Lecture 1 – Introduction to cryptography

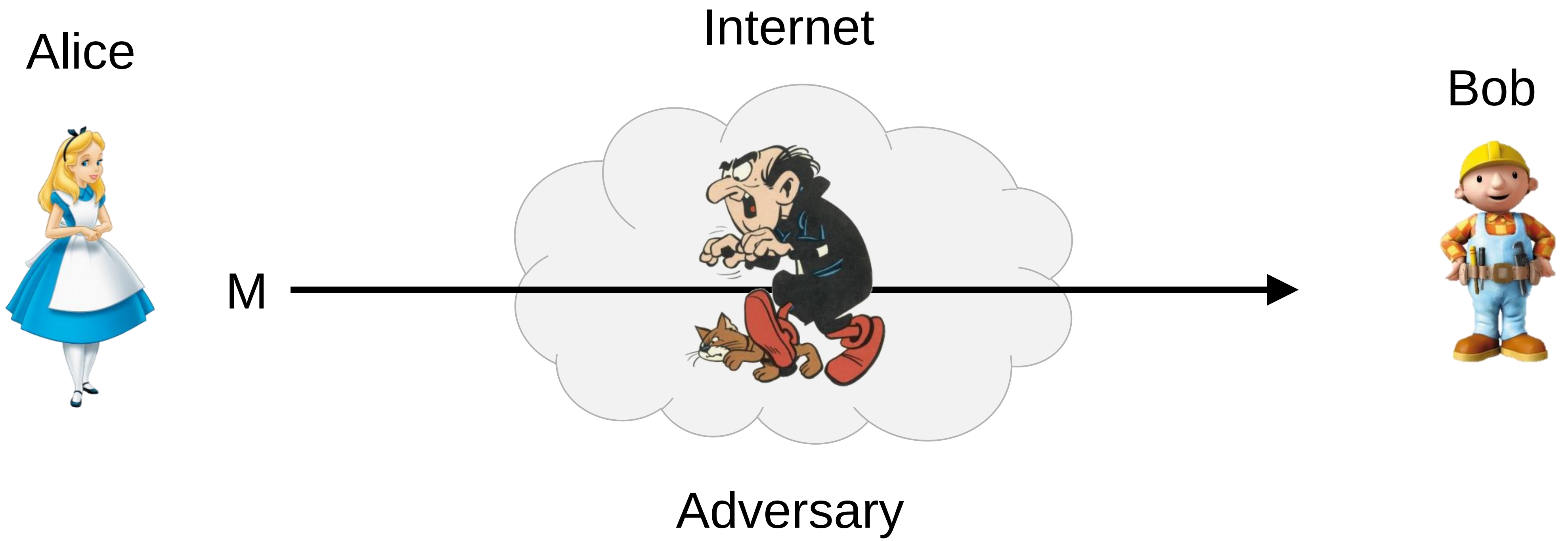
TEK4500

30.08.2023

Håkon Jacobsen

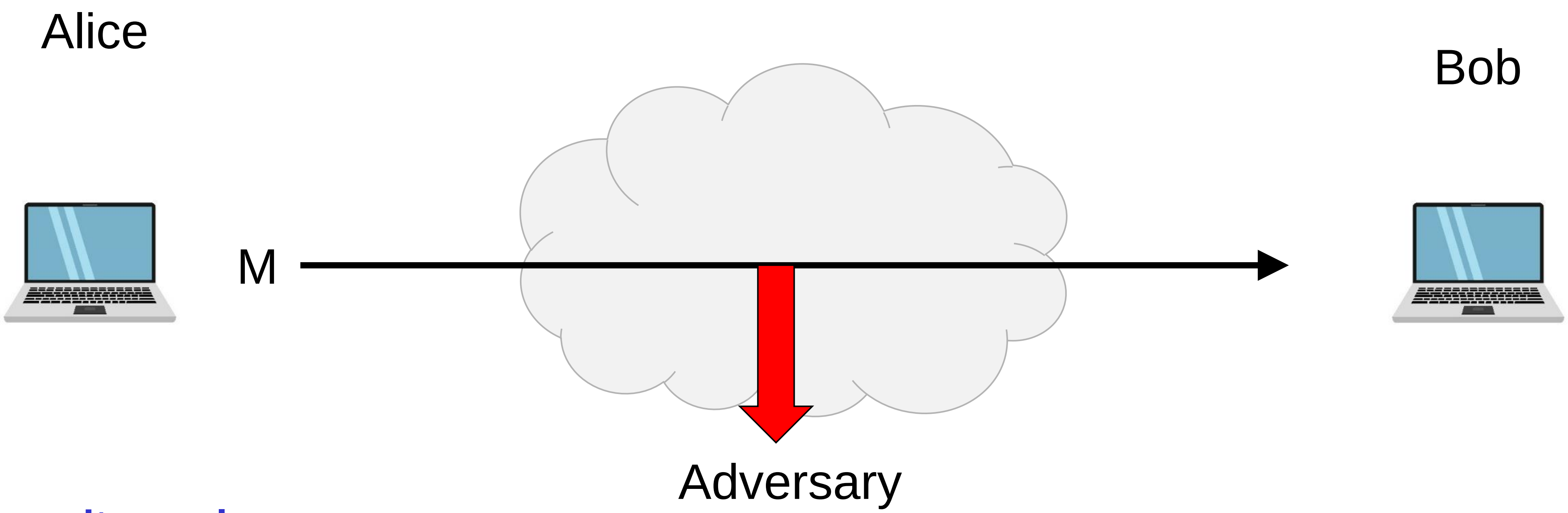
hakon.jacobsen@its.uio.no

What is cryptography?



What is cryptography?

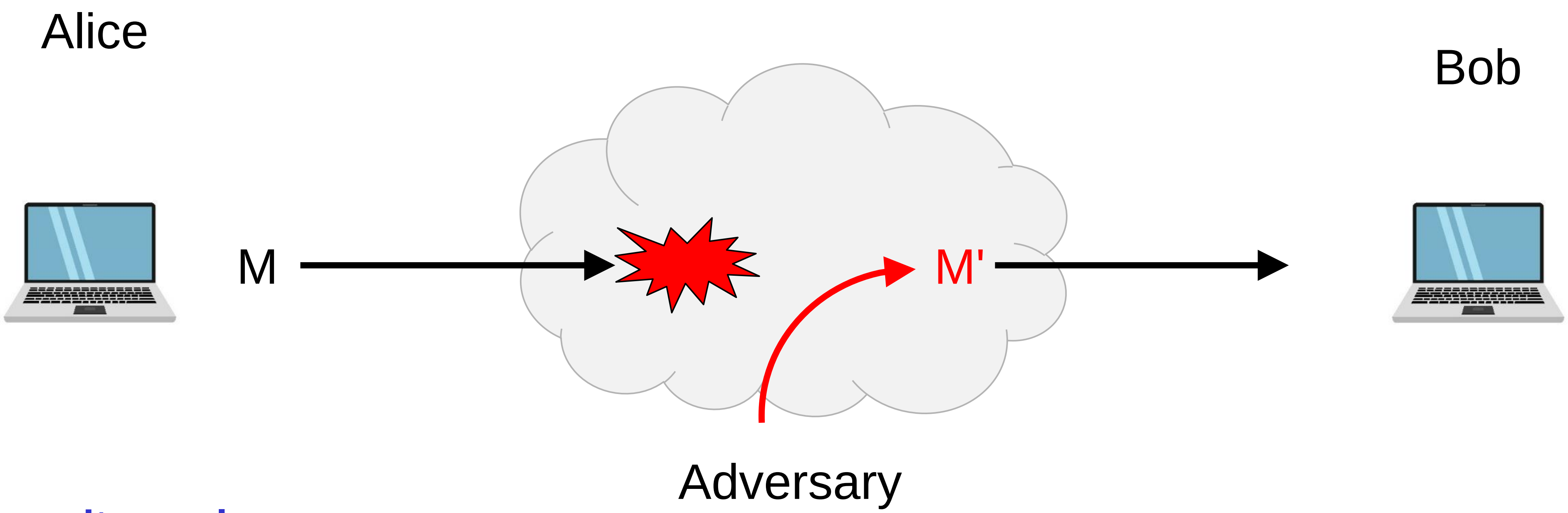
What is cryptography?



Security goals:

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

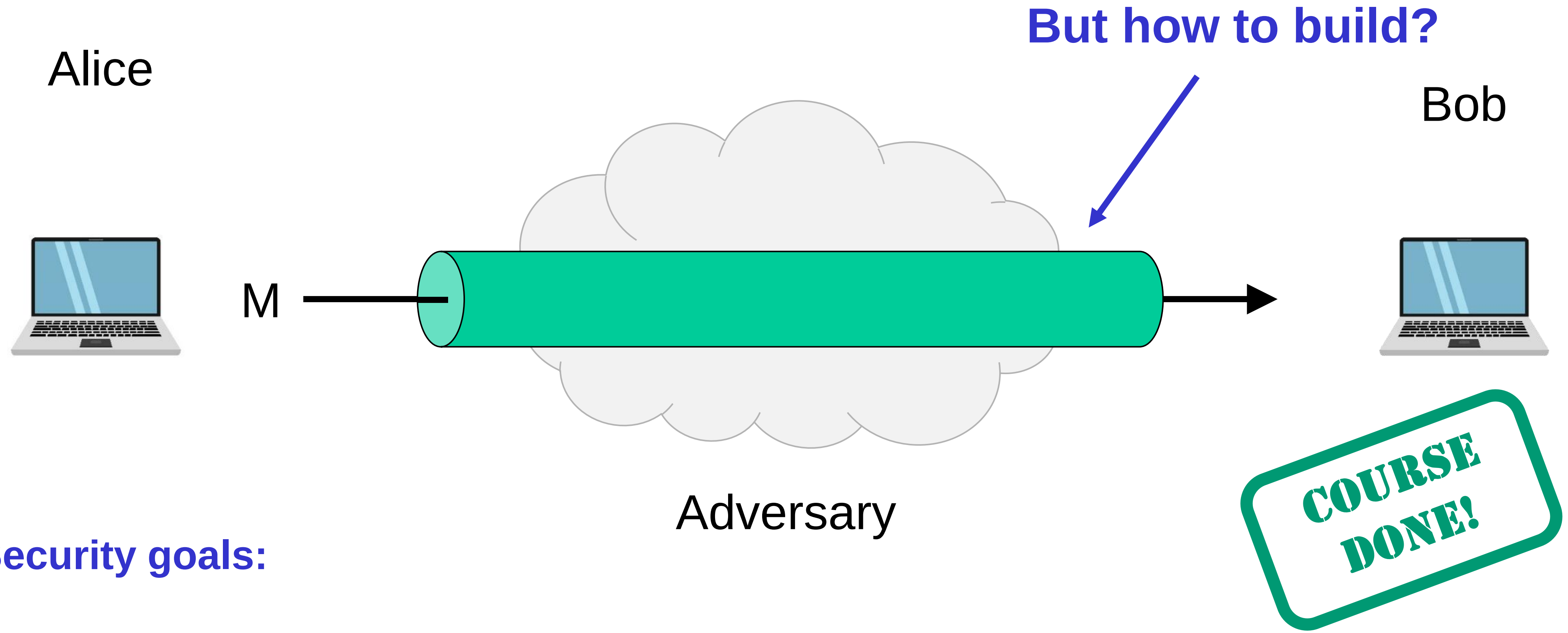
What is cryptography?



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

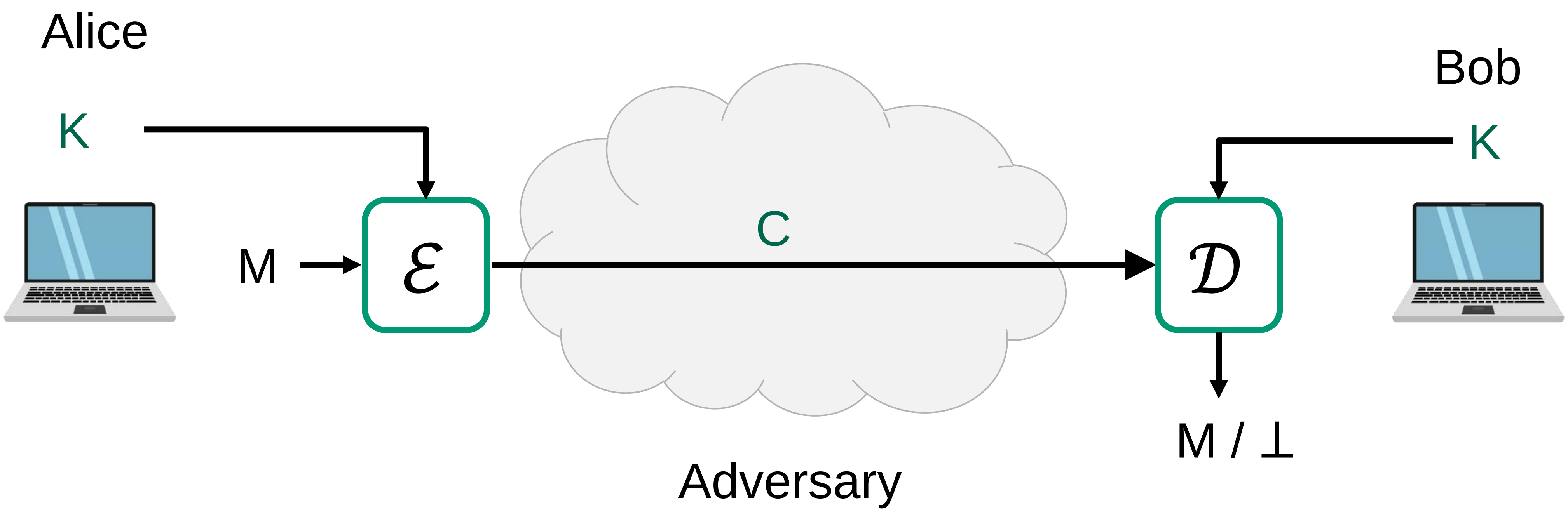
Ideal solution: secure channels



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

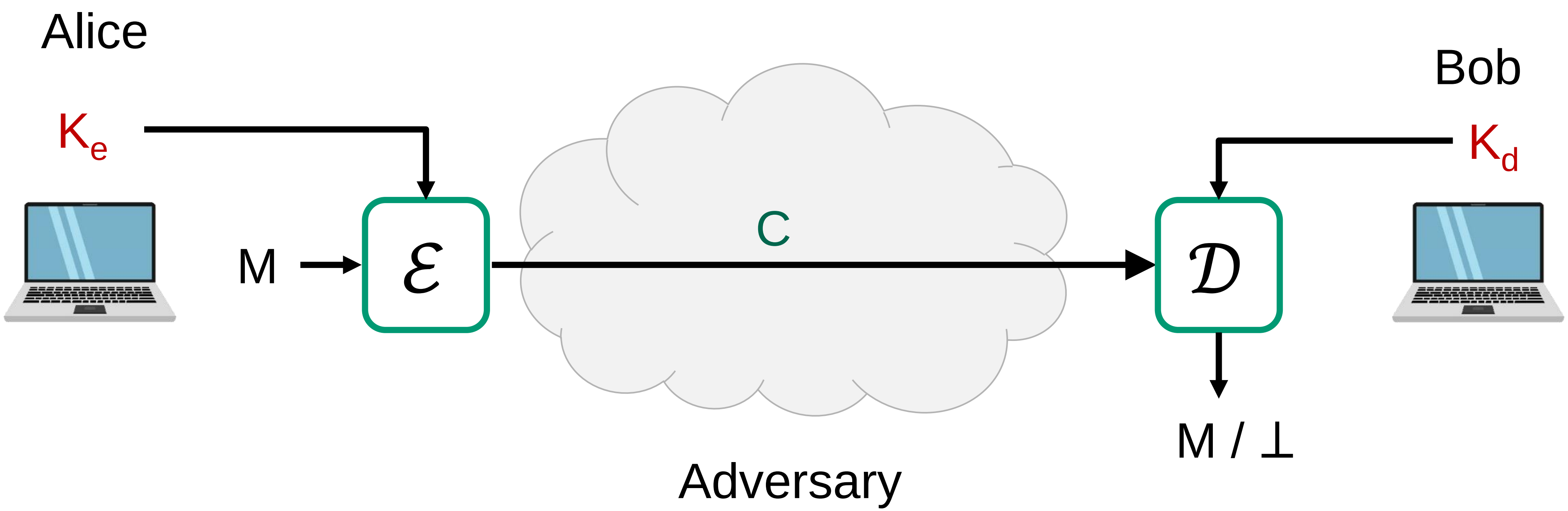


$\mathcal{E}$: encryption algorithm (public)

$\mathcal{D}$: 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 (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 (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
  - $1, 1001, 10, 10001101000001 \in \{0,1\}^*$
- 1^n or 0^n – string of n "ones" (or "zeros")
  - $1^5 = 11111$
  - $0^3 = 000$
- $F : \mathcal{X} \to \mathcal{Y}$ – function from set $\mathcal{X}$ to set $\mathcal{Y}$
  - $F : \{0,1\}^5 \to \{0,1\}^3$
  - $G : \{A, B, C, D\} \to \{0,1,2, \dots\}$
- $\forall$ – "for all"
  - "$\forall X \in \{0,1\}^4 \dots$" $=$ "for all bitstrings of length 4…"
- $\exists$ – "there exists"
  - "$\exists X \in \{0,1,2, \dots\}$ such that $X > 13$"
- $\mathcal{X} \times \mathcal{Y}$ – set of pairs (X, Y) with $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$
  - $F : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ function taking two inputs $X \in \mathcal{X}$, $Y \in \mathcal{Y}$ and producing single output $Z \in \mathcal{Z}$
- $X \leftarrow 5$ – "assign value 5 to X"
- $X \xleftarrow{\$} \mathcal{X}$ – "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:

$\mathcal{K} = \{0,1\}^{128}$ $\quad \mathcal{M} = \{0,1\}^*$ $\quad \mathcal{C} = \{0,1\}^*$

$\mathcal{K} = \{0,1\}^{128}$ $\quad \mathcal{M} = \{A, B, \dots, Z\}$ $\quad \mathcal{C} = \{A, B, \dots, Z\}$

$\mathcal{K} = \{0,1\}^{128}$ $\quad \mathcal{M} = \{\mathrm{YES}, \mathrm{NO}\}$ $\quad \mathcal{C} = \{0,1\}^*$

$\mathcal{K} = \{1, \dots, p\}$ $\quad \mathcal{M} = \{A, B, \dots, Z\}$ $\quad \mathcal{C} = \{0,1\}^*$

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 M from C
- Hard to recover K 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

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

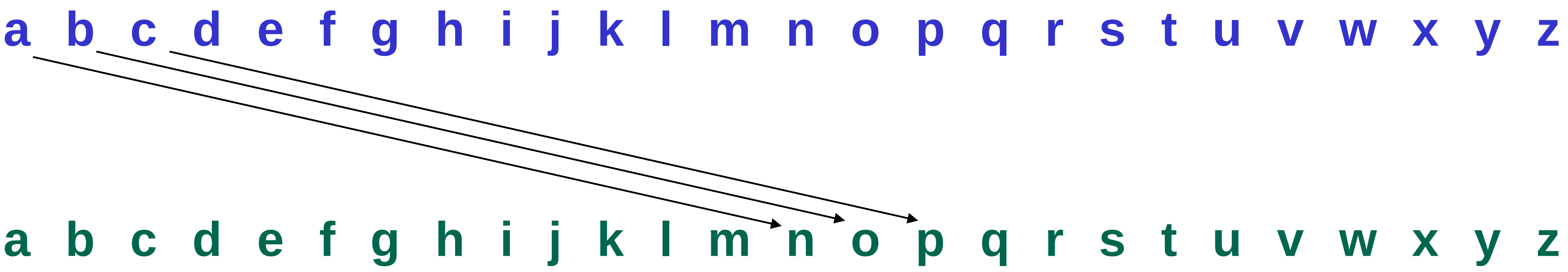
...

a 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

```
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

Ceasar cipher

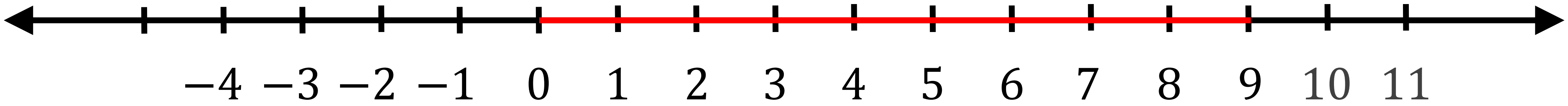
- a ↔ 0
- b ↔ 1
- c ↔ 2
- d ↔ 3
- e ↔ 4

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

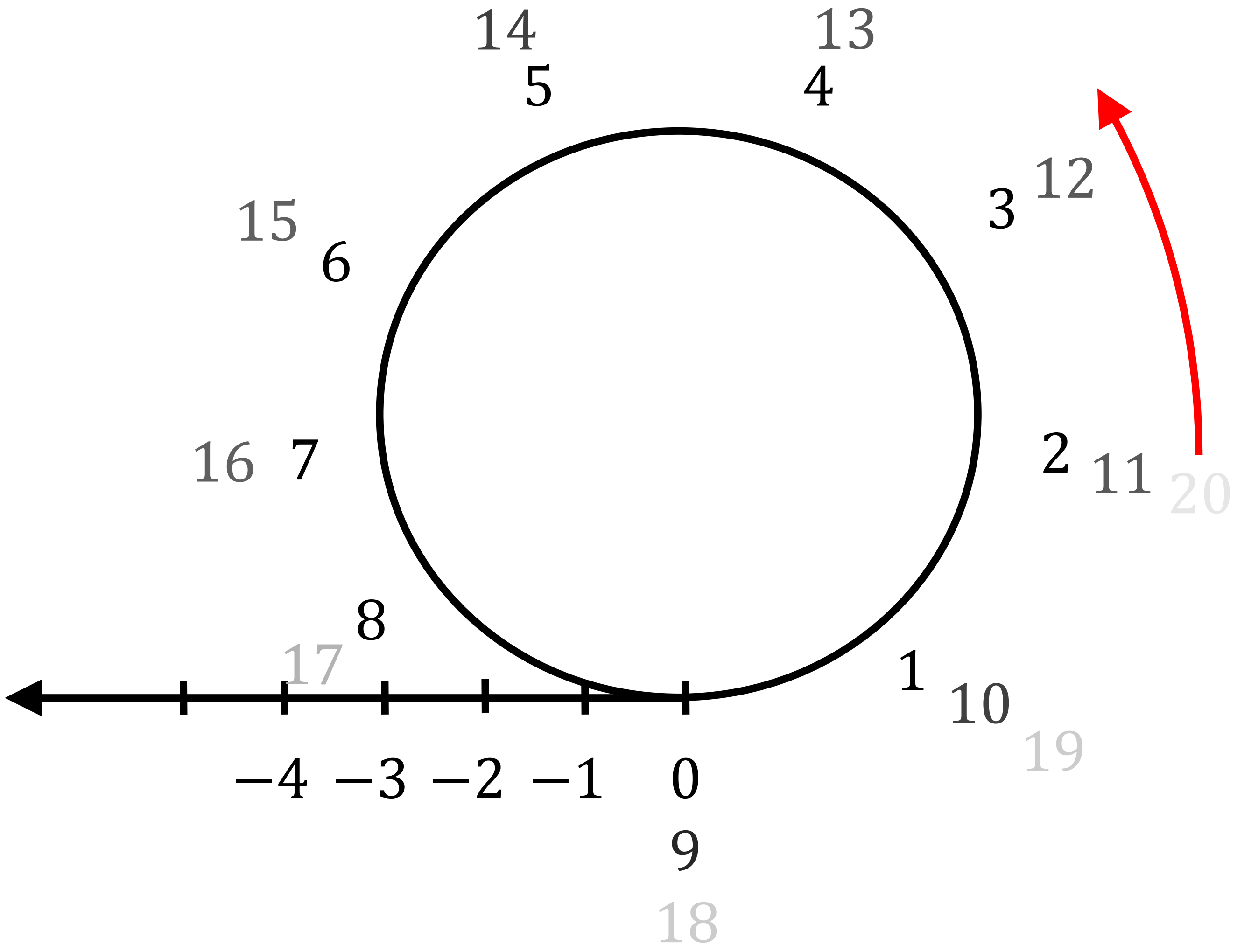
⋮

- z ↔ 25

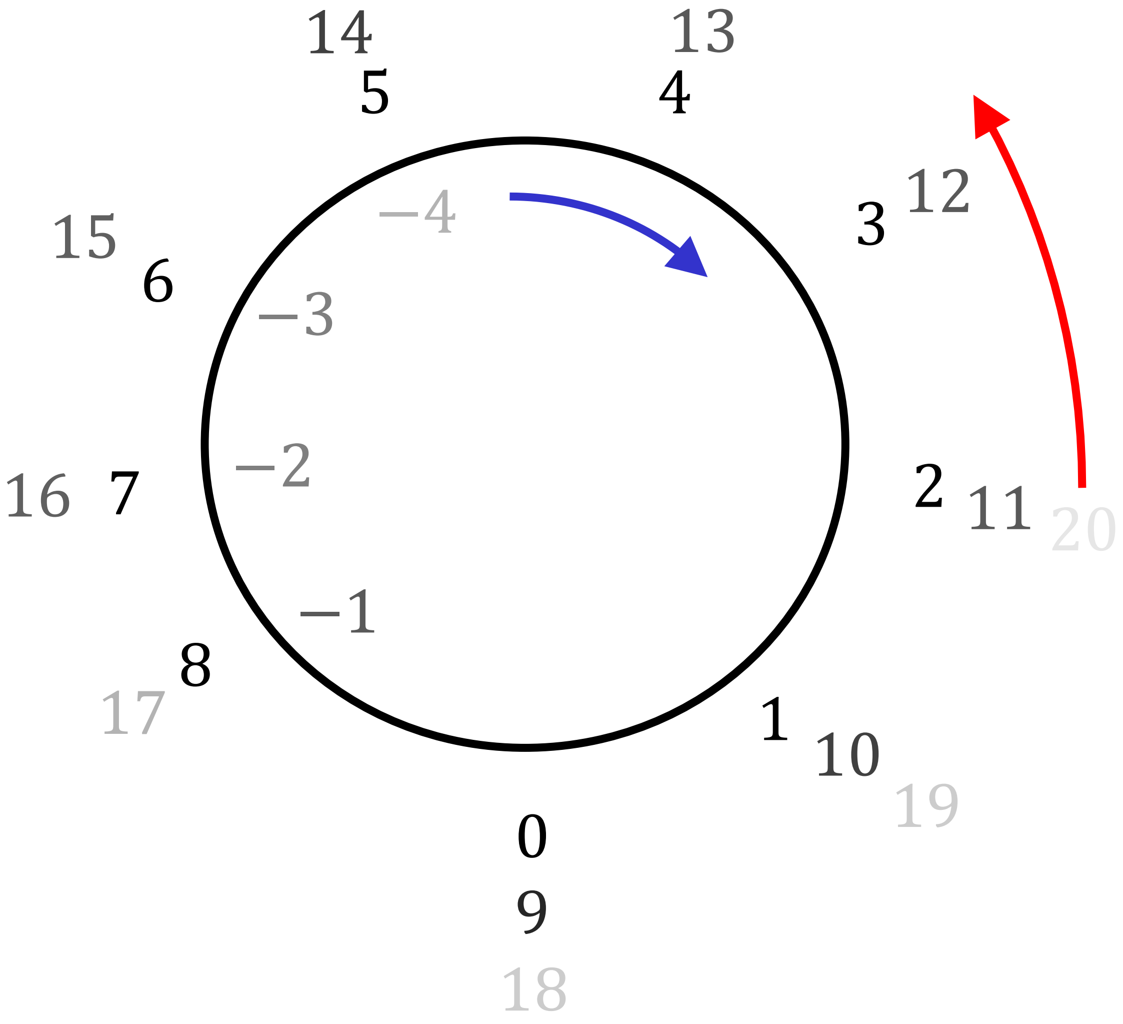
Modular arithmetic



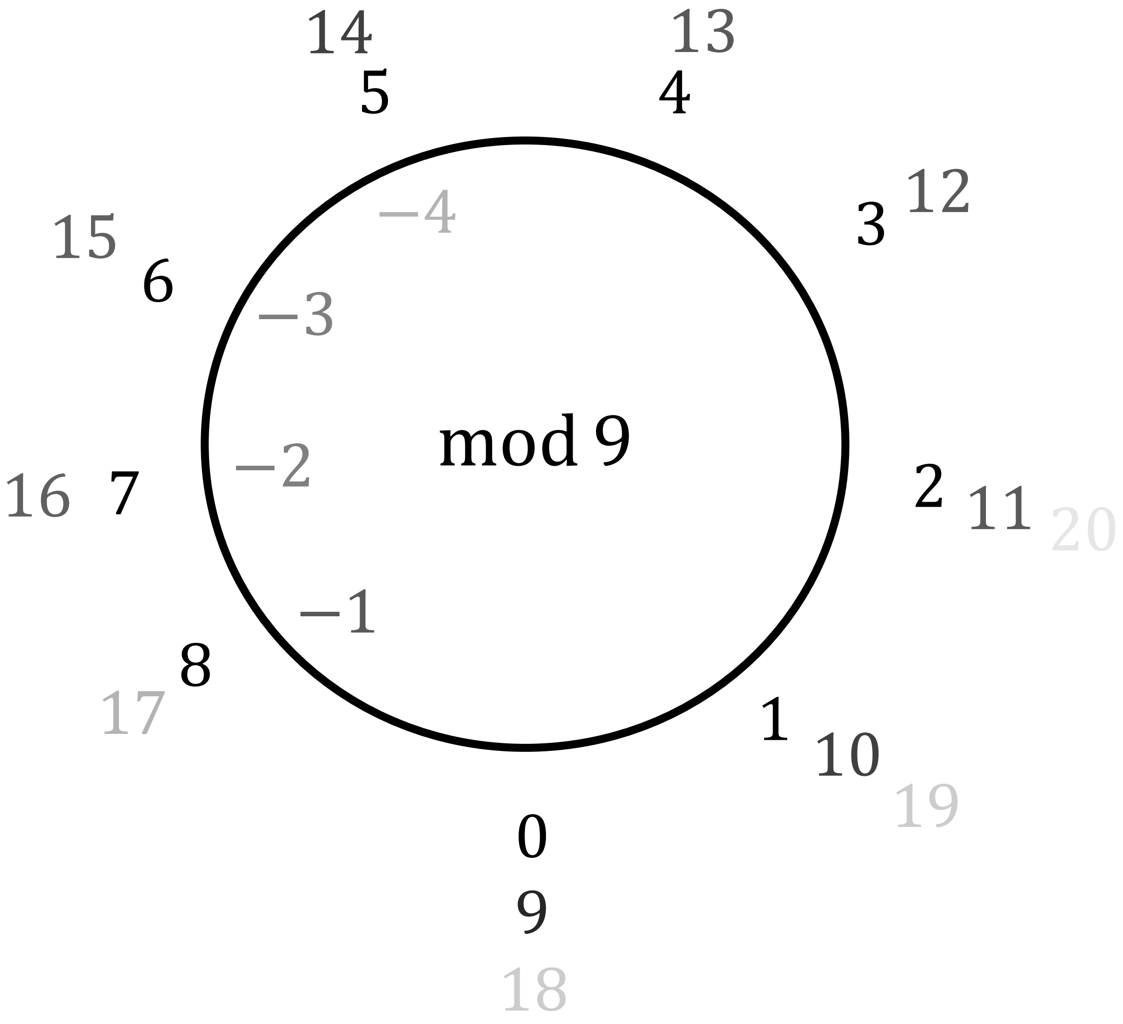
Modular arithmetic



Modular arithmetic



Modular arithmetic



$1 + 3 = 4$

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

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

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

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

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

$r < 9$

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

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

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

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

$$\mathcal{K} = \{13\}$$

$$\mathcal{E} : \mathcal{K} \times \mathcal{M} \to \mathcal{C} \qquad \mathcal{M} = \{0,1,2,\ldots,25\}$$

$$\mathcal{D} : \mathcal{K} \times \mathcal{C} \to \mathcal{M} \qquad \mathcal{C} = \{0,1,2,\ldots,25\}$$

ROT-K

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

⋮

- z ↔ 25

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

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

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

$$\mathcal{E} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C} \qquad \mathcal{M} = \{0,1,2,\ldots,25\}$$

$$\mathcal{D} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M} \qquad \mathcal{C} = \{0,1,2,\ldots,25\}$$

Attacking ROT-K

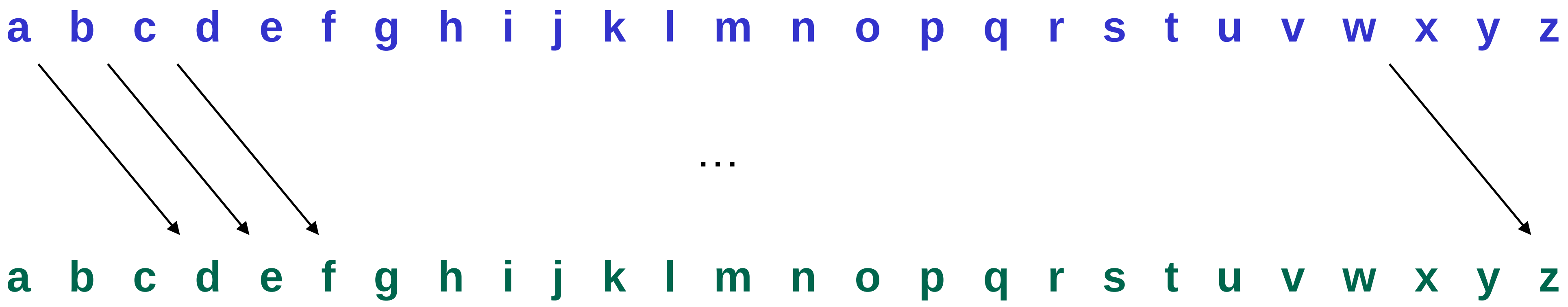
$|\mathcal{K}| = 26$

K	M
0	va gur sne qvfgnapr n uryvpbcgre …

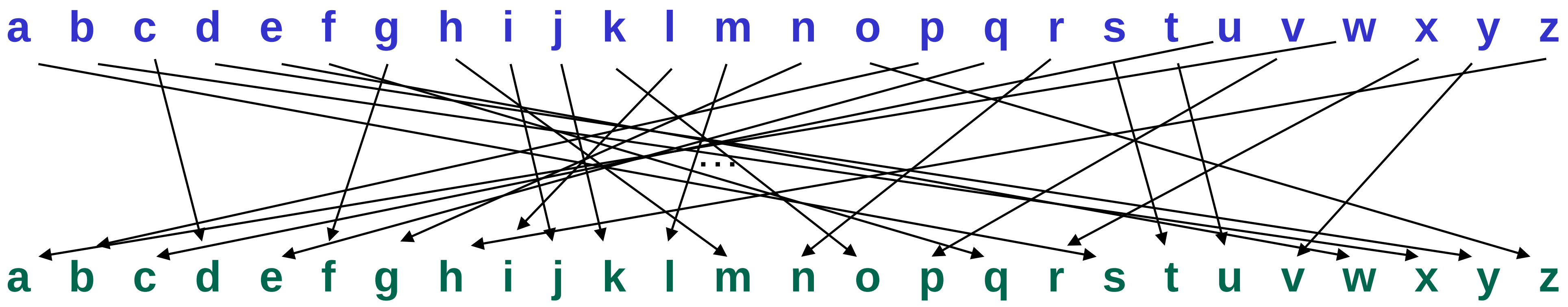
C = va gur sne qvfgnapr n uryvpbcgre …

Conclusion: key space must be large enough!

Substitution cipher



Substitution cipher



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

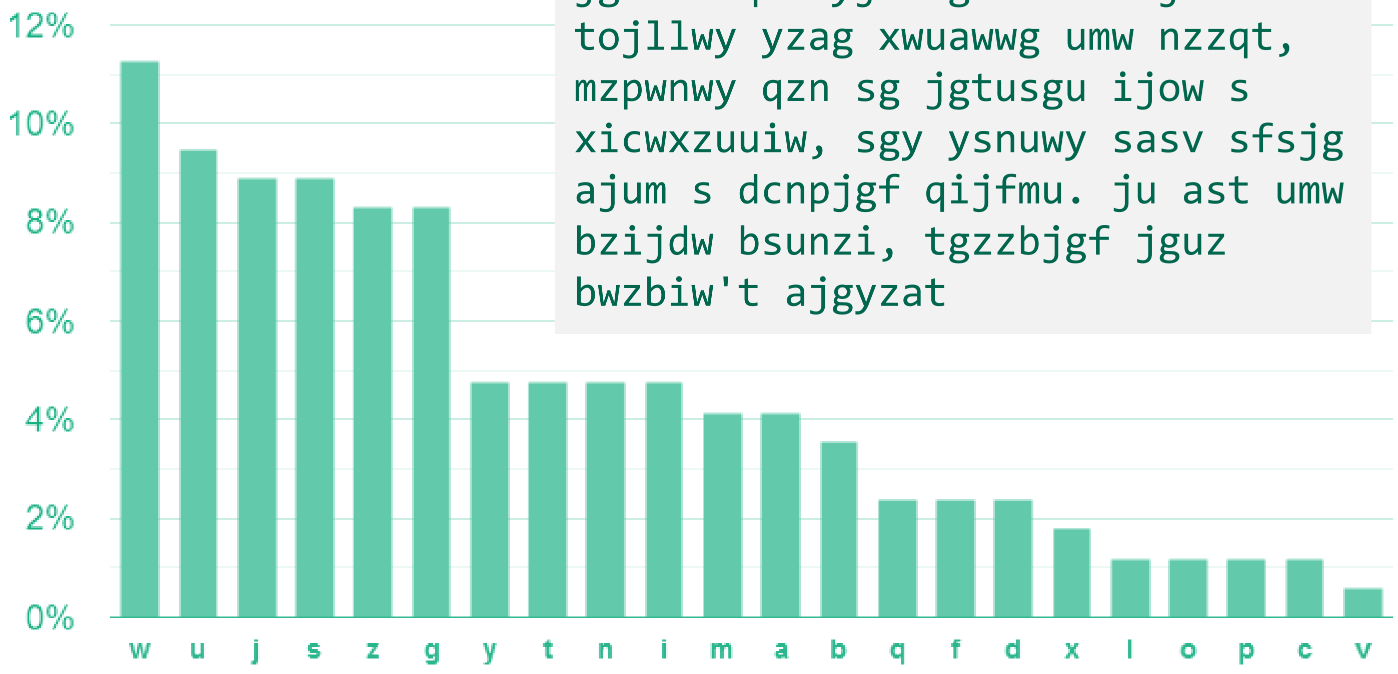
```
in the far distance a helicopter skimmed down between the roofs,
hovered for an instant like a bluebottle, and darted away again
with a curving flight. It was the police patrol, snooping into
people's windows
```

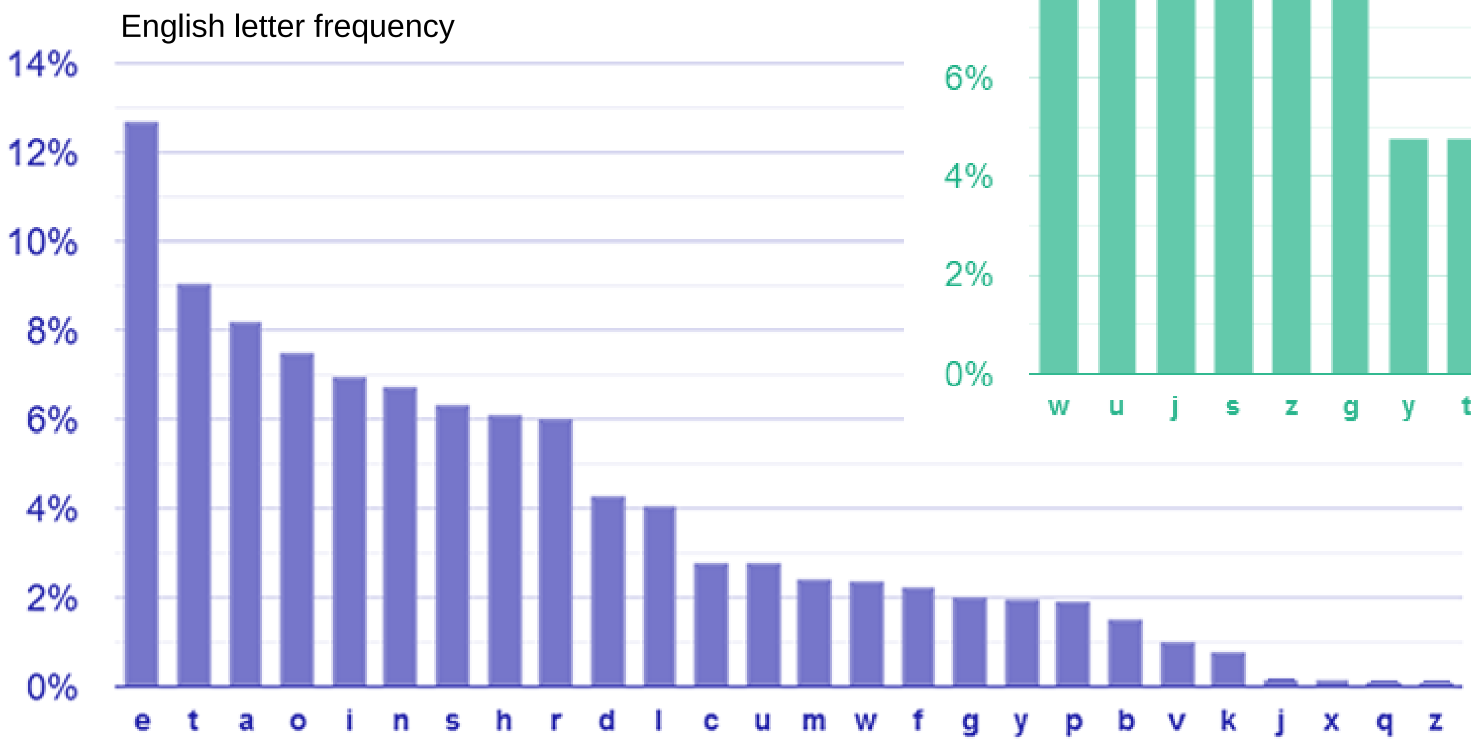
```
jg umw qsn yjtusgdw s mwijdzbuwn tojllwy yzag xwuawwg umw nzzqt,
mzpwnwy qzn sg jgtusgu ijow s xicwxzuuiw, sgy ysnuwy sasv sfsjg
ajum s dcnpjgf qijfmu. ju ast umw bzijdw bsunzi, tgzzbjgf jguz
bwzbiw't ajgyzat
```

Attacking the substitution cipher

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

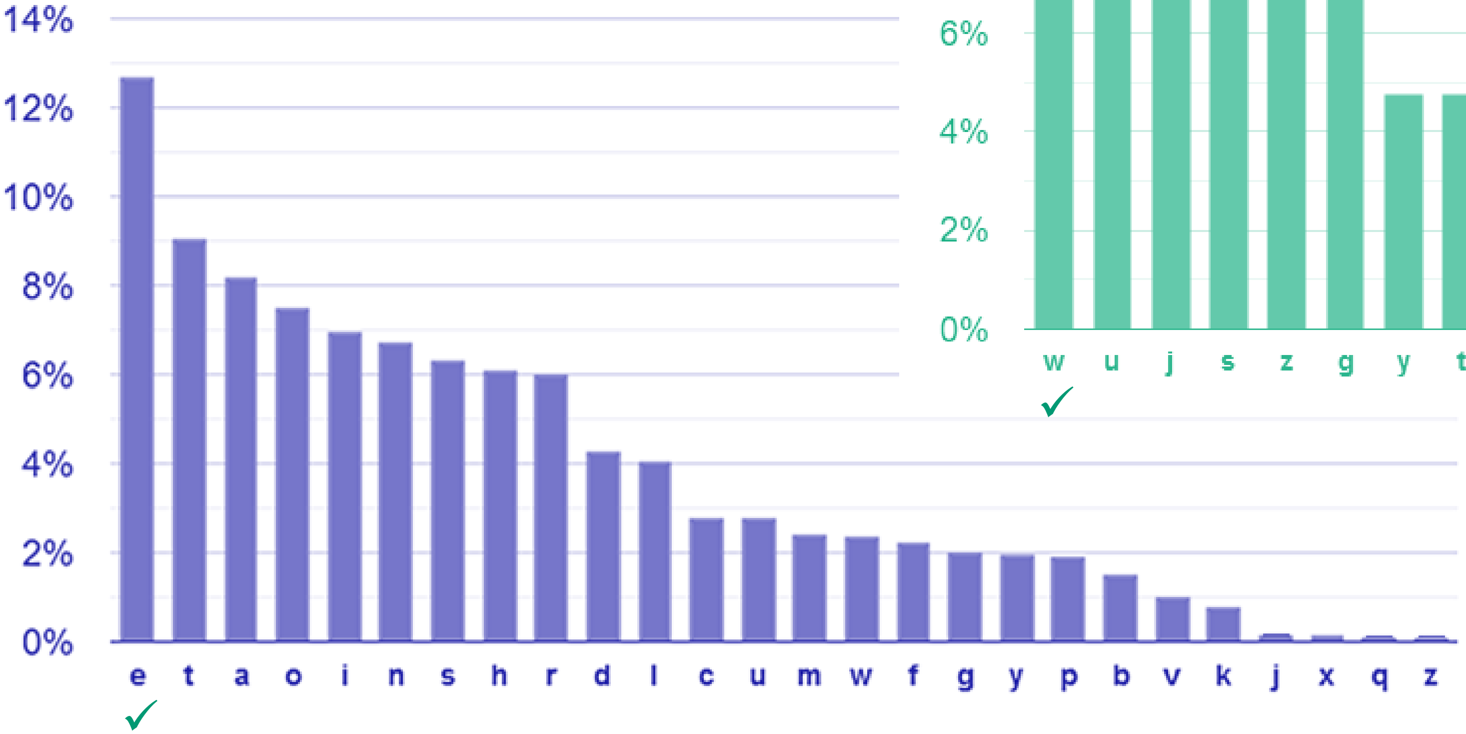
```
jg umw qsn yjtusgdw s mwijdzbuwn
tojllwy yzag xwuawwg umw nzzqt,
mzpwnwy qzn sg jgtusgu ijow s
xicwxzuuiw, sgy ysnuwy sasv sfsjg
ajum s dcnpjgf qijfmu. ju ast umw
bzijdw bsunzi, tgzzbjgf jguz
bwzbiw't ajgyzat
```

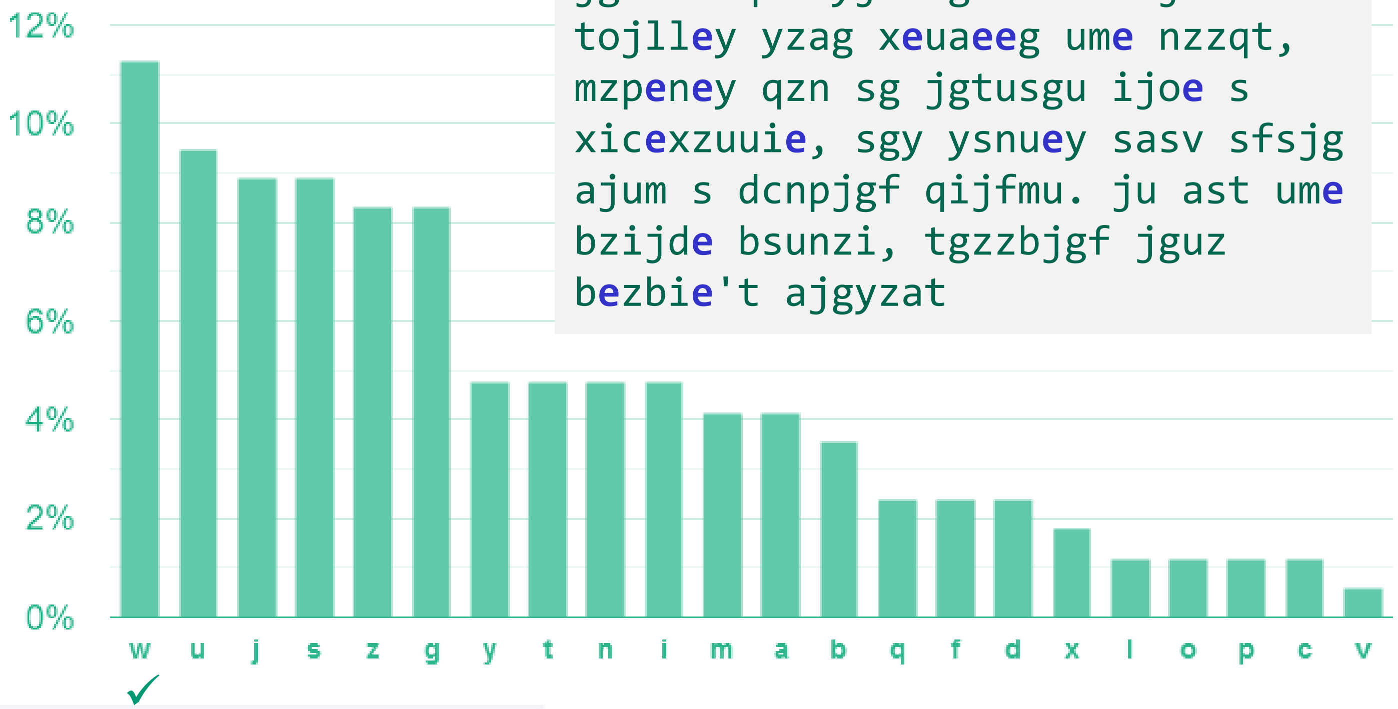




Attacking the substitution cipher

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

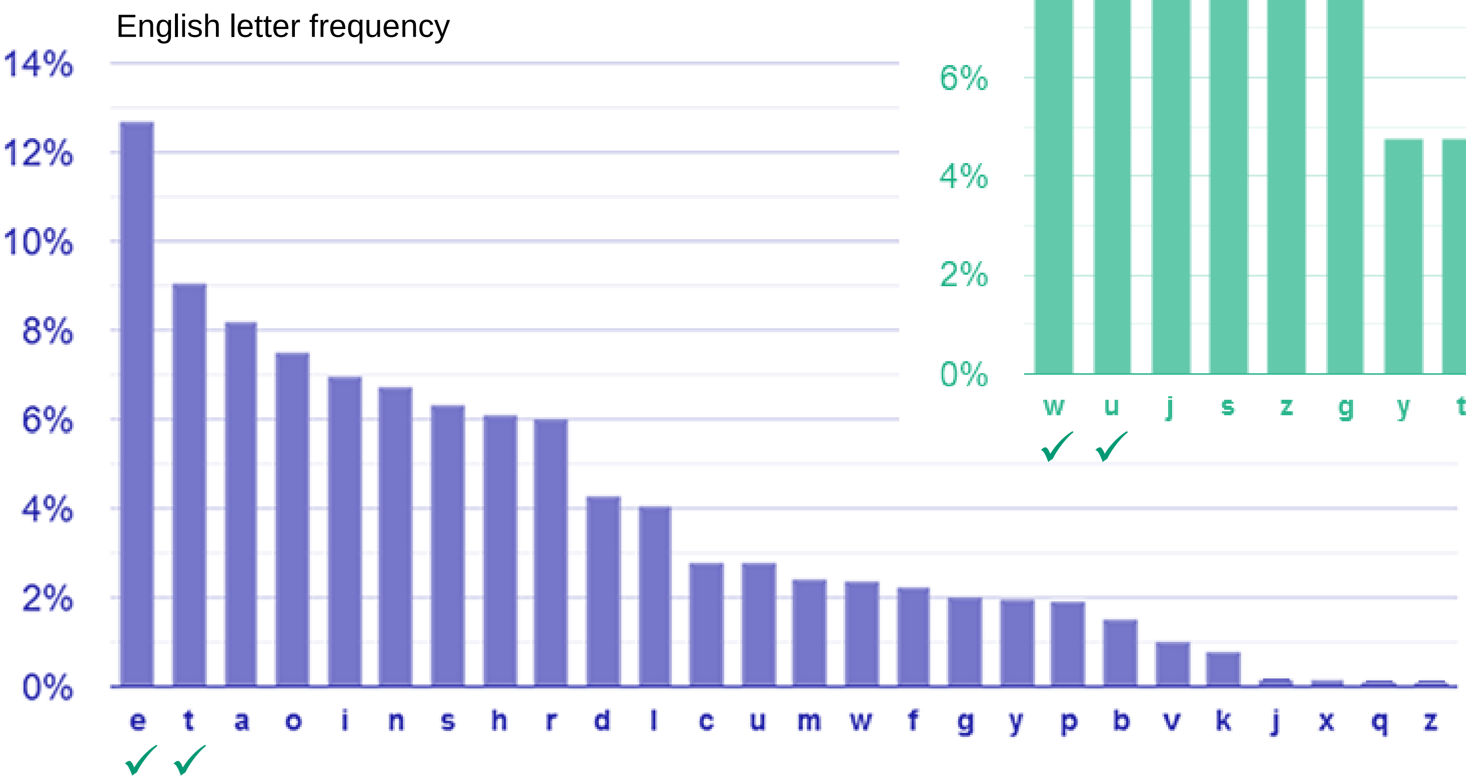


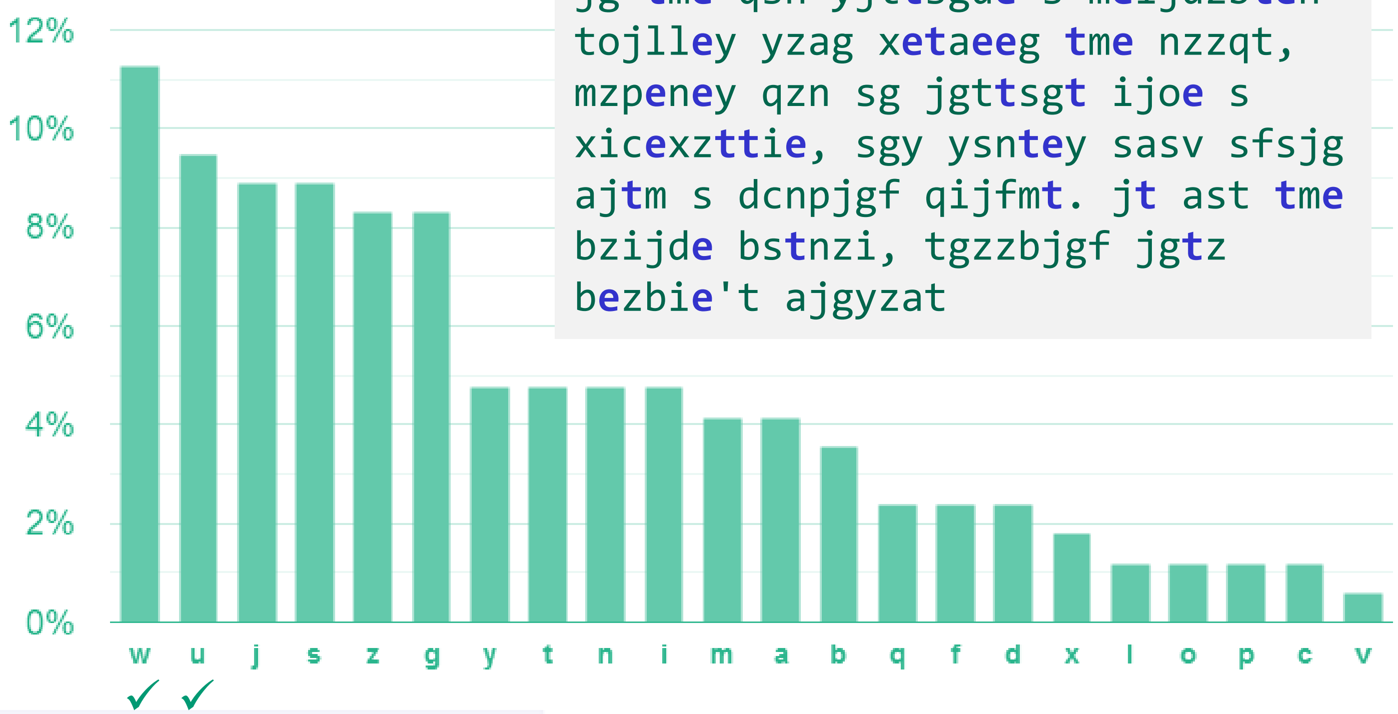



```
jg ume qsn yjtusgde s meijdzbuen
tojlley yzag xeuaeeg ume nzzqt,
mzpeney qzn sg jgtusgu ijoe s
xicexzuuie, sgy ysnuey sasv sfsjg
ajum s dcnpjgf qijfmu. ju ast ume
bzijde bsunzi, tgzzbjgf jguz
bezbie't ajgyzat
```

Attacking the substitution cipher

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

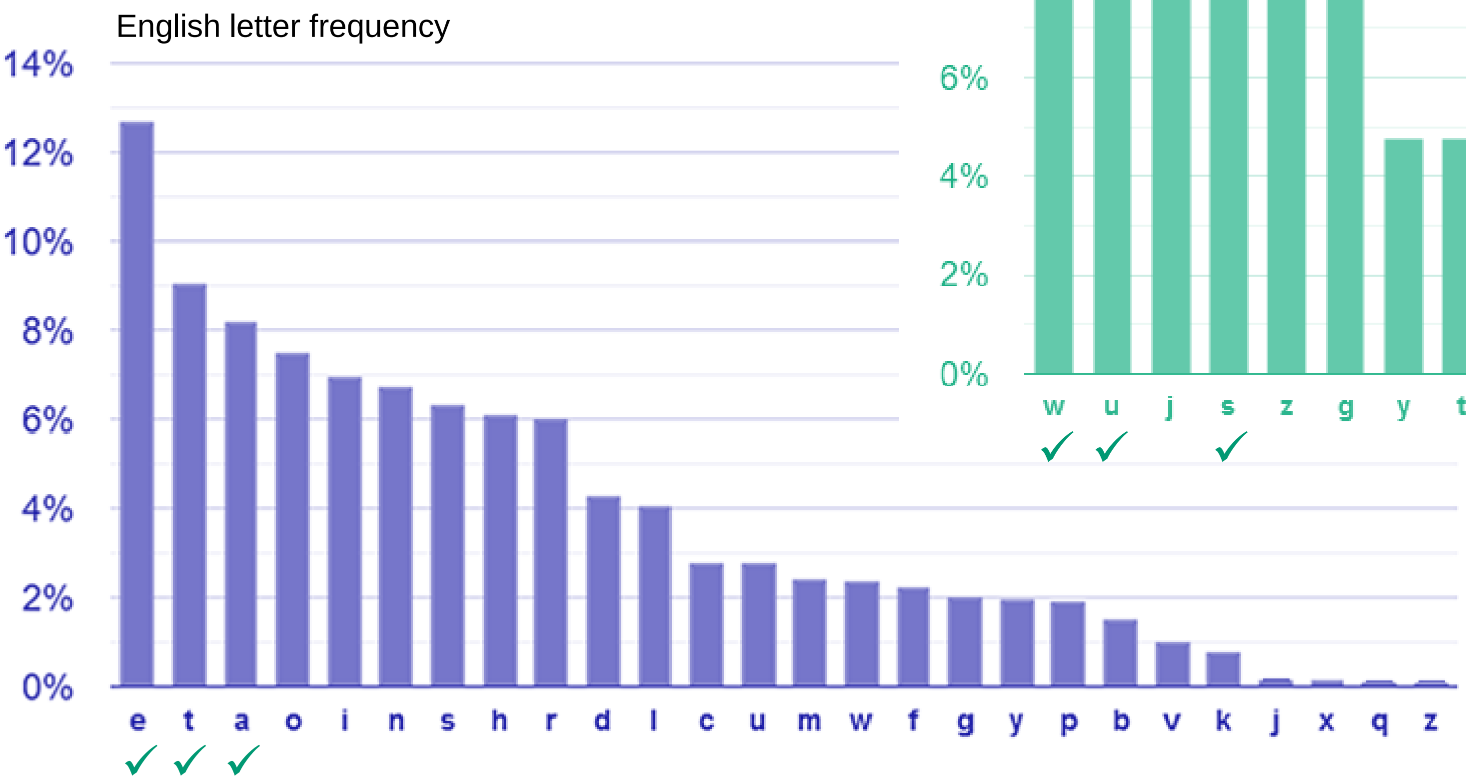


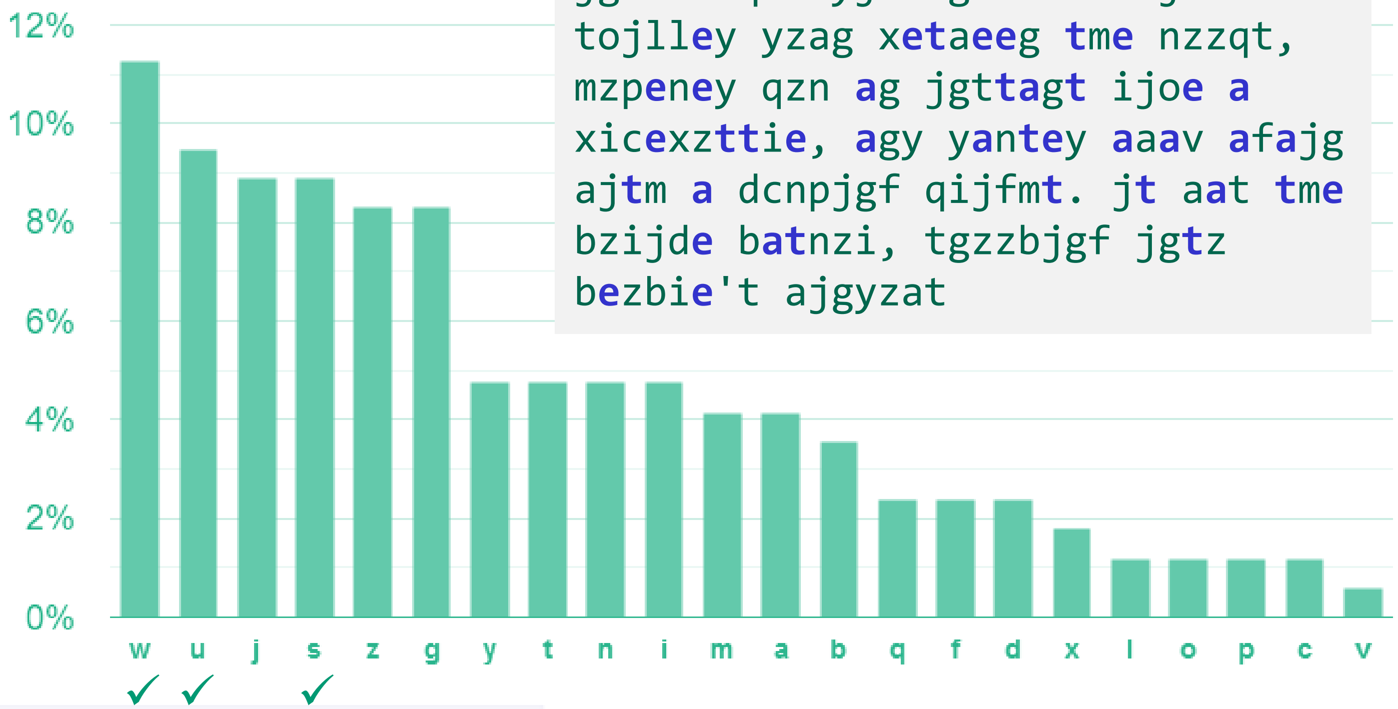


jg tme qsn yjttsgde s meijdzbten
tojlley yzag xetaeeg tme nzzqt,
mzpeney qzn sg jgttsgt ijoe s
xicexzttie, sgy ysntey sasv sfsjg
ajtm s dcnpjgf qijfmt. jt ast tme
bzijde bstnzi, tgzzbjgf jgtz
bezbie't ajgyzat

Attacking the substitution cipher

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



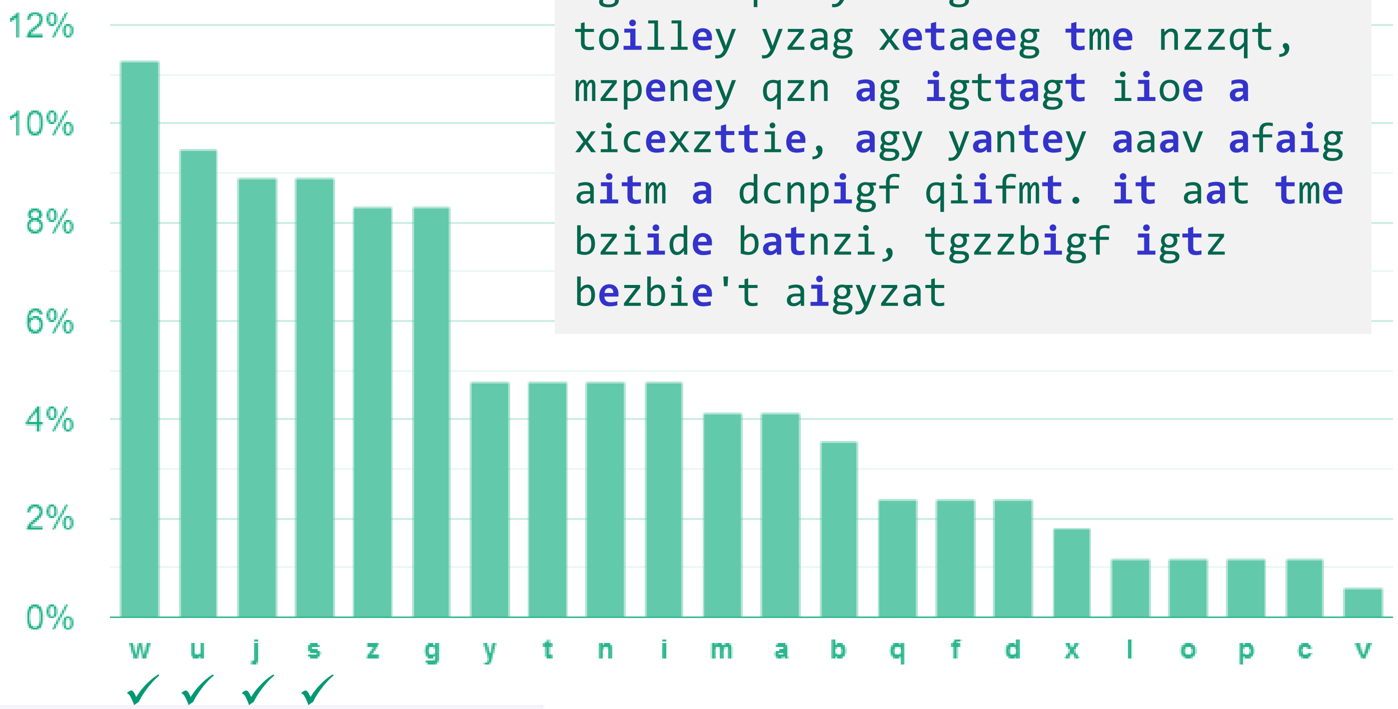


jg tme qan yjttagde a meijdzbten
tojlley yzag xetaeeg tme nzzqt,
mzpeney qzn ag jgttagt ijoe a
xicexzttie, agy yantey aaav afajg
ajtm a dcnpjgf qijfmt. jt aat tme
bzijde batnzi, tgzzbjgf jgtz
bezbie't ajgyzat

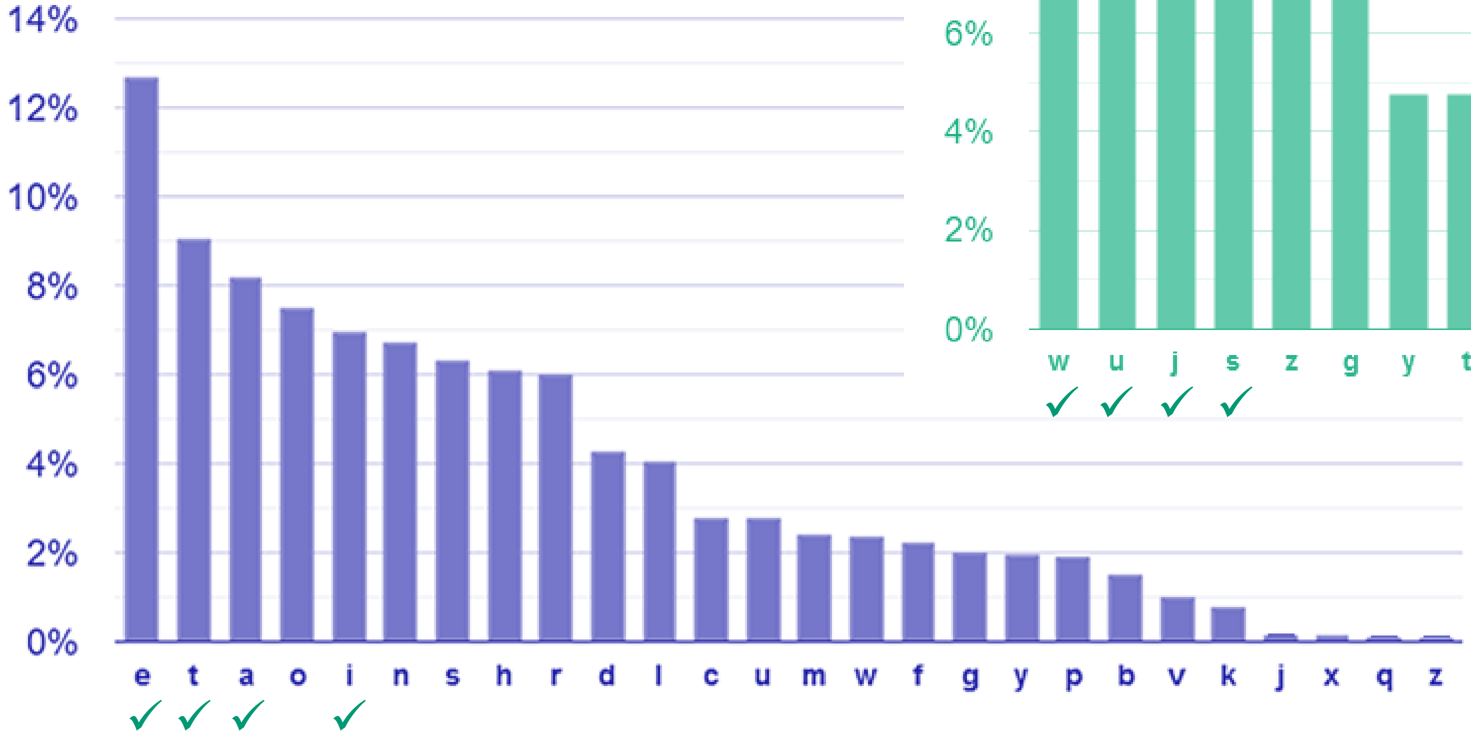
Attacking the substitution cipher

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

```
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
```

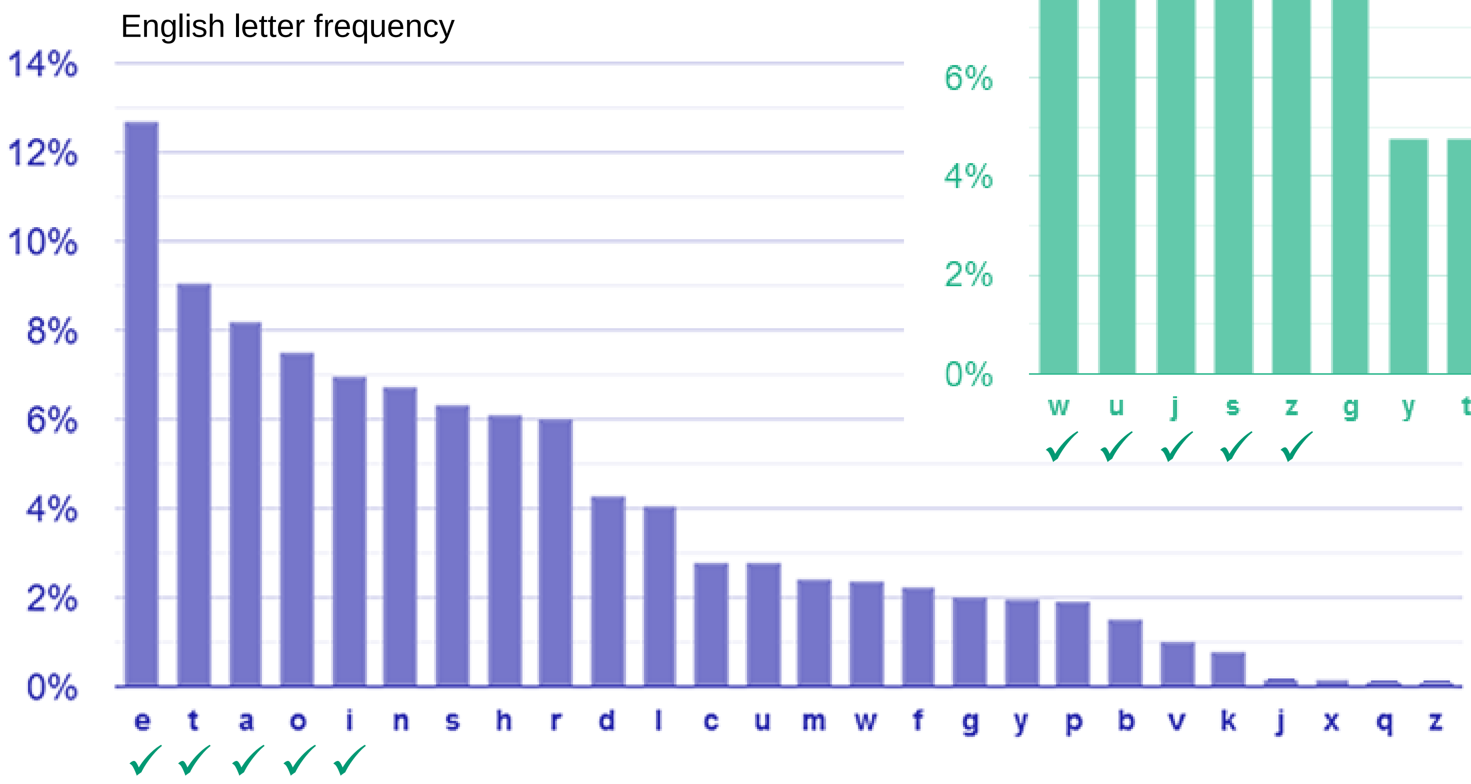


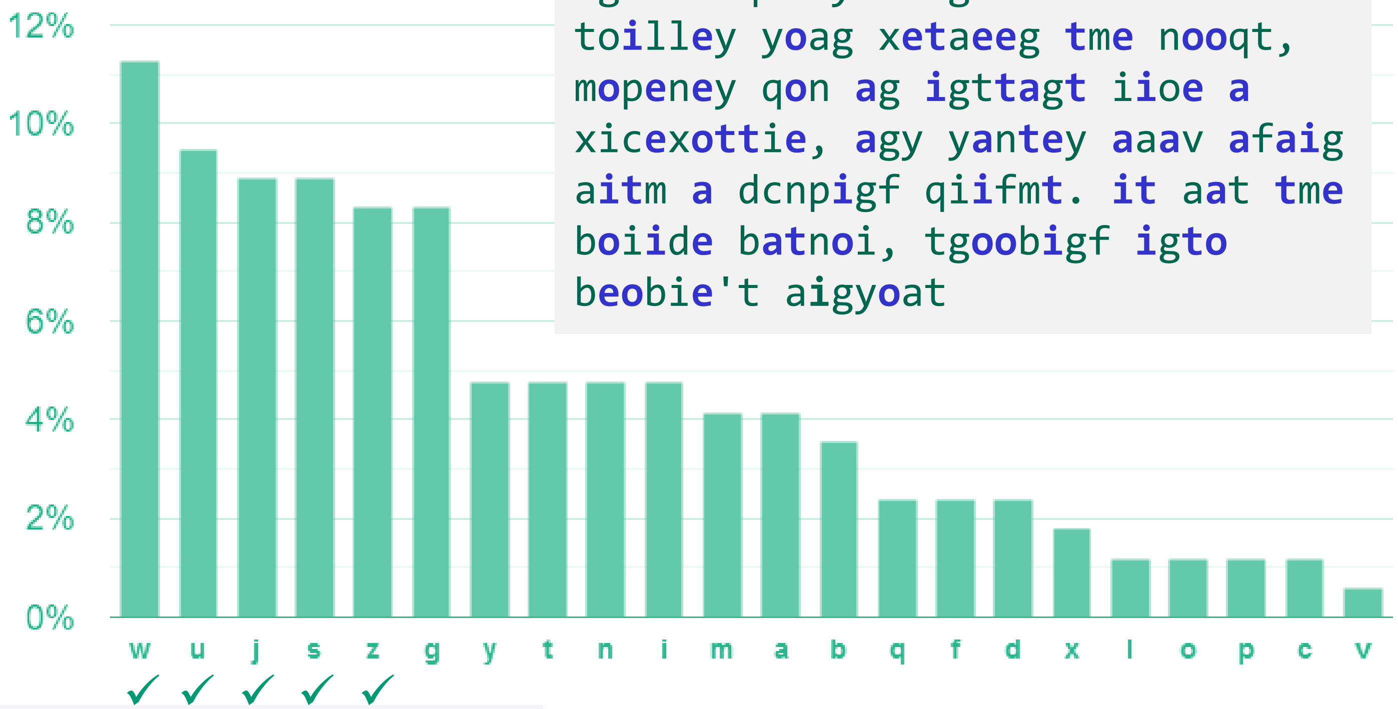
English letter frequency



Attacking the substitution cipher

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



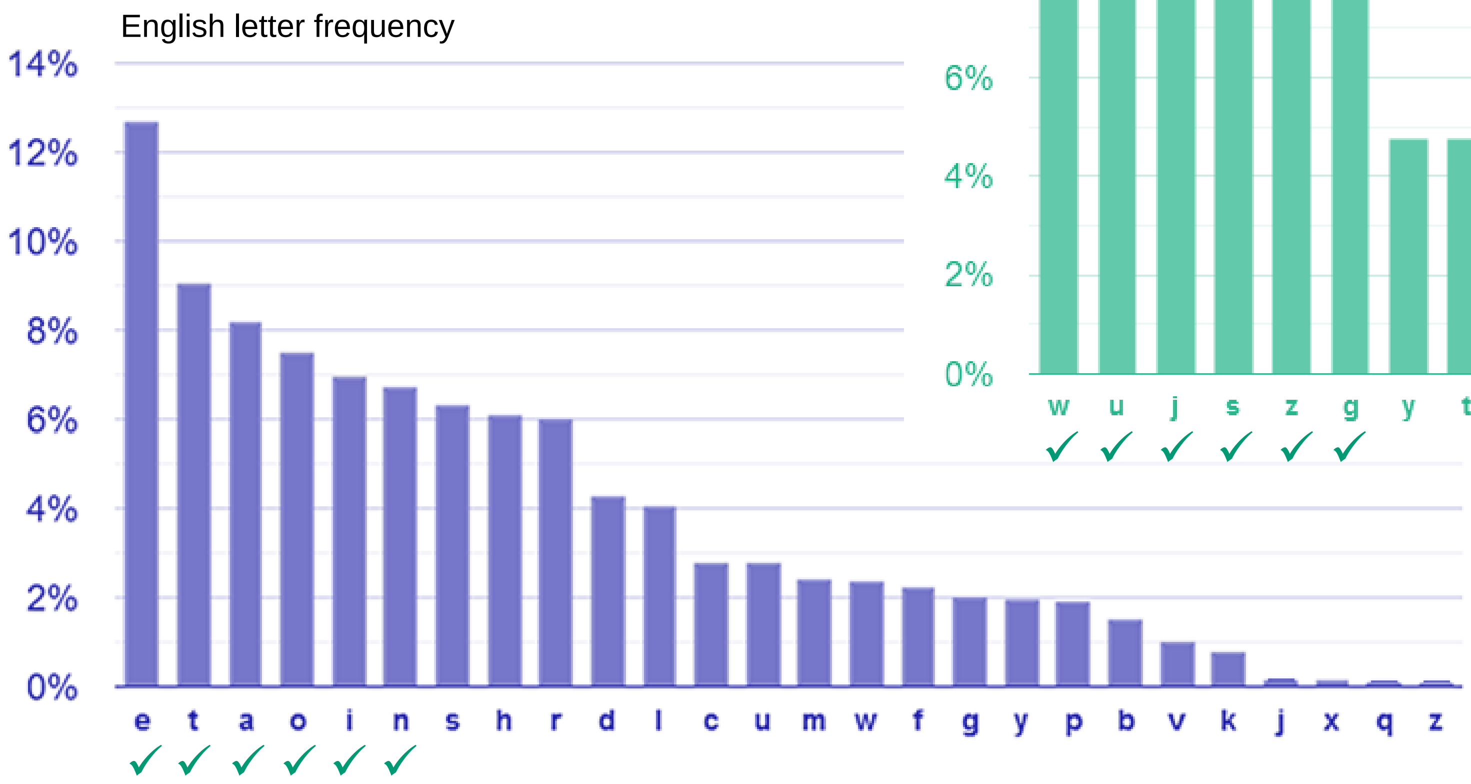


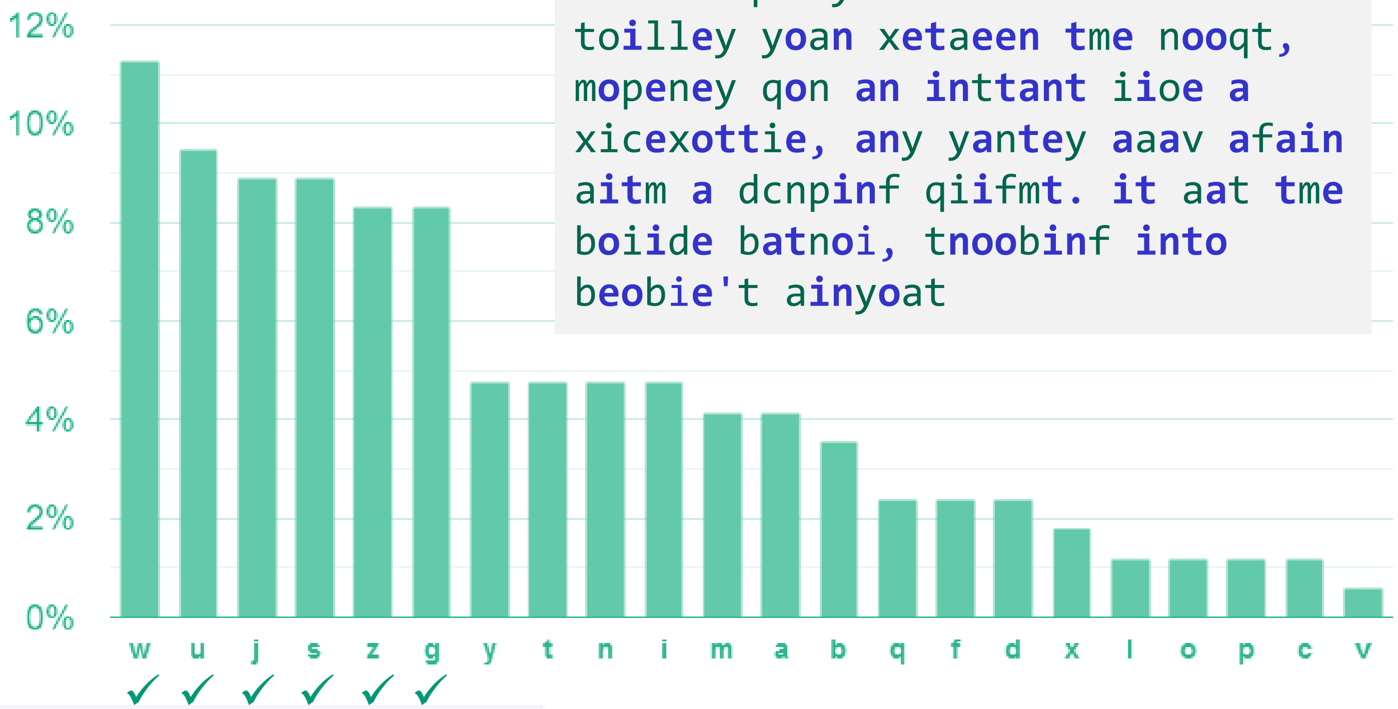

```
ig tme qan yittagde a meiidobten
toilley yoag xetaeeg tme nooqt,
mopeney qon ag igttagt iioe a
xicexottie, agy yantey aaav afaig
aitm a dcnpigf qiifmt. it aat tme
boiide batnoi, tgoobigf igto
beobie't aigyoat
```

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
```

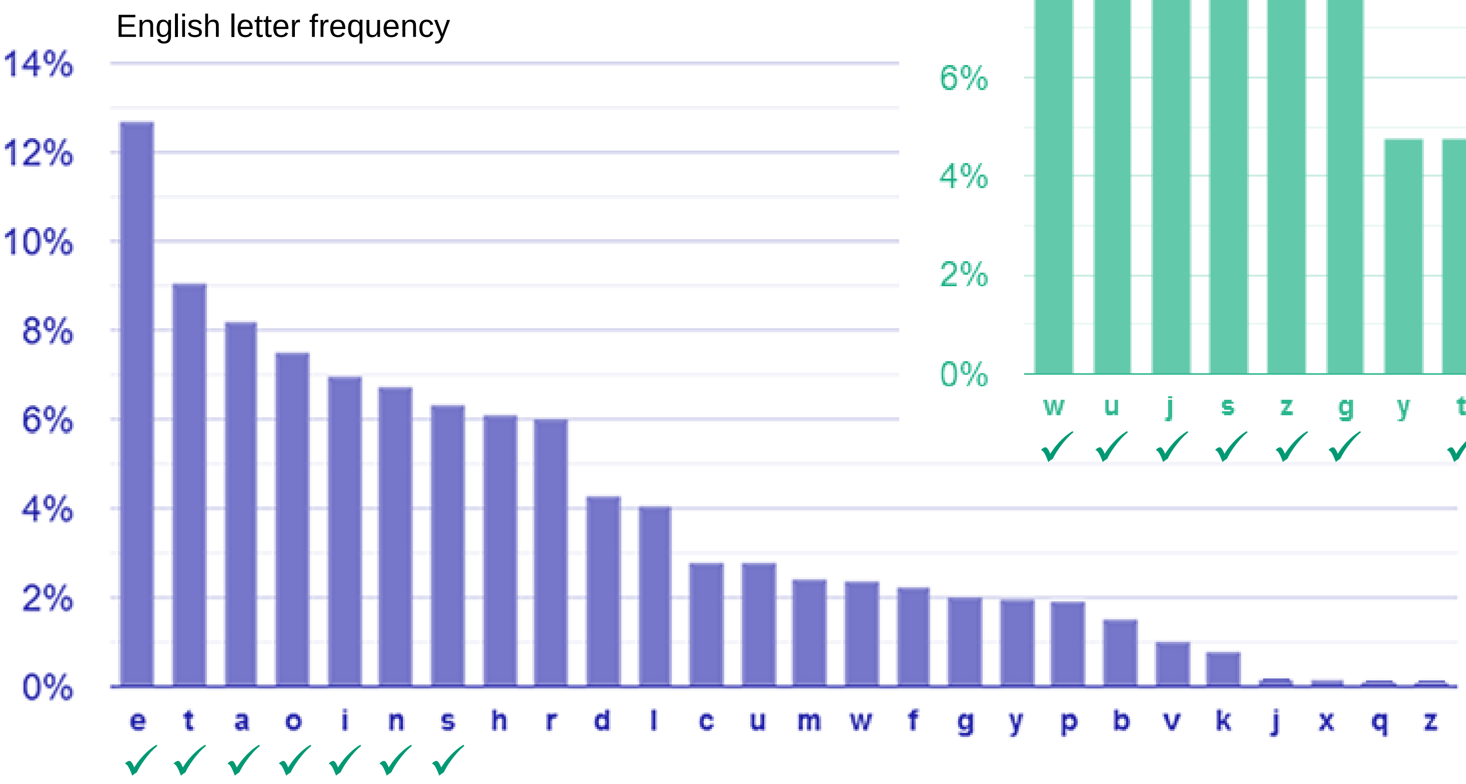


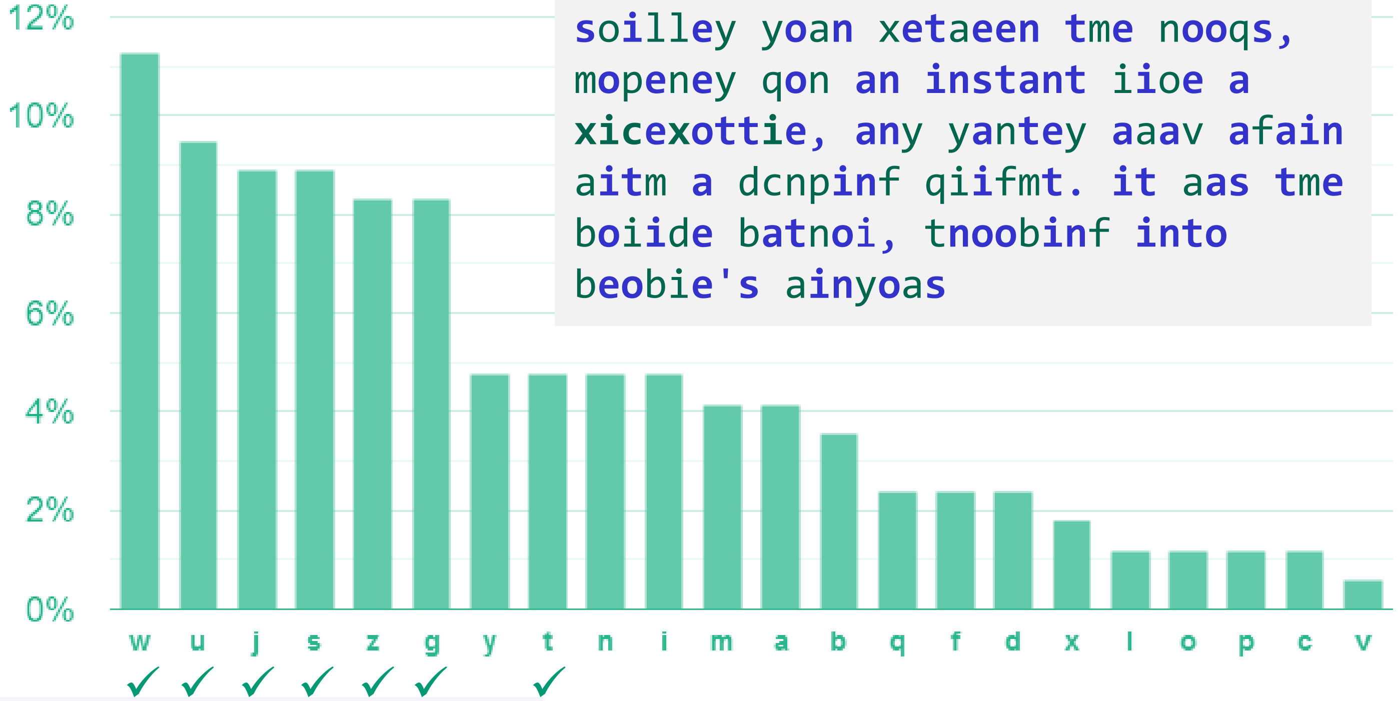


Attacking the substitution cipher

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

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



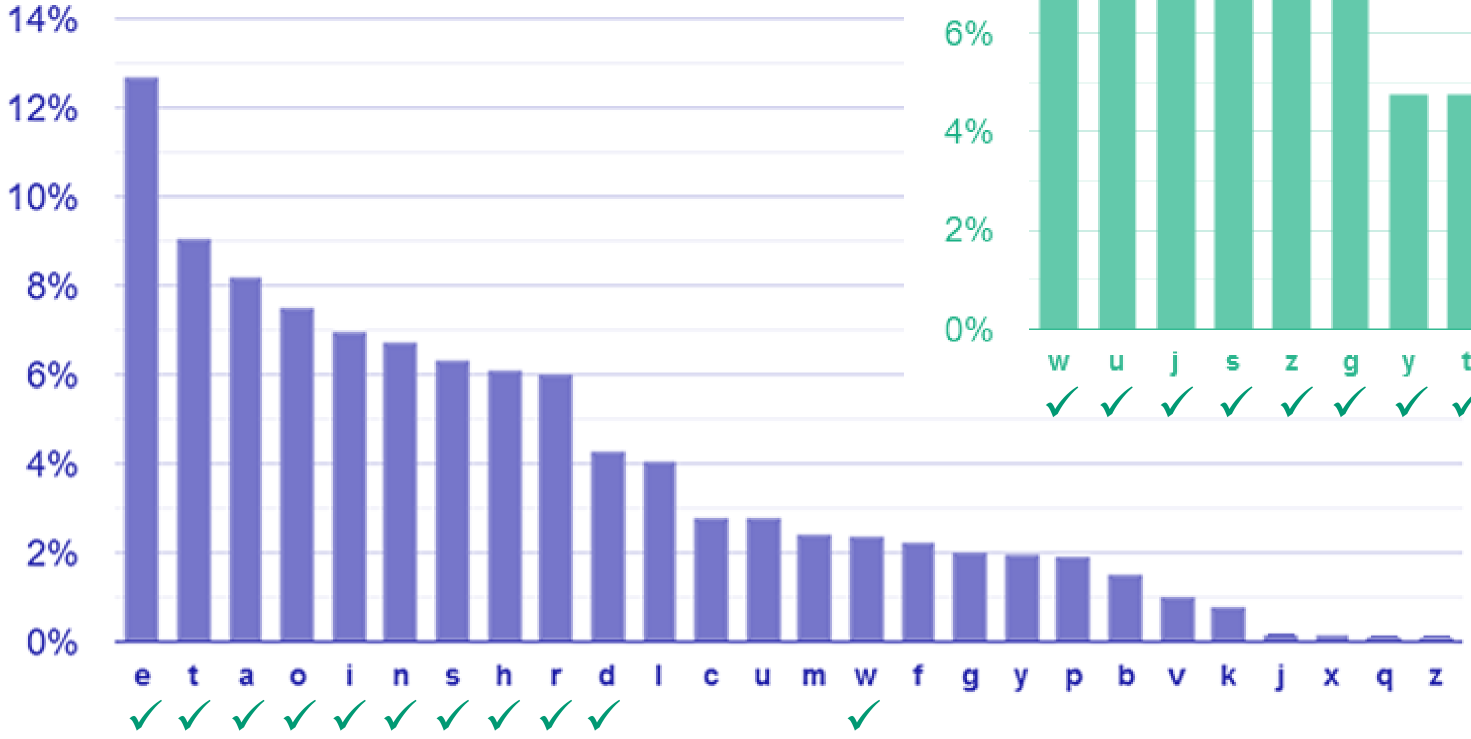


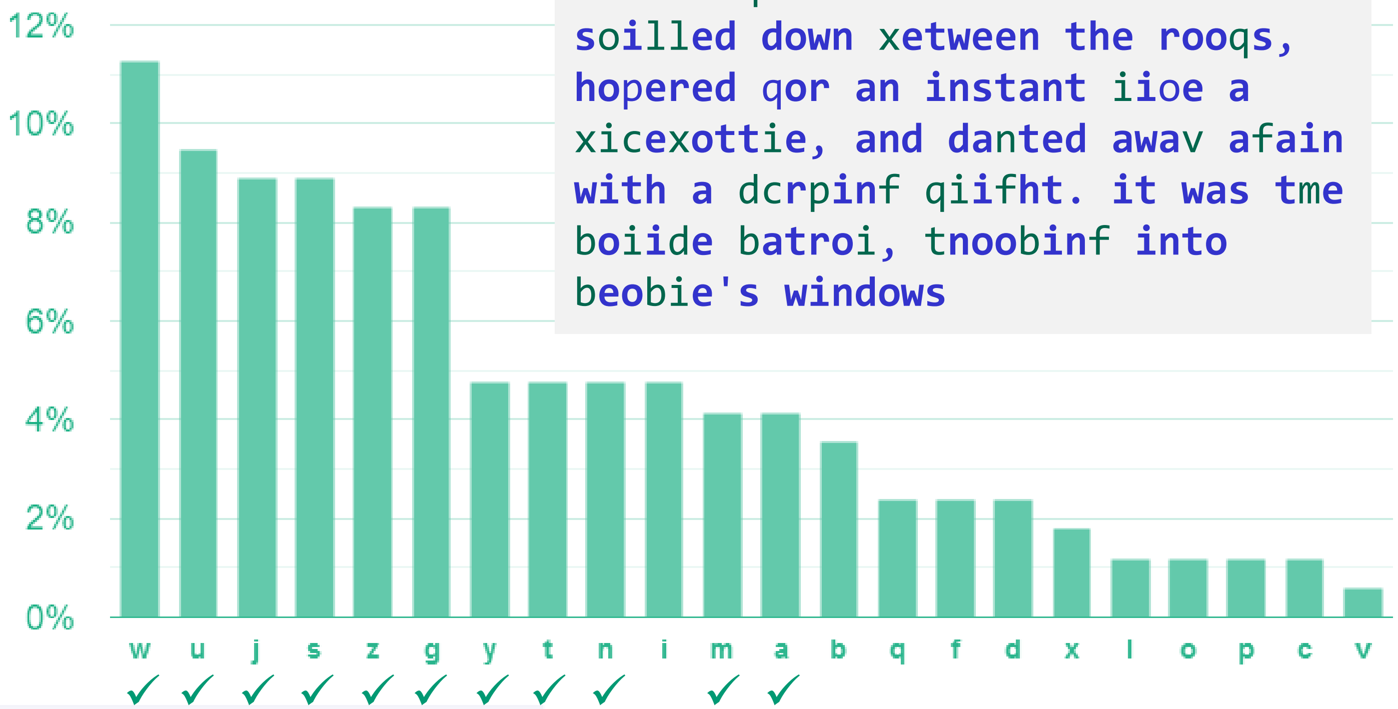
Attacking the substitution cipher

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

```
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
```

English letter frequency

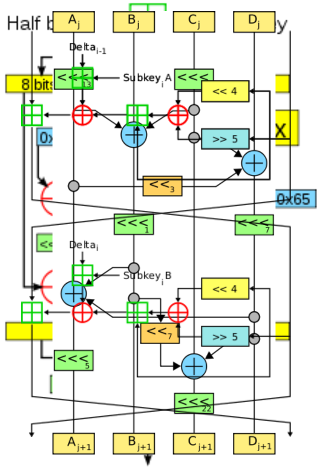


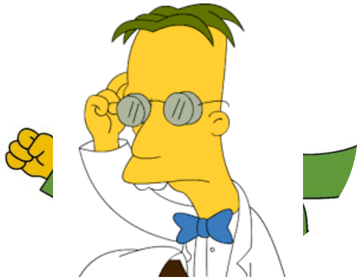


Conclusions

- 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)

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

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

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

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

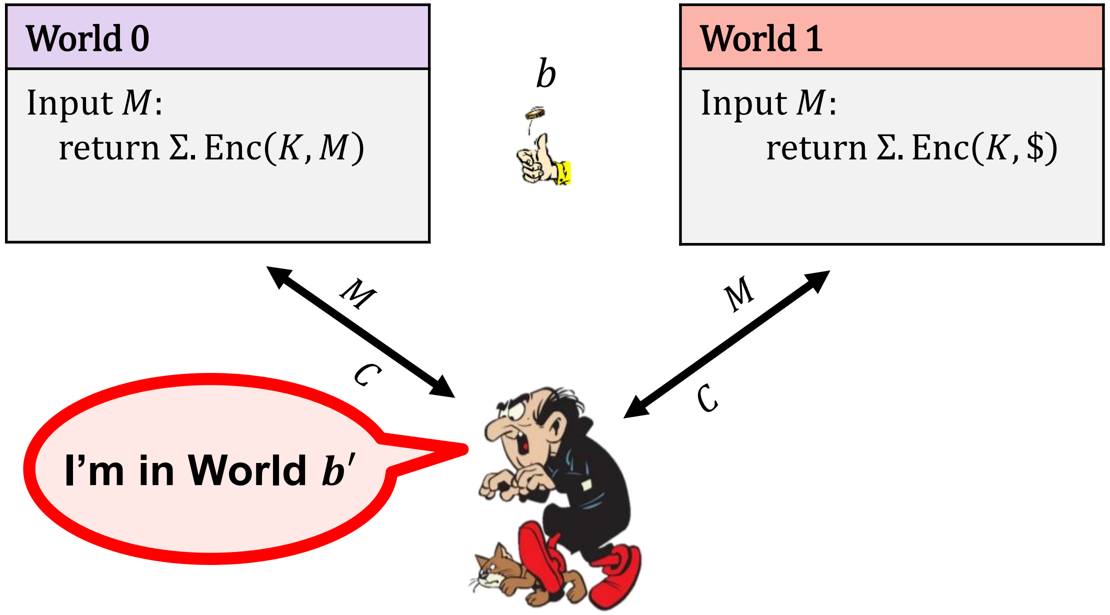
$$\begin{array}{lll} & 0101100100 & M \\ \oplus & 1110001101 & K \\ \hline = & 1011101001 & C \end{array} \qquad \begin{array}{lll} & 1011101001 & C \\ \oplus & 1110001101 & K \\ \hline = & 0101100100 & M \end{array}$$

Is the one-time pad secure?

(One-time) perfect privacy

$\mathbf{Exp}_{\Sigma}^{\text{1-priv}}(A)$

```
b ←$ {0,1}
K ←$ Σ.KeyGen
M ← A
R ←$ {0,1}^|M|
C_0 ← Σ.Enc(K, M)
C_1 ← Σ.Enc(K, R)
b' ← A(C_b)
return b' =? b
```



Definition: An encryption scheme Σ has **(one-time) perfect privacy** if for any adversary A:

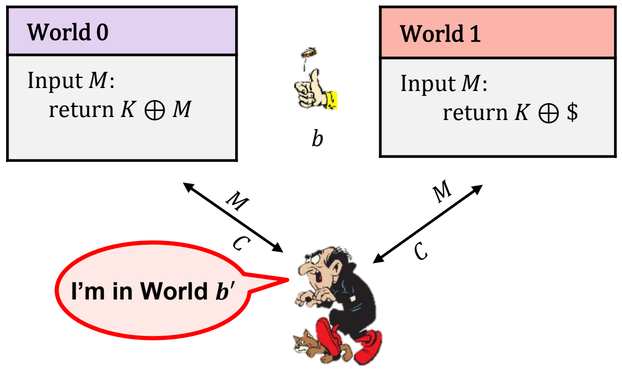
$$\Pr[b' = b] = \frac{1}{2}$$

The one-time-pad (OTP) – security

Theorem (Shannon 1949): The one-time pad encryption scheme has **one-time perfect privacy**

Proof: Need to show: $\Pr[b' = b] = 1/2$

Prob	K	M



Suppose A submits $M = 110$ and receives $C = 101$

$\Pr[\, C = 101 \mid b = 0\,] = \Pr[K = 011] = 1/8$

$\Pr[\, C = 101 \mid b = 1\,] = 1/8$

$\Pr[C = 101] = 1/8$

Probability that A sees $C = 101$ is *independent* of which world it's in! $\implies$ C contains no information about b

$\implies$ $\Pr[b' = b] = 1/2$

One-time pad – perfect?

- One-time pad has perfect privacy…for *one* message
  - What happens if you use 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
  - Key management becomes very difficult
  - Sort of defeats the purpose
  - What happens if it is shorter?

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

- **One-time perfect privacy:**

$$\Pr[b' = b] = \frac{1}{2}$$

- 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

Modern cryptography – idea

- computational ~~One-time perfect~~ **privacy:**

$$\Pr[b' = b] = \frac{1}{2} \pm \varepsilon$$

- Security holds for *resource bounded* *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 ✓

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

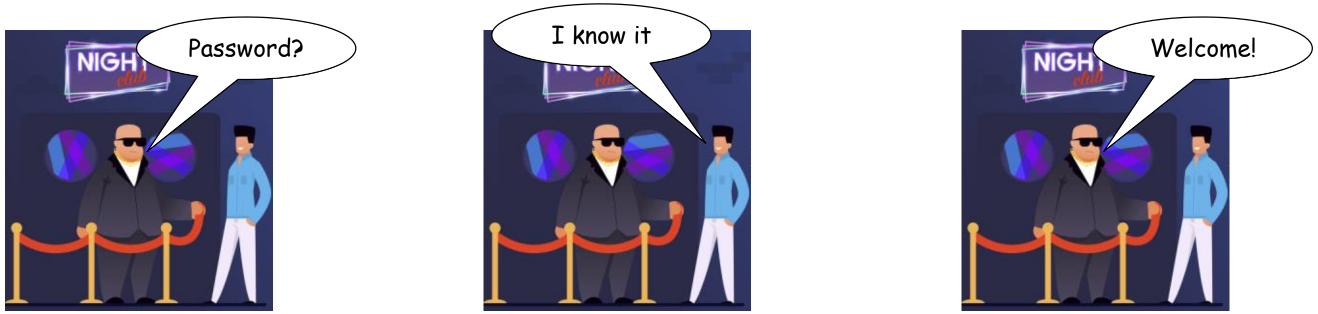
	Message privacy	Message integrity / authentication	
Symmetric keys	Symmetric encryption	Message authentication codes (MAC)	Part I
Asymmetric keys	Asymmetric encryption (a.k.a. public-key encryption)	Digital signatures	

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 II

Much more to cryptography

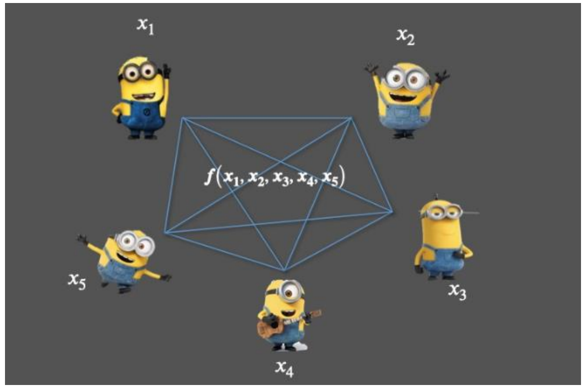
- Zero-knowledge proofs



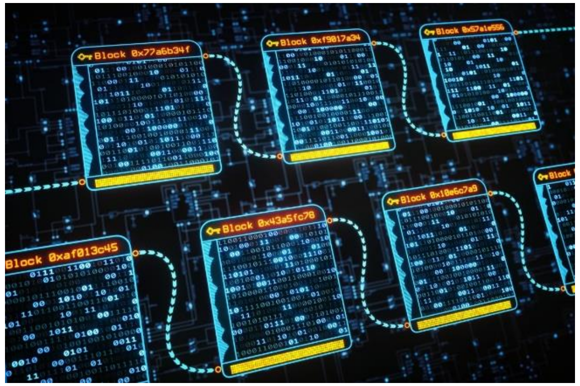
- Fully-homomorphic encryption

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

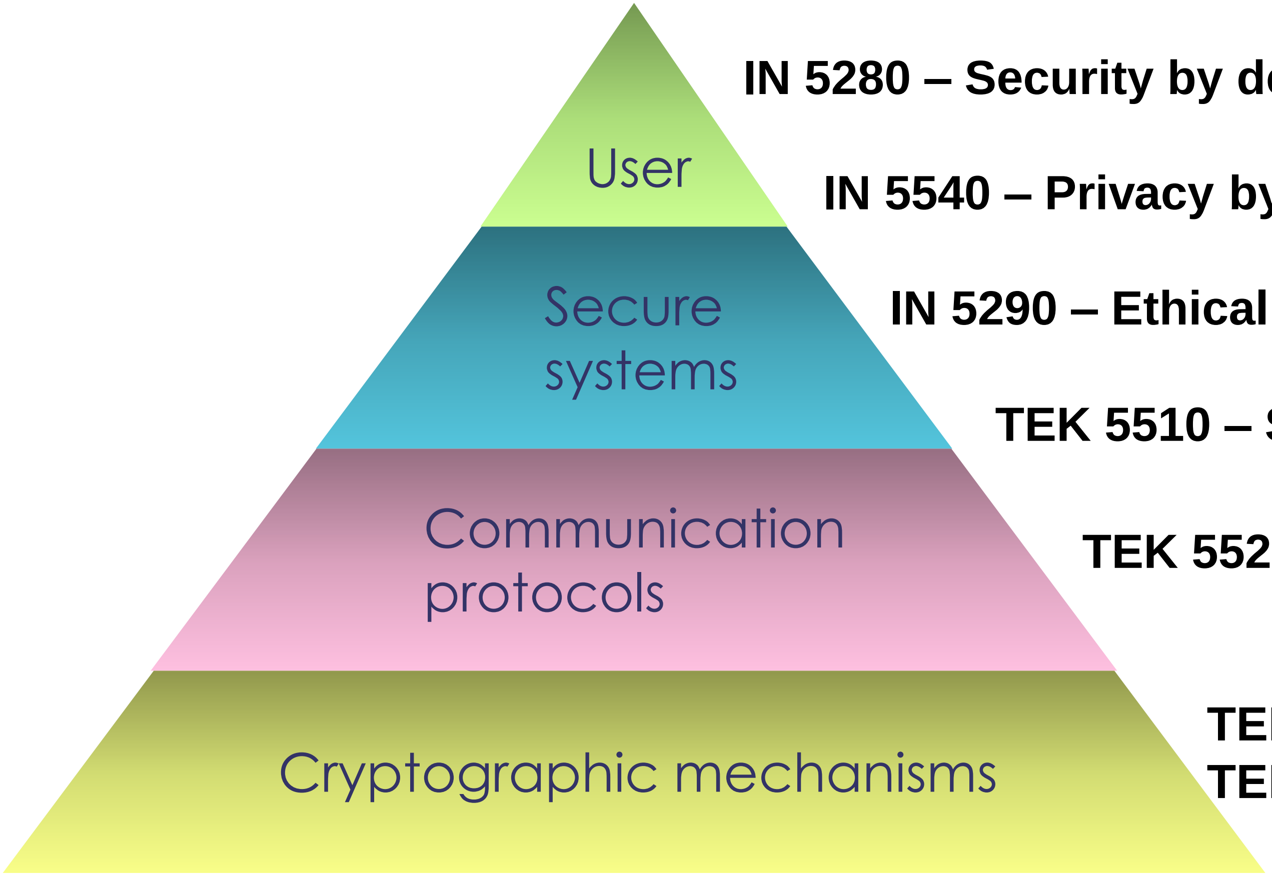
- Multi-party computation



- Blockchain



The security pyramid



IN 5280 – Security by design

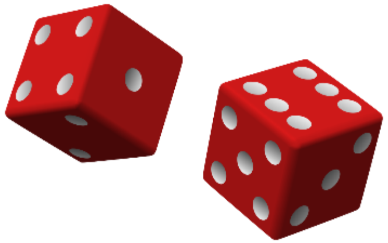
IN 5540 – Privacy by design

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 details: https://en.wikibooks.org/wiki/High_School_Mathematics_Extensions/Discrete_Probability

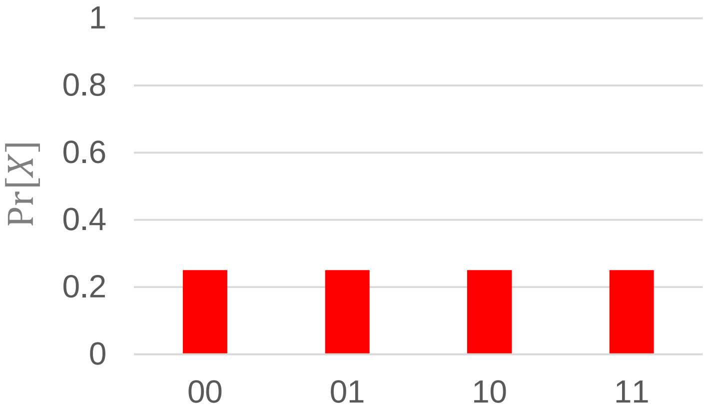
Discrete probability

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

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

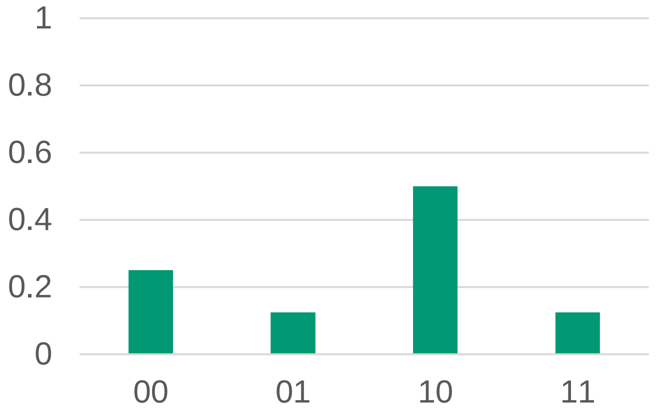
$$\sum_{X \in \mathcal{U}} \Pr[X] = 1$$

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

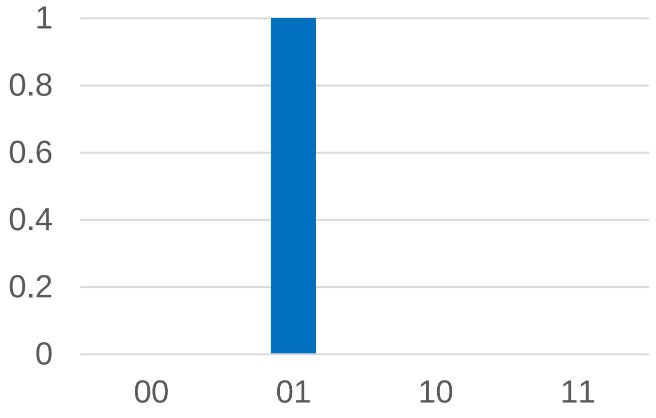


$\Pr[00] = 1/4$
$\Pr[01] = 1/4$
$\Pr[10] = 1/4$
$\Pr[11] = 1/4$

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 $A \subseteq \mathcal{U}$ is called an **event** and $\Pr[A] = \sum_{x \in A} \Pr[x]$

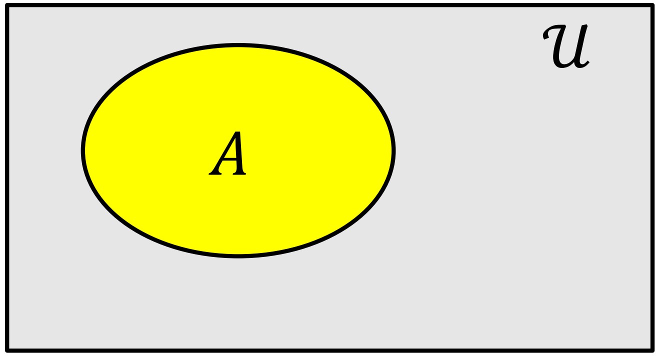
- The **complement** of A is $\mathcal{U} \setminus A$ and denoted $\bar{A}$
  - Fact: $\Pr[\bar{A}] = 1 - \Pr[A]$

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

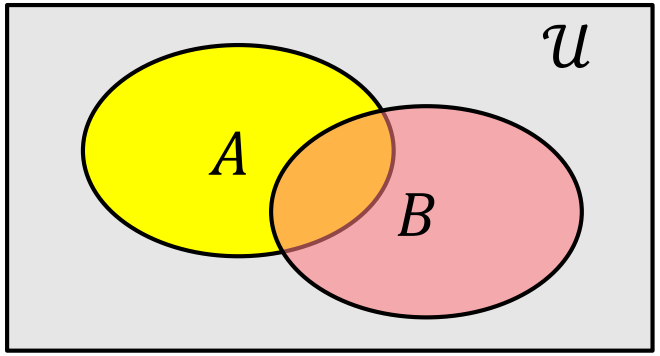
$$A = \{x \in \mathcal{U} \ \mid x = 11\text{xx xxxx}\} \subset \mathcal{U}$$

With the uniform distribution over $\mathcal{U}$, 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 $\mathcal{U}$:

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

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

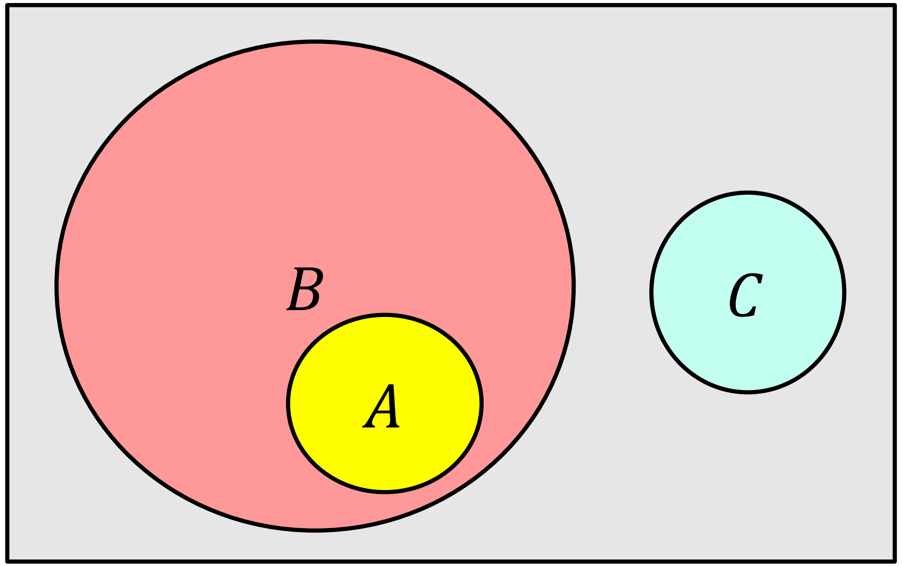
Law of total probability

- **Conditional probability**

$$\Pr[\,X \mid Y\,] \stackrel{\text{def}}{=} \frac{\Pr[X \text{ and } Y]}{\Pr[Y]}$$

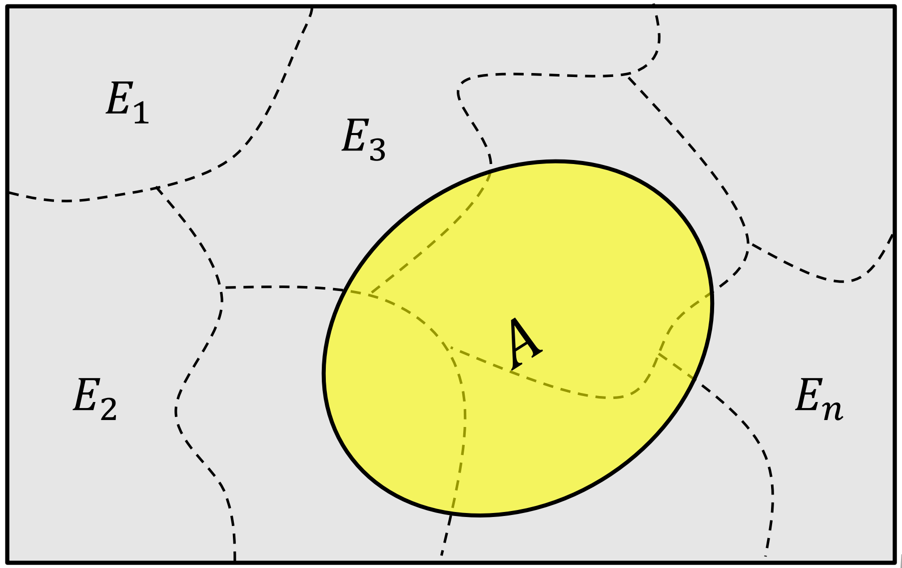
$$\Pr[A \mid B] > \Pr[A]$$

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



- **Law of total probability**

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



Random variables

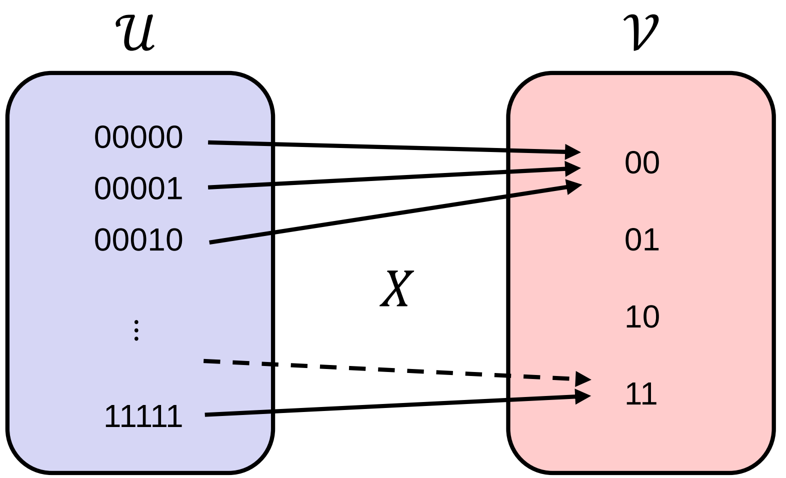
A **random variable** X is a function $X : \mathcal{U} \to \mathcal{V}$

Example:

$$\overset{\mathcal{U}}{}\qquad\overset{\mathcal{V}}{}$$

$$X : \{0,1\}^5 \to \{0,1\}^2$$

$$X(s) \stackrel{\text{def}}{=} \text{msb}_2(s)$$



$$\Pr[X = 11] \stackrel{\text{def}}{=} \Pr_{s \in \mathcal{U}}[s = 11\text{xxx}] = \frac{2^3}{2^5} = 1/4$$

Depends on the probability distribution on $\mathcal{U}$

Uniform distribution on $\mathcal{U}$

Random variables

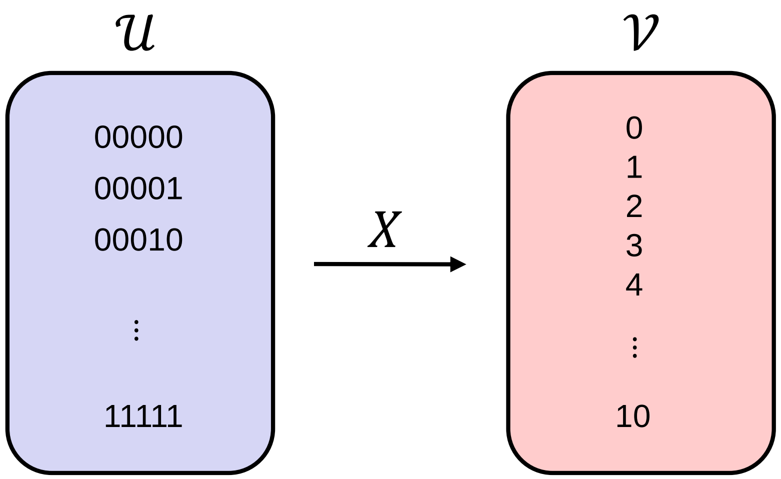
A **random variable** X is a function $X : \mathcal{U} \rightarrow \mathcal{V}$

Example:

$$\overset{\color{blue}{\mathcal{U}}}{} \qquad \overset{\color{red}{\mathcal{V}}}{}$$

$$X : \{0,1\}^5 \rightarrow [0,1,2,\dots,10]$$

$$X(s) \overset{\text{def}}{=} s_1 + s_2 + s_3 + s_4 + s_5$$



$\Pr[X = 0] = 1/32$

$\Pr[X = 1] = 5/32$

$\Pr[X = 2] = \binom{5}{2} / 32 = 10/32$

$\Pr[X = 10] = 0$

Uniform distribution on $\mathcal{U}$

but not on $\mathcal{V}$!

Random variables

A **random variable** X is a function $X : \mathcal{U} \to \mathcal{V}$

Example:

$$\overset{\color{blue}{\mathcal{U}}}{} \qquad \overset{\color{red}{\mathcal{V}}}{}$$

$$X : \{0,1\}^5 \to [0,1,2,\ldots,10]$$

$$X(s) \overset{\text{def}}{=} s_1 + s_2 + s_3 + s_4 + s_5$$

$$U : \{0,1\}^5 \to [0,1,2,\ldots,10]$$

$\Pr[X = 0] = 1/32$

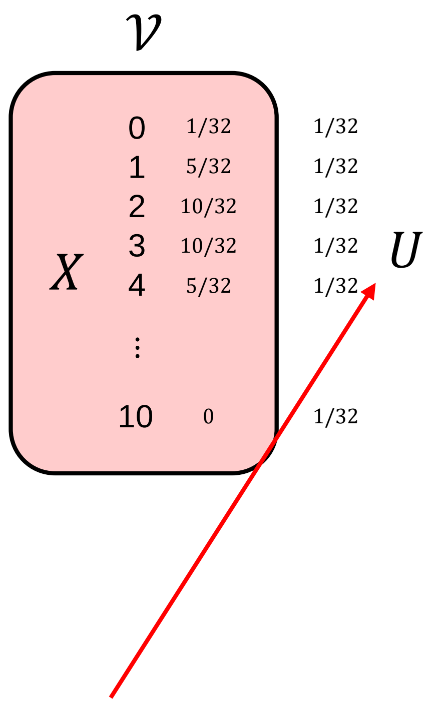
$\Pr[X = 1] = 5/32$

$\Pr[X = 2] = \binom{5}{2} / 32 = 10/32$

$\Pr[X = 10] = 0$

Uniform distribution on $\mathcal{U}$

but not on $\mathcal{V}$!



Uniform distribution on $\mathcal{V}$

i.e. U is a **uniform random variable** (on $\mathcal{V}$)

Randomized algorithms

- Deterministic algorithm:

  $$y \leftarrow A(x)$$

- Randomized algorithm:

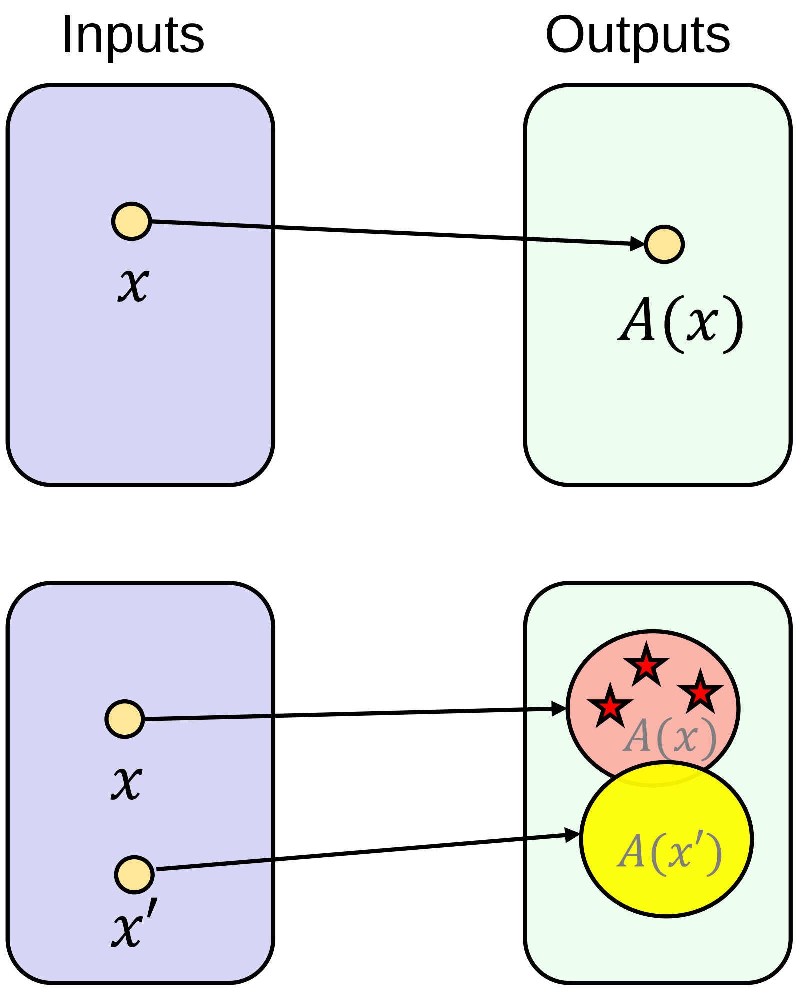
  $$y \leftarrow A(x; r) \qquad \text{where } r \overset{\$}{\leftarrow} \{0,1\}^n$$

  $$y \overset{\$}{\leftarrow} A(x)$$

  $A(x)$ is a random variable!

- **Example:**

  $$A(X; K) = \mathrm{Enc}(K, X) \qquad\qquad Y \overset{\$}{\leftarrow} A(X)$$



Next week

- Block ciphers

- Pseudorandom functions and pseuorandom permutations

- AES

- **NOTE:** different room!