insecurity)
- Clearly stated **assumptions**
- Analysis supported by mathematical **proofs**
- ... but old fashioned **cryptanalysis** continues to be very important!

# The one-time-pad (OTP)

$\mathcal{K} = \{0,1\}^n$

$\mathcal{M} = \{0,1\}^n$

$\mathcal{C} = \{0,1\}^n$

**Is OTP secure?**

$\mathcal{E} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$

$\mathcal{E}(K, M) = K \oplus M$

$\mathcal{D} : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$

$\mathcal{D}(K, C) = K \oplus C$

$$\begin{array}{rll} & 0101100100 & M \\ \oplus & 1110001101 & K \\ \hline = & 1011101001 & C \end{array}$$

$$\begin{array}{rll} & 1011101001 & C \\ \oplus & 1110001101 & K \\ \hline = & 0101100100 & M \end{array}$$

# The one-time-pad (OTP)

$\mathcal{K} = \{0,1\}^n$

$\mathcal{M} = \{0,1\}^n$

$\mathcal{C} = \{0,1\}^n$

**Is OTP secure?**

$\mathcal{E} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$

$\mathcal{E}(K, M) = K \oplus M$

$\mathcal{D} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$

$\mathcal{D}(K, C) = K \oplus C$

**Theorem:** The OTP encryption scheme has **one-time perfect privacy**

**Definition (Shannon 1949):** An encryption scheme has **one-time perfect privacy** if for any two $M_1, M_2 \in \mathcal{M}$ and any $C \in \mathcal{C}$

$$\Pr[\mathcal{E}_K(M_1) = C] = \Pr[\mathcal{E}_K(M_2) = C]$$

probability taken over the random choice $K \stackrel{\$}{\leftarrow} \mathcal{K}$ and the random coins used by $\mathcal{E}$ (if any)

# (One-time) perfect secrecy

- From adversary's POV the ciphertext is *uniformily* distributed over $\mathcal{C}$
- $C$ cannot give *any* information about $M$!

$$\boldsymbol{C = 101}$$

| **Prob** | $\boldsymbol{K}$ | $\boldsymbol{M}$ |
|---|---|---|
| | | 000 |
| | | 001 |
| | | 010 |
| | | 011 |
| | | 100 |
| | | 101 |
| | | 110 |
| | | 111 |

# Proof of OTP one-time perfect privacy

**Theorem:** The OTP encryption scheme has **one-time perfect privacy**

**Definition:** An encryption scheme has **one-time perfect privacy** if for any $M_1, M_2 \in \mathcal{M}$ and any $C \in \mathcal{C}$

$$\Pr[\mathcal{E}_K(M_1) = C] = \Pr[\mathcal{E}_K(M_2) = C]$$

probability taken over the random choice $K \stackrel{\$}{\leftarrow} \mathcal{K}$ and the random coins used by $\mathcal{E}$ (if any)

**Proof:** fix $M_1, M_2, C \in \{0,1\}^n$

**Need to show:** $\Pr[K \oplus M_1 = C] = \Pr[K \oplus M_2 = C]$

$$\Pr[K \oplus M_1 = C] = \Pr[K = M_1 \oplus C] = \Pr[K = Z_1] = \frac{1}{2^n}$$

$$\Pr[K \oplus M_2 = C] = \Pr[K = M_2 \oplus C] = \Pr[K = Z_2] = \frac{1}{2^n}$$

**QED**

# One-time pad – perfect?

- OTP gives perfect privacy…for *one* message
  - What happens if you reuse the same key for two messages?
  - $C_1 \oplus C_2 = (K \oplus M_1) \oplus (K \oplus M_2) = M_1 \oplus M_2$

- Key is as long as the message
  - What happens if it is shorter?
  - Key management becomes very difficult
  - Sort of defeats the purpose

**Theorem:** No encryption scheme can have perfect secrecy if $|\mathcal{K}| < |\mathcal{M}|$

- Nothing special about XOR: ROT-K also has one-time perfect privacy
  - Why doesn't this contradict what we saw earlier about ROT-K?

# Wanted: security definition for symmetric encryption

- **Perfect privacy:** for any $M_0, M_1 \in \mathcal{M}$ and any $C \in \mathcal{C}$:

$$\Pr[\mathcal{E}_K(M_0) = C] = \Pr[\mathcal{E}_K(M_1) = C]$$

- Security holds for *any* adversary (no limit on resource usage)

- Very strict requirements:
  - Keys need to be as long as message
  - Key can only be used for one message

# Wanted: security definition for symmetric encryption

- **Perfect privacy:** for any $M_0, M_1 \in \mathcal{M}$ and any $C \in \mathcal{C}$:

$$\Pr[\mathcal{E}_K(M_0) = C] = \Pr[\mathcal{E}_K(M_1) = C]$$

- Security holds for *any* adversary (no limit on resource usage)

- Very strict requirements:
  - Keys need to be as long as message…want keys to be short
  - Key can only be used for one message…want to encrypt many messages

# Modern cryptography – idea

- ~~Perfect~~ Computational **privacy:** for any $M_0, M_1 \in \mathcal{M}$ and any $C \in \mathcal{C}$:

$$\Pr[\mathcal{E}_K(M_0) = C] \not= \Pr[\mathcal{E}_K(M_1) = C]$$

$$\approx$$

- Security holds for *any* (*resource bounded*) adversary ~~(no limit on resource usage)~~

- Very strict requirements:
  - ~~Keys need to be as long as message~~…want keys to be short ✓
  - ~~Key can only be used for one message~~…want to encrypt many messages ✓

# Outline of course

| | Message privacy | Message integrity / authentication |
|---|---|---|
| **Symmetric keys** | Symmetric encryption | Message authentication codes (MAC) |
| **Asymmetric keys** | Asymmetric encryption (a.k.a. public-key encryption) | Digital signatures |

# Outline of course

| | Message privacy | Message integrity / authentication |
|---|---|---|
| **Symmetric keys** | Symmetric encryption | Message authentication codes (MAC) |
| **Asymmetric keys** | Asymmetric encryption (a.k.a. public-key encryption) | Digital signatures |

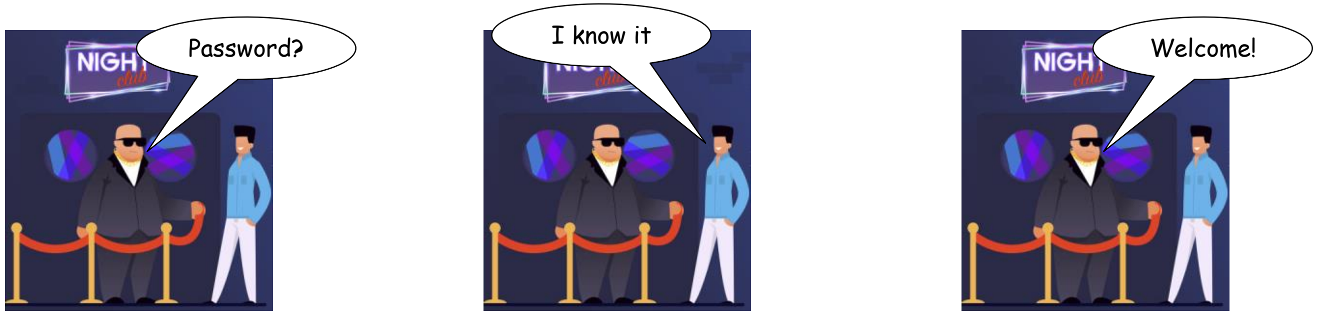
Part I

# Outline of course

| | Message privacy | Message integrity / authentication | |
|---|---|---|---|
| **Symmetric keys** | Symmetric encryption | Message authentication codes (MAC) | |
| **Asymmetric keys** | Asymmetric encryption (a.k.a. public-key encryption) | Digital signatures | Part II |

# Much more to cryptography

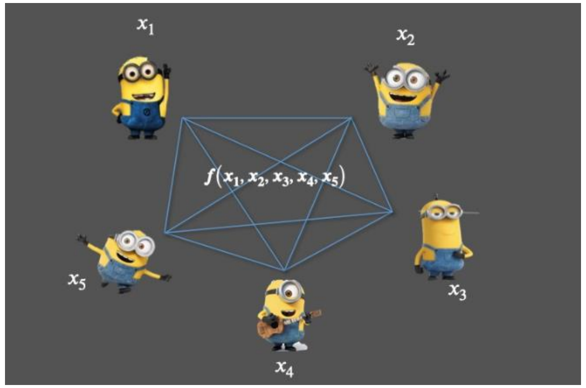
- Zero-knowledge proofs



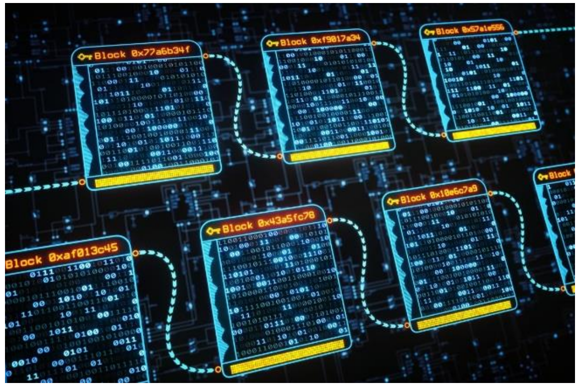

- Fully-homomorphic encryption

$$Enc(K, M_1 + M_2) = Enc(K, M_1) + Enc(K, M_2)$$

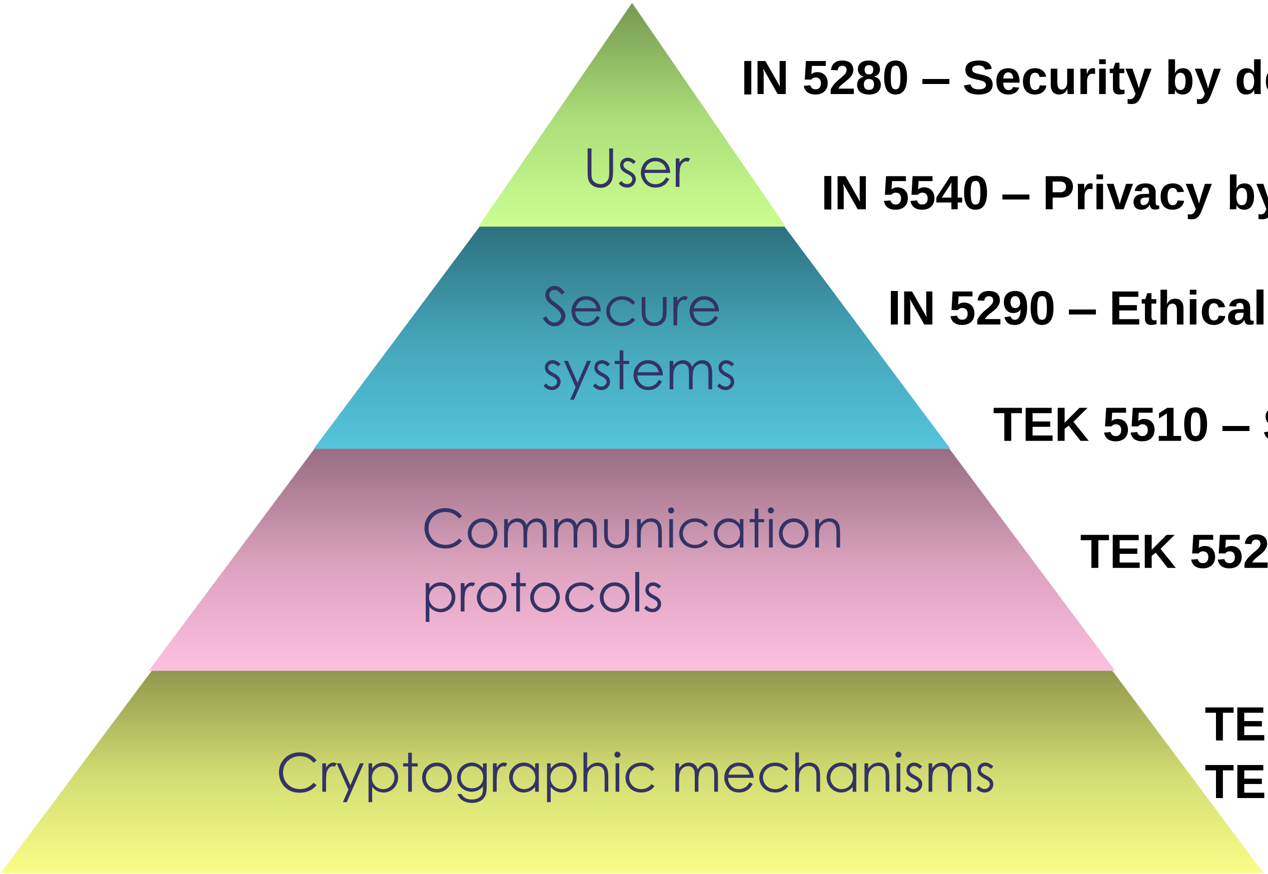
- Multi-party computation




- Blockchain



# The security pyramid




**IN 5280 – Security by design**

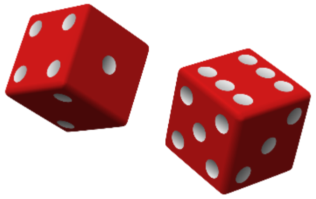
**IN 5540 – Privacy by design**

**IN 5290 – Ethical hacking**

**TEK 5510 – Security in operating systems and software**

**TEK 5520 – Cyber security of industrial systems**

**TEK 4500 – Introduction to cryptography**
**TEK 5550 – Advanced topics in cryptograpy**



# Discrete probability

**the bare minimum**

More detail: https://en.wikibooks.org/wiki/High_School_Mathematics_Extensions/Discrete_Probability

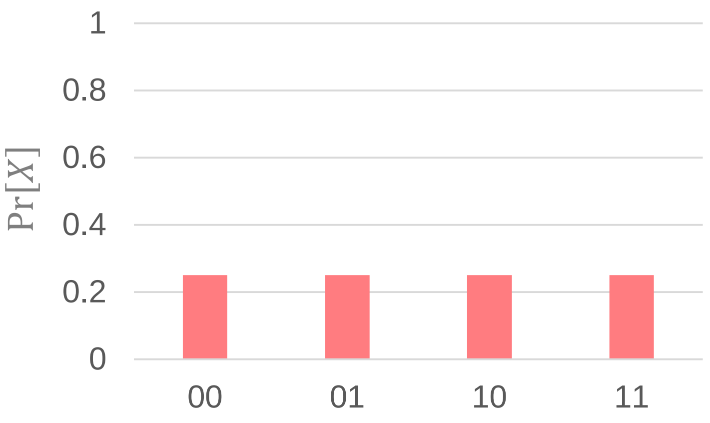
# Discrete probability

- $\mathcal{X}$ – a finite set (e.g. $\mathcal{X} = \{0,1\}^n$)

**Definition:** A **probability distribution** over $\mathcal{X}$ is a function $\Pr : \mathcal{X} \to [0,1]$ such that

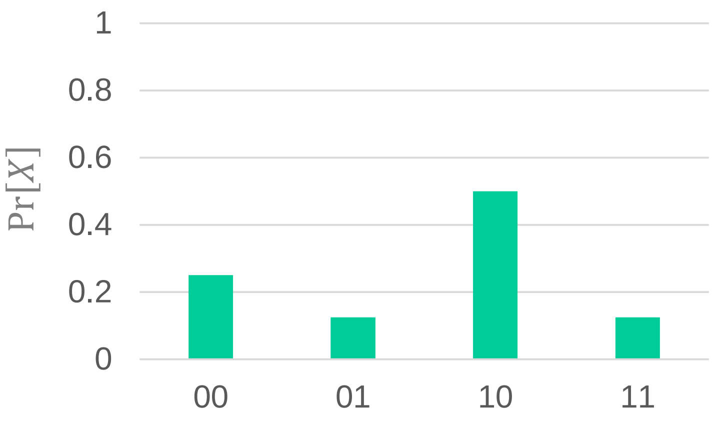
$$\sum_{X \in \mathcal{X}} \Pr[X] = 1$$

$$\mathcal{X} = \{0,1\}^2 = \{00, 01, 10, 11\}$$

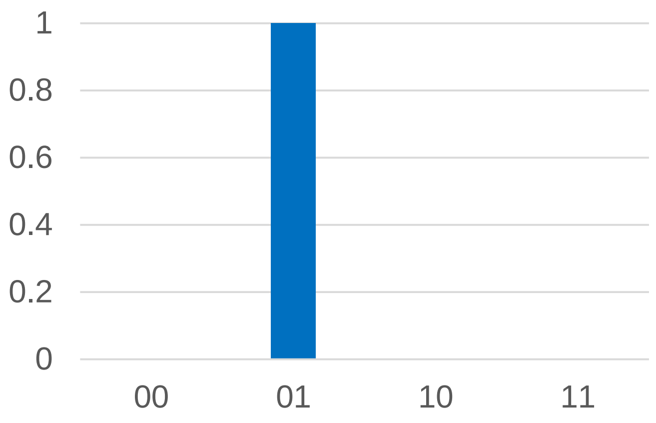



$\Pr[00] = 1/4$
$\Pr[01] = 1/4$
$\Pr[10] = 1/4$
$\Pr[11] = 1/4$

**Uniform distribution**




$\Pr[00] = 1/4$
$\Pr[01] = 1/8$
$\Pr[10] = 1/2$
$\Pr[11] = 1/8$



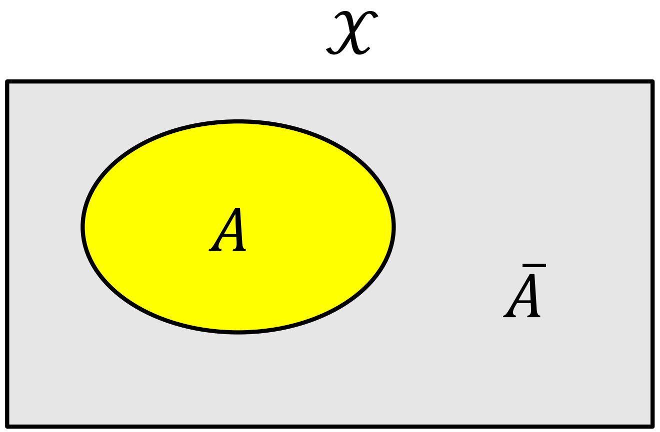

$\Pr[00] = 0$
$\Pr[01] = 1$
$\Pr[10] = 0$
$\Pr[11] = 0$

**Point distribution**

# Discrete probability

- A subset $A \subseteq \mathcal{X}$ is called an **event** and $\Pr[A] = \sum_{X \in \mathrm{A}} \Pr[X]$

- The **complement** of $A$ is $\mathcal{X} \setminus A$ and denoted $\bar{A}$
  - Fact: $\Pr[\bar{A}] = 1 - \Pr[A]$



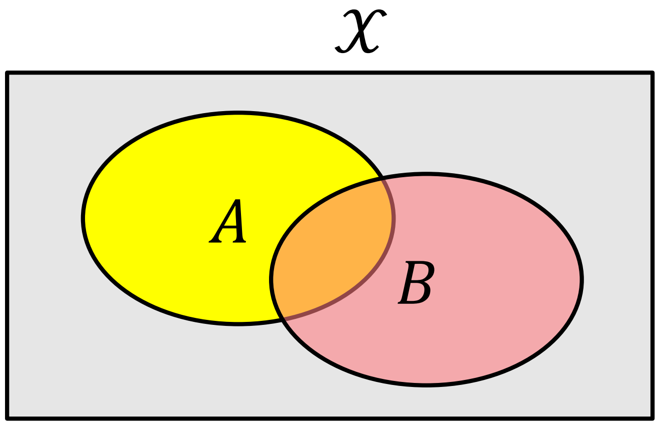

- **Example**: $\mathcal{X} = \{0,1\}^8$

$$A = \{X \in \mathcal{X} \mid X = 1\,1xx\;xxxx\} \subset \mathcal{X}$$

With the uniform distribution over $\mathcal{X}$, what is $\Pr[A]$?

**Answer:** $\Pr[A] = \Pr[1100\;0000] + \Pr[1100\;0001] + \cdots + \Pr[1111\;1111]$
$= 2^6 \cdot 1/\,2^8$
$= 1/2^2$
$= 1/4$

# Union bound and independence




- **Union bound:** For events $A$ and $B$ in $\mathcal{X}$:

$$\Pr[A \cup B] \leq \Pr[A] + \Pr[B]$$

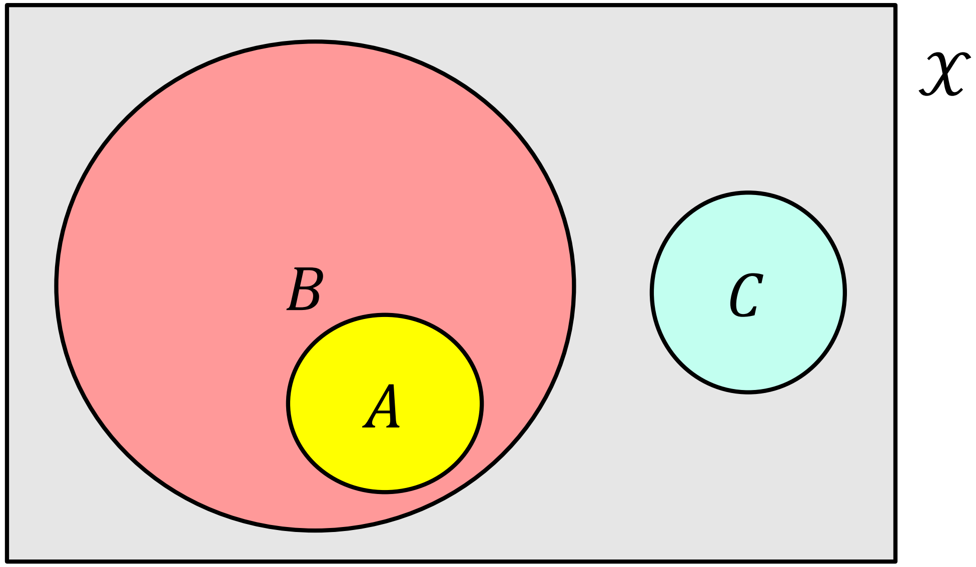
- Events $A$ and $B$ are **independent** if $\Pr[A \text{ and } B] = \Pr[A] \cdot \Pr[B]$

# Law of total probability

- Conditional probability

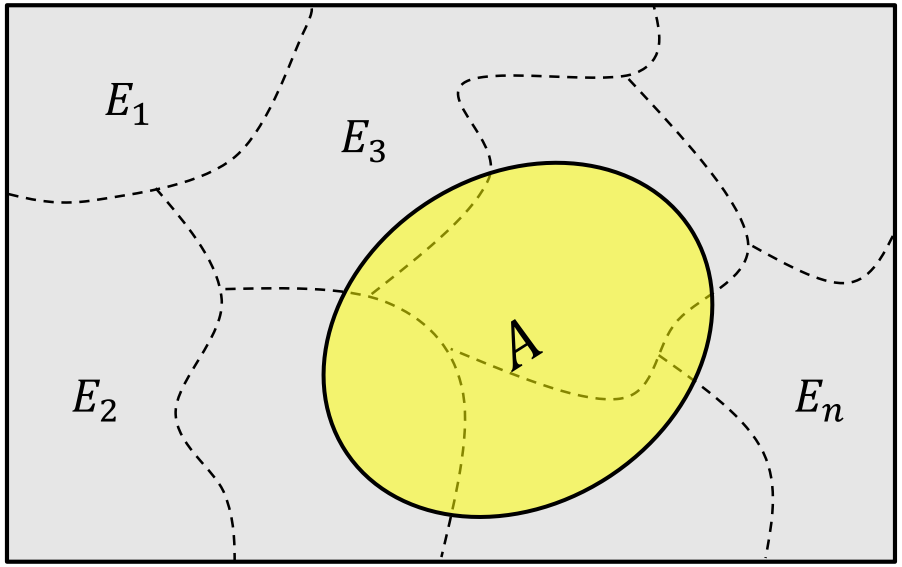
$$\Pr[A \mid B] > \Pr[A]$$

$$\Pr[A \mid C] = 0$$




- **Total probability:**

$$\begin{aligned}\Pr[A] = \Pr[A \mid E_1] \cdot \Pr[E_1] \\ + \Pr[A \mid E_2] \cdot \Pr[E_2] \\ \vdots \\ + \Pr[A \mid E_n] \cdot \Pr[E_n]\end{aligned}$$



# Randomized algorithms

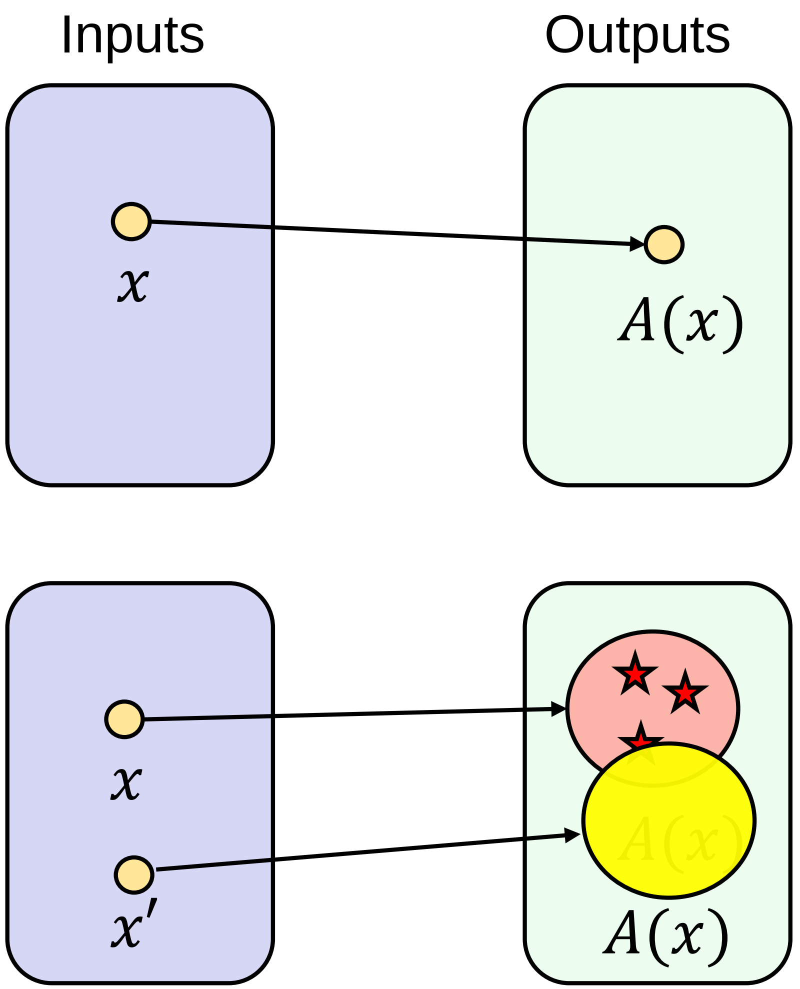
- Deterministic algorithm:

$$y \leftarrow A(x)$$

- Randomized algorithm:

$$y \leftarrow A(x; r) \qquad \text{where } r \xleftarrow{\$} \{0,1\}^n$$

$$y \xleftarrow{\$} A(x)$$



# Next week

- Block ciphers
- Pseudorandom functions and pseuorandom permutations
- DES, AES