
Lecture 1 – Introduction to cryptography

TEK4500

28.08.2024

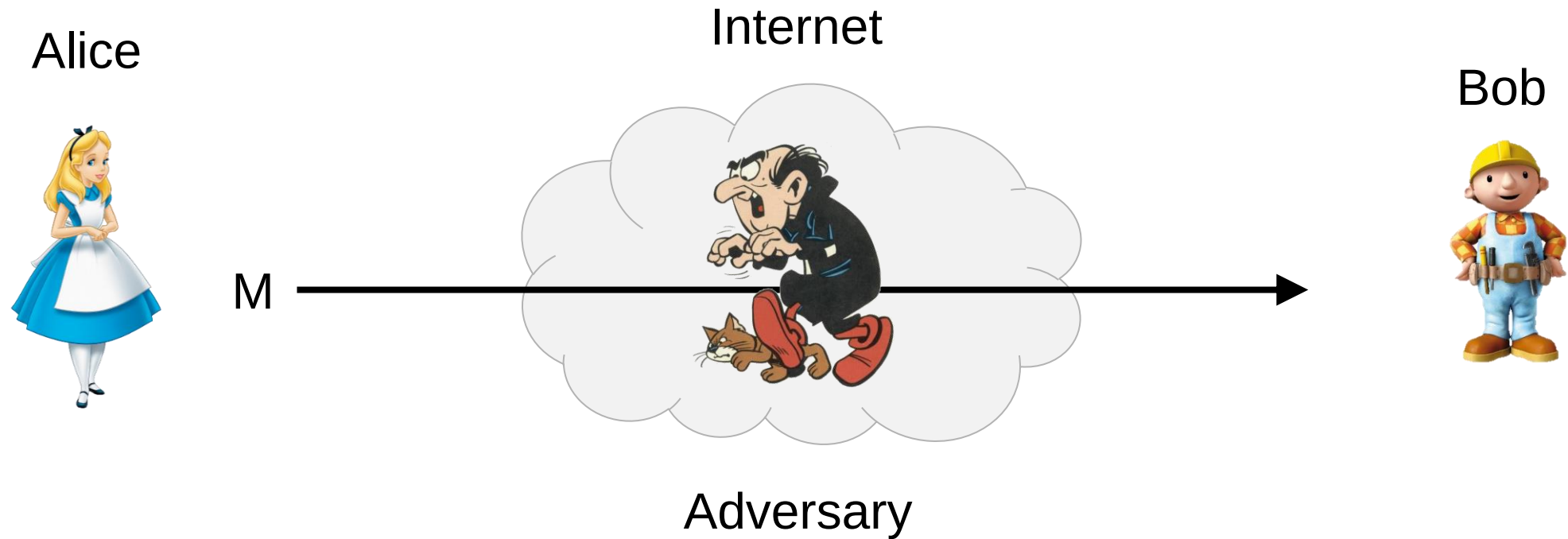
Håkon Jacobsen

hakon.jacobsen@its.uio.no

Today's agenda

- What is cryptography?
- Some historical ciphers
- Recap: modular arithmetic
- Secure encryption: searching for a definition
- Recap: probability theory

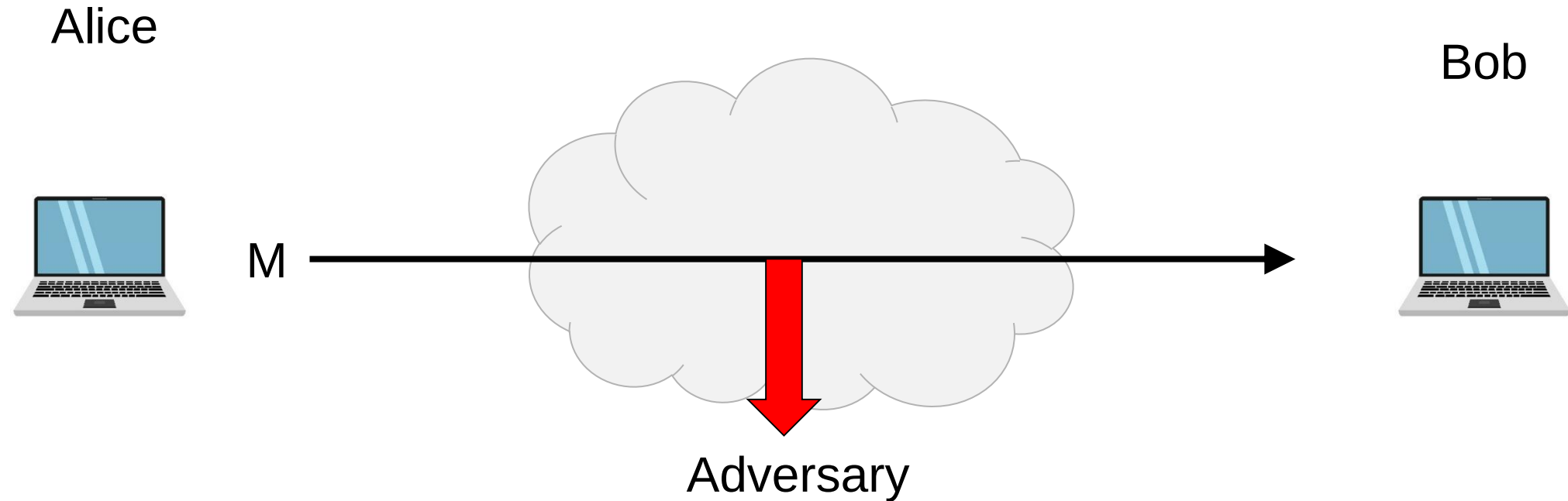
What is cryptography?



What is cryptography?



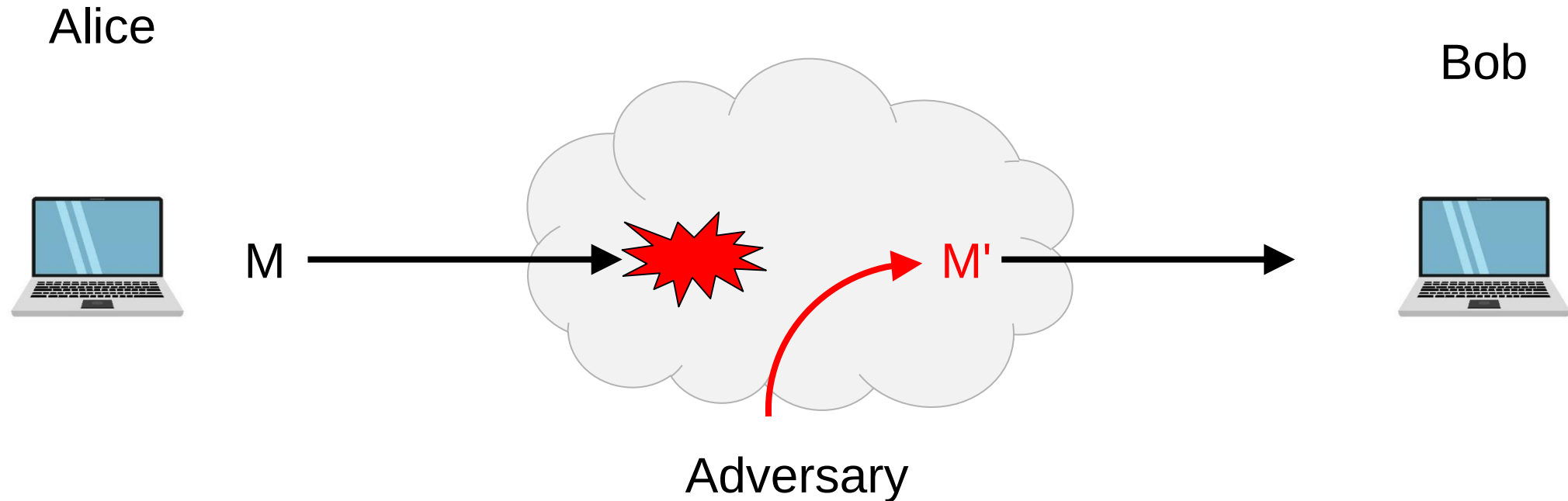
What is cryptography?



Security goals:

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

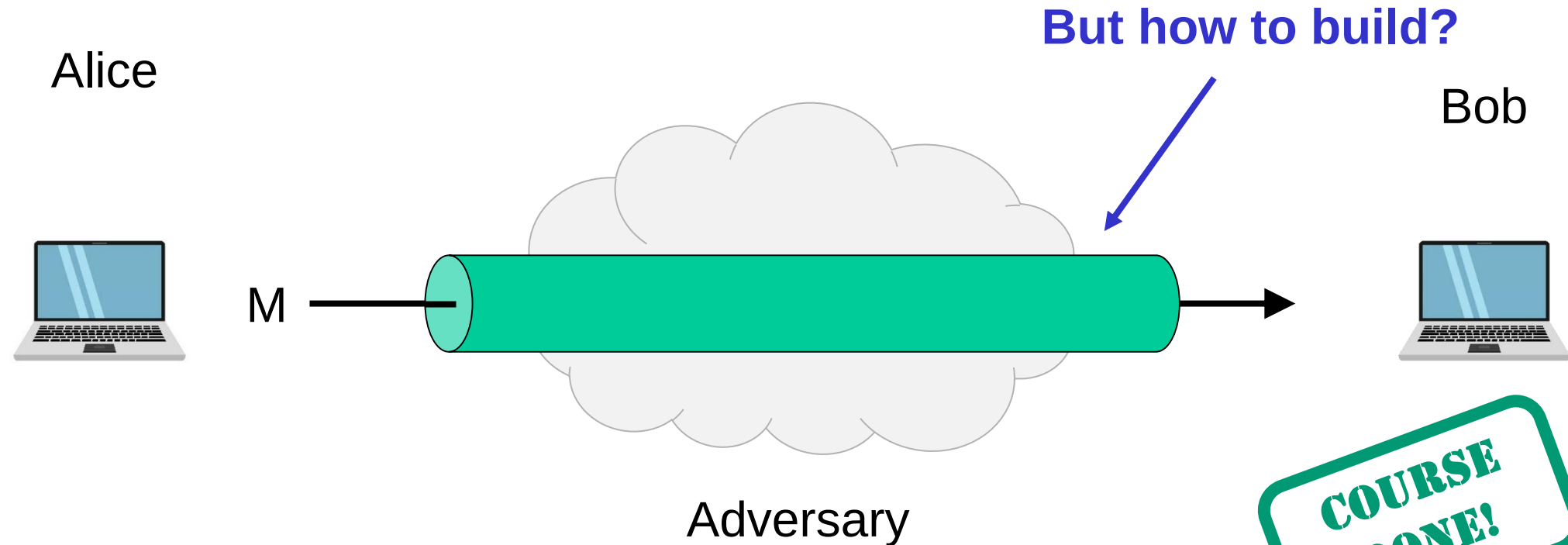
What is cryptography?



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

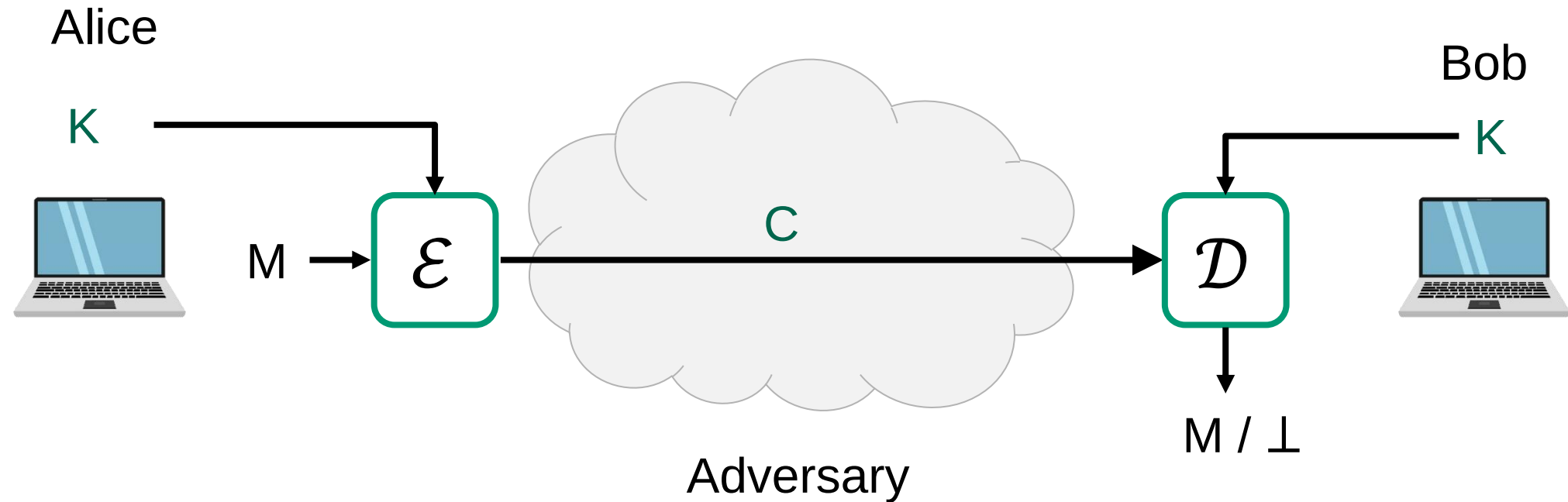


Security goals:

- **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 ✓

**COURSE
DONE!**

Creating secure channels: encryption schemes

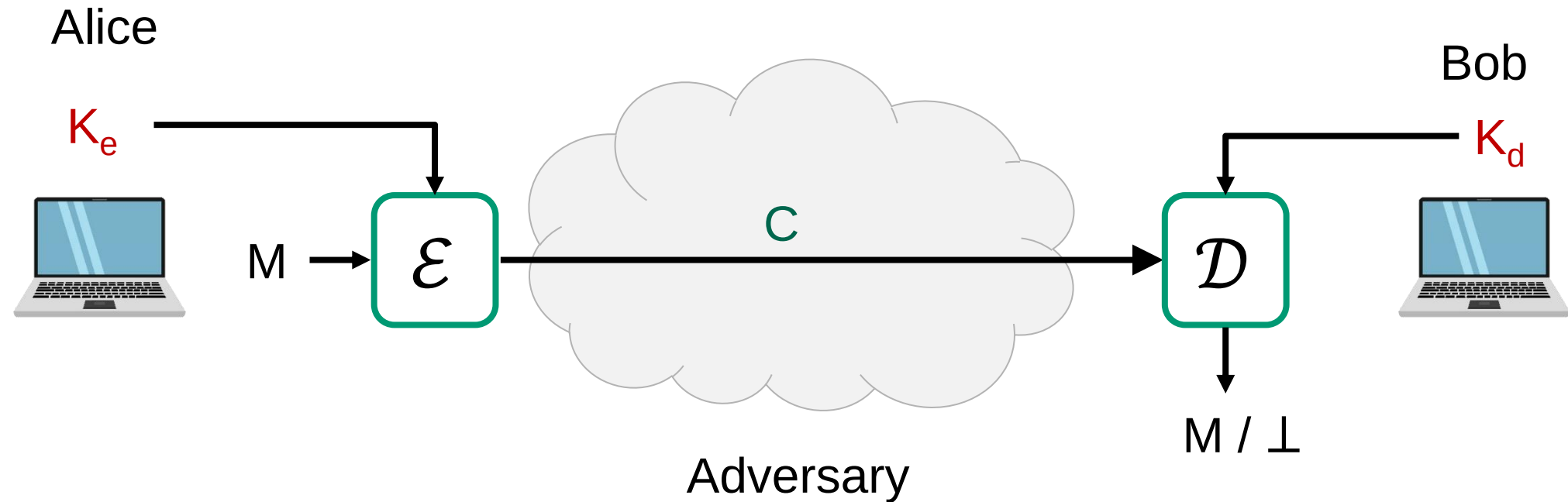


$\mathcal{E}$: encryption algorithm (public)

K : encryption / decryption key (secret)

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

Creating secure channels: encryption schemes



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

K_e : encryption key (public)

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

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"
 - $3 \in \{1,2,3,4,5\}$
 - $7 \notin \{1,2,3,4,5\}$
- $\forall$ – "for all"
 - " $\forall x \in \{1,2,3\} : x^2 > 0$ "
- $\exists$ – "there exists"
 - " $\exists X \in \{0,1,2, \dots\}$ such that $X > 13$ "
- $\{0,1\}^n$ – 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")
 - $1^5 = 11111$
 - $0^3 = 000$
- $F : \mathcal{X} \rightarrow \mathcal{Y}$ – function from set $\mathcal{X}$ to set $\mathcal{Y}$
 - $F : \{0,1\}^5 \rightarrow \{0,1\}^3$
 - $G : \{A,B,C,D\} \rightarrow \{0,1,2, \dots\}$
- $\mathcal{X} \times \mathcal{Y}$ – set of pairs (X, Y) with $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$
 - $F : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ function taking two inputs $X \in \mathcal{X}$, $Y \in \mathcal{Y}$ and producing $Z \in \mathcal{Z}$...**...independent, and uniformly distributed...**
- $X \leftarrow 5$ – "assign value 5 to X "
- $X \overset{\$}{\leftarrow} \mathcal{X}$ – "assign X a *random* value from set $\mathcal{X}$ "

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:

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

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

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

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

Correctness requirement:

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

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

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
- ...

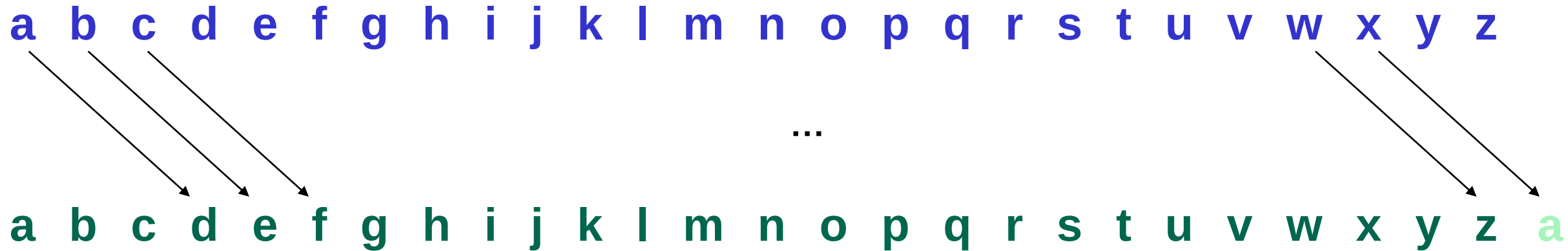


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

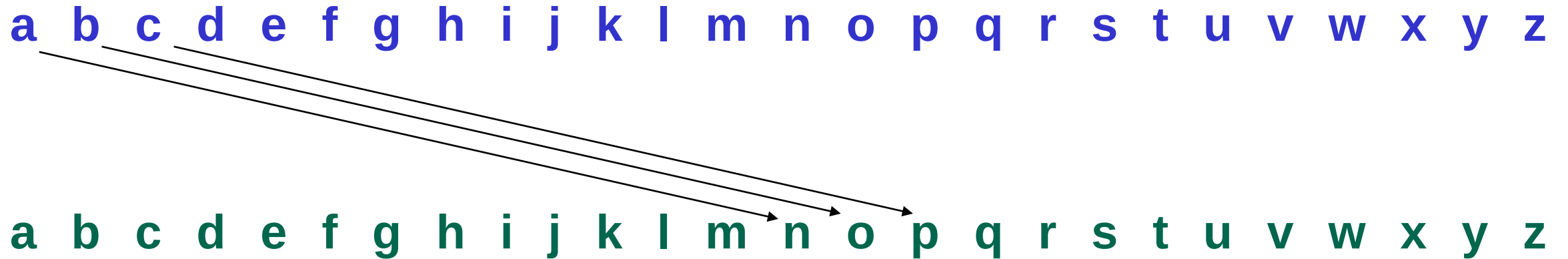
Ceasar cipher



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 zlw 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 orgjrre
gur ebbsf, ubirerq sbe na vafgnag yvxn n oyhrobggyr,
naq qnegrq njnl ntnva jvgu n pheivat syvtug. Vg jnf
gur cbyvpr cngeby, fabbcvat vagb crbcyr'f jvaqbjf

Ceasar cipher

$a \leftrightarrow 0$

$b \leftrightarrow 1$

$c \leftrightarrow 2$

$d \leftrightarrow 3$

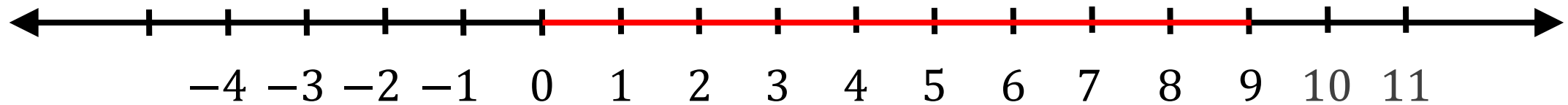
$e \leftrightarrow 4$

$\vdots$

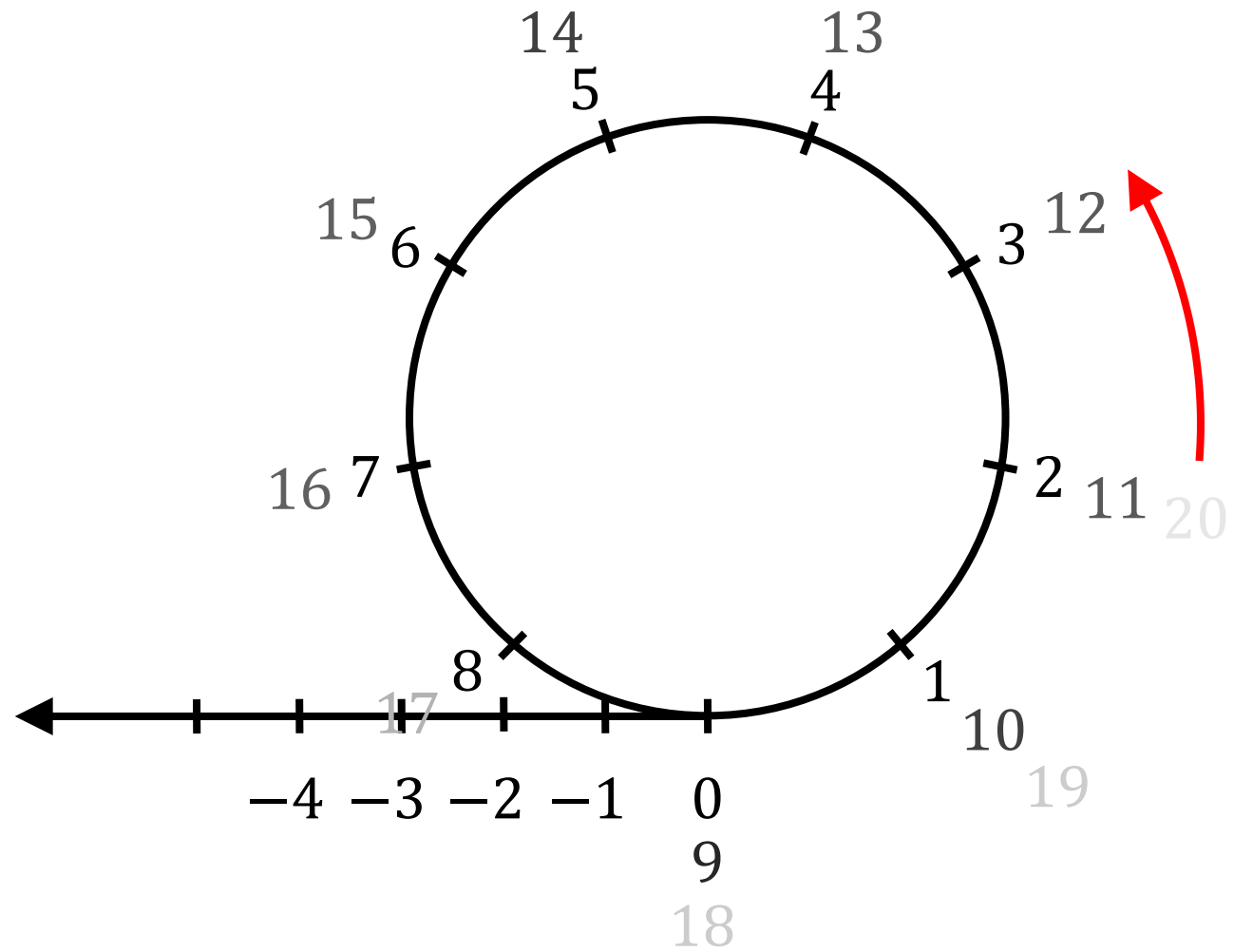
$z \leftrightarrow 25$

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

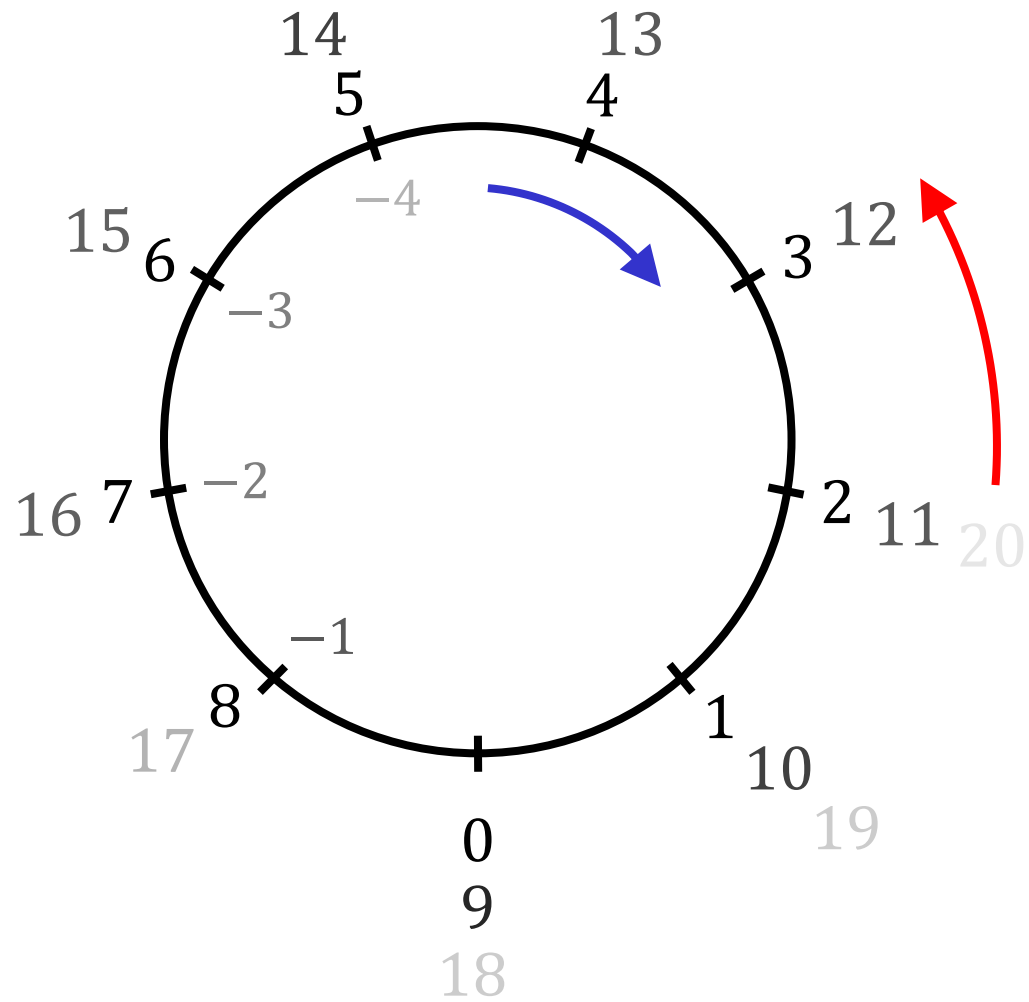
Modular arithmetic



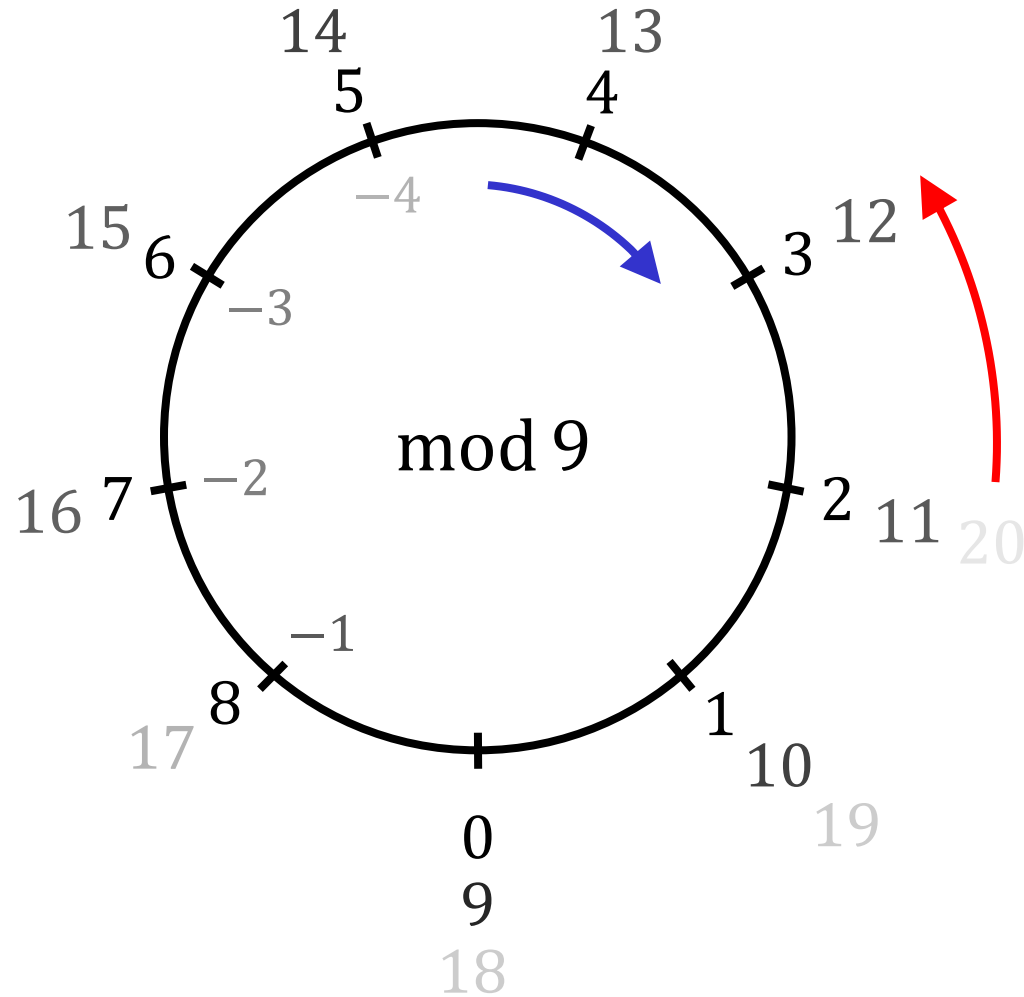
Modular arithmetic



Modular arithmetic



Modular arithmetic



$$1 + 3 = 4$$

$$5 + 8 = 13 \equiv 4 \pmod{9}$$

$$5 \cdot 4 = 20 \equiv 2 \pmod{9}$$

$$2 - 5 = -3 \equiv 6 \pmod{9}$$

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

$$158 \pmod{9} = 153 + r \equiv r \pmod{9}$$

$$r < 9$$

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

Ceasar cipher

a $\leftrightarrow$ 0

b $\leftrightarrow$ 1

c $\leftrightarrow$ 2

d $\leftrightarrow$ 3

e $\leftrightarrow$ 4

⋮

z $\leftrightarrow$ 25

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

ROT-13

a $\leftrightarrow$ 0

b $\leftrightarrow$ 1

c $\leftrightarrow$ 2

d $\leftrightarrow$ 3

e $\leftrightarrow$ 4

$\vdots$

z $\leftrightarrow$ 25

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

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

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

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

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

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

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

ROT-K

a $\leftrightarrow$ 0

b $\leftrightarrow$ 1

c $\leftrightarrow$ 2

d $\leftrightarrow$ 3

e $\leftrightarrow$ 4

$\vdots$

z $\leftrightarrow$ 25

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

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

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

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

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

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

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

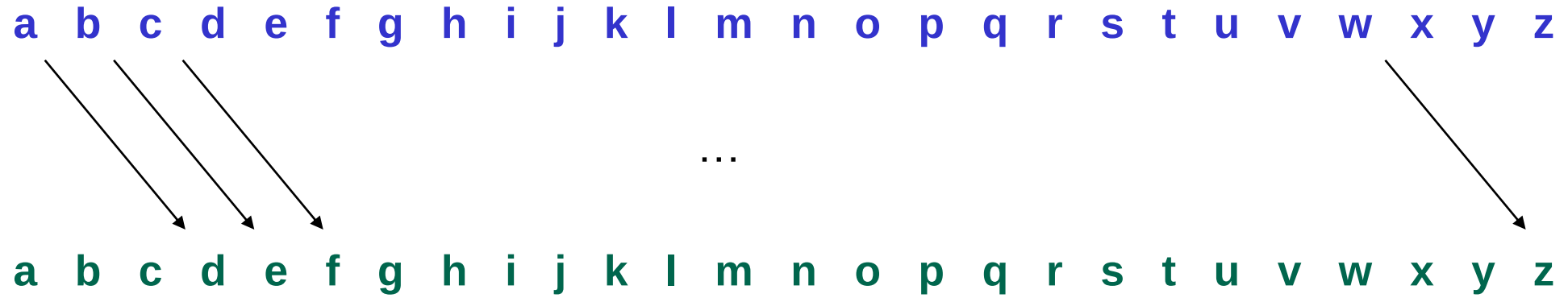
Attacking ROT-K

$$|\mathcal{K}| = 26$$

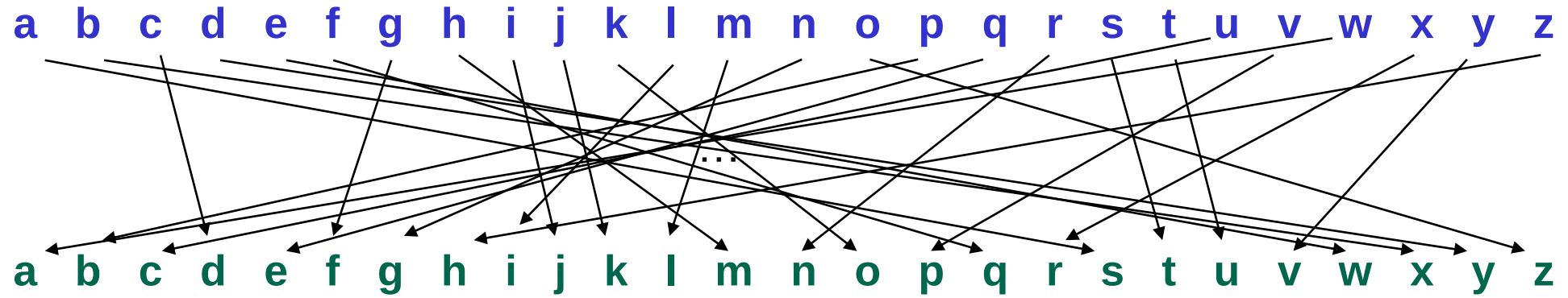
$C =$ va gur sne qvfgnapr n uryvpbcgre ...

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

↕ ↕ ↕ ↕

...

↕

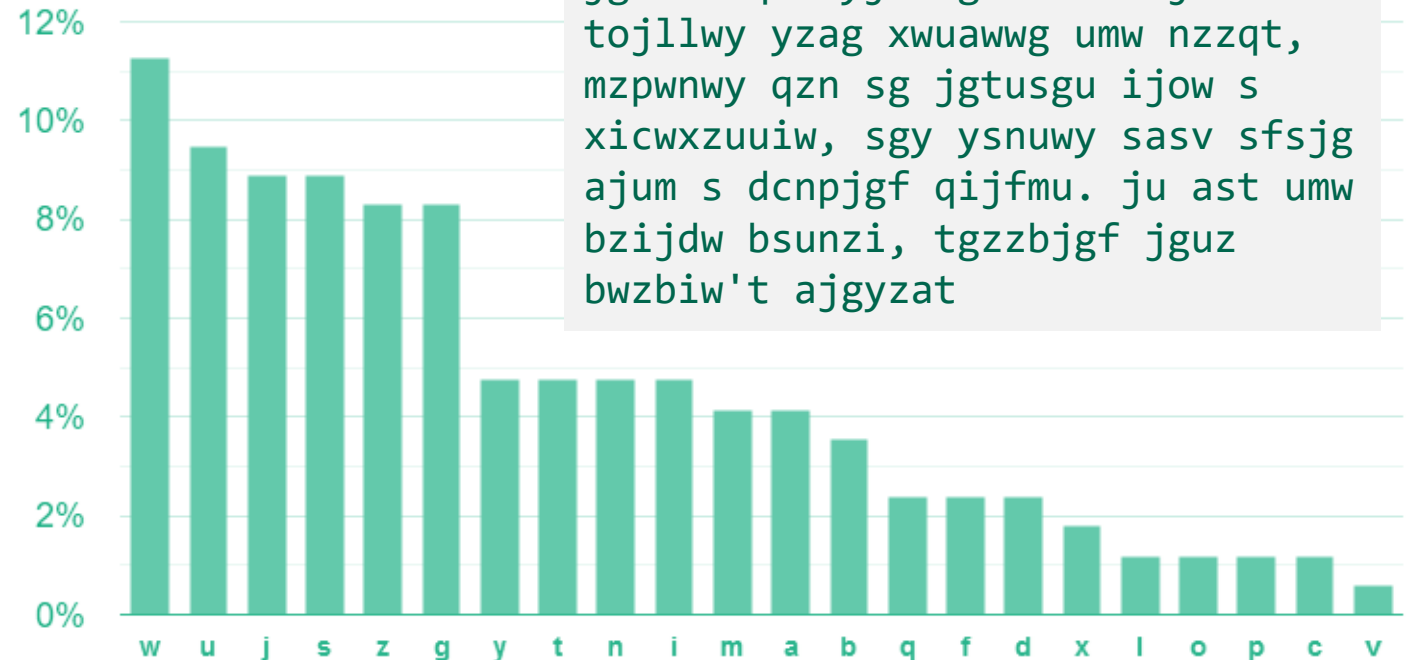
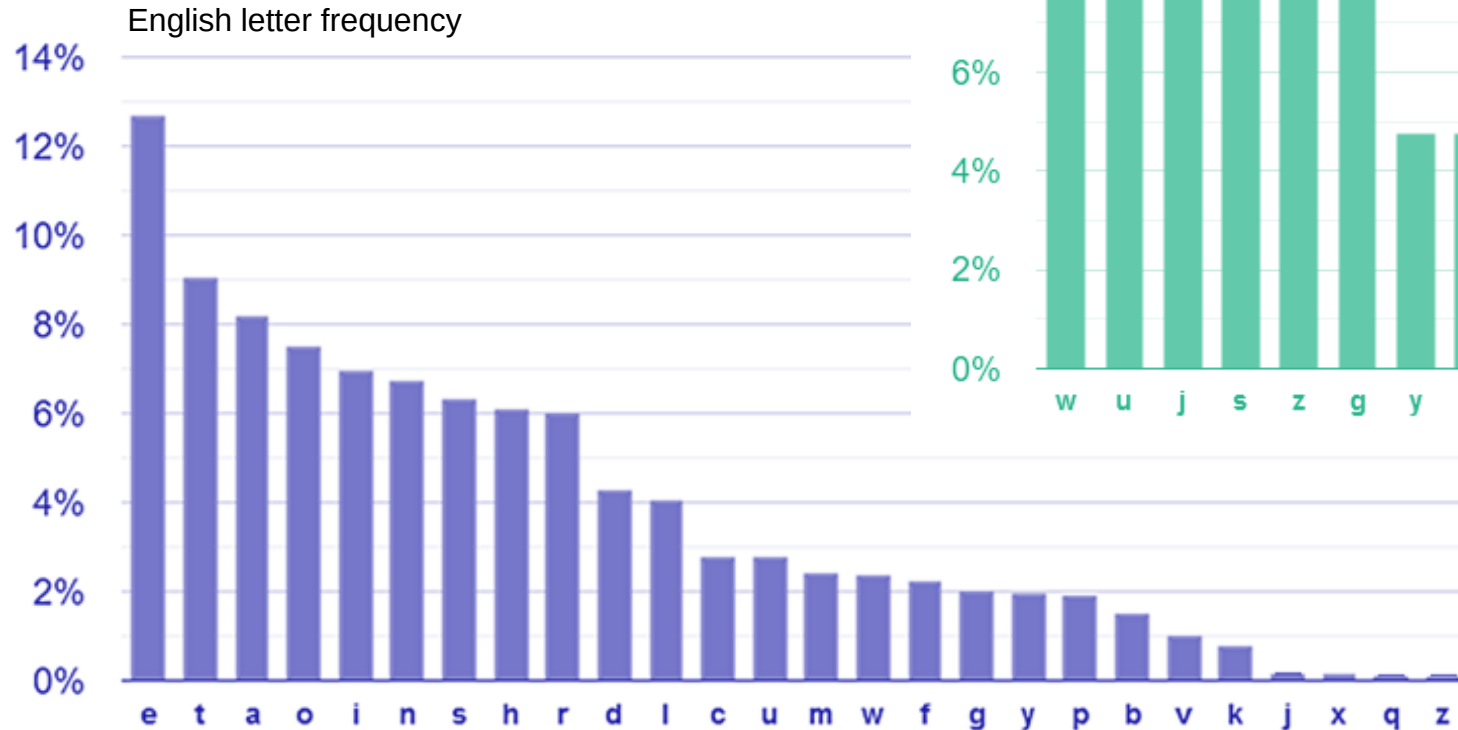
s x d y w q f m j k o i l g z b e n t u c p a r v h

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

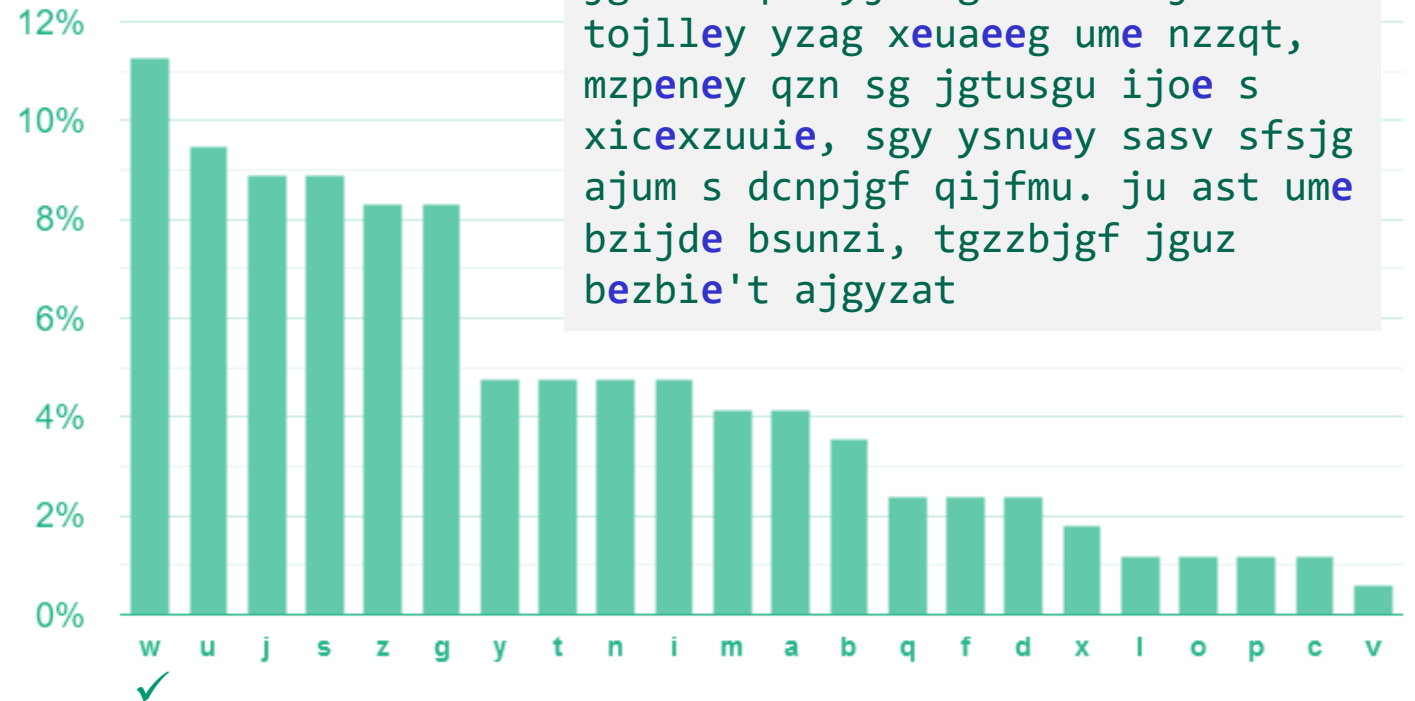
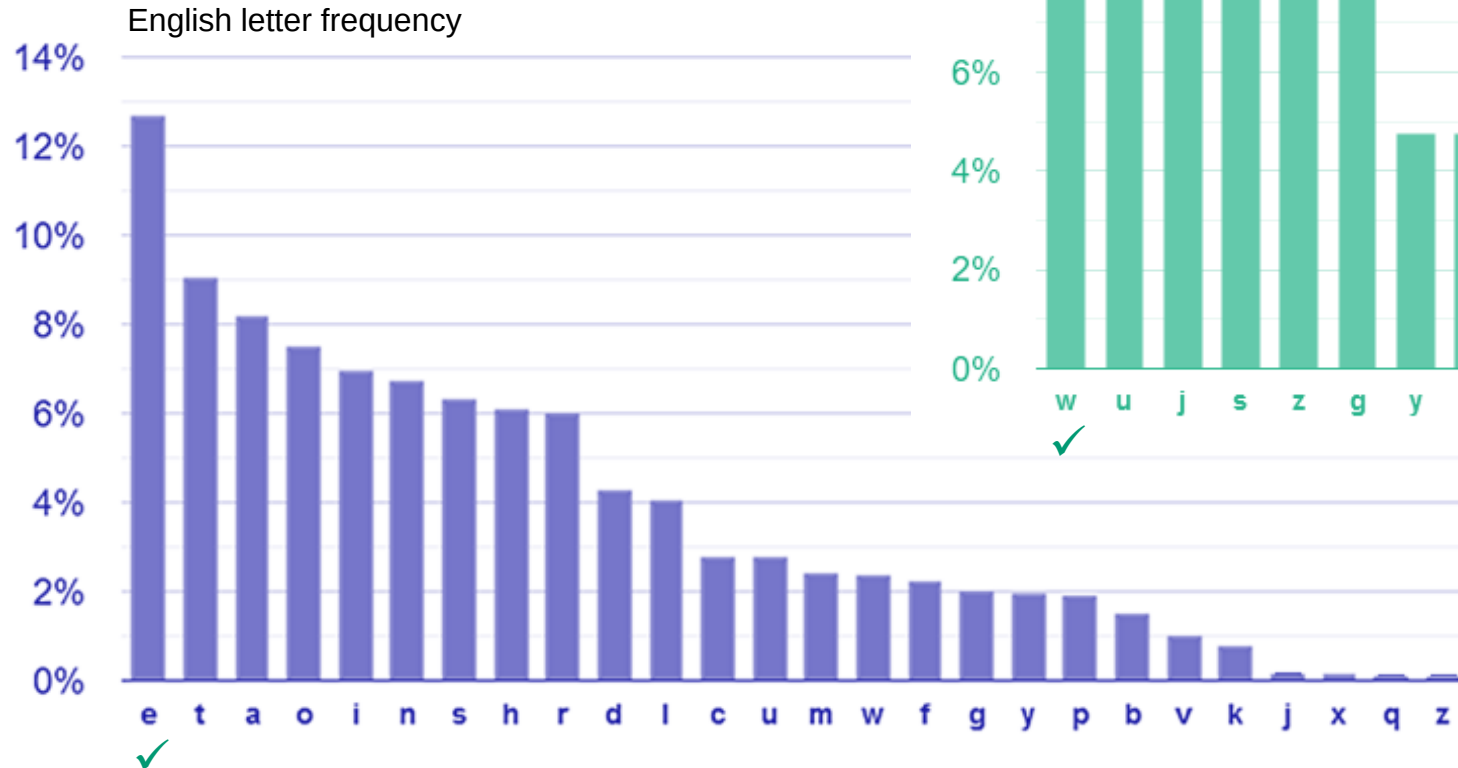
Attacking the substitution cipher

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



Attacking the substitution cipher

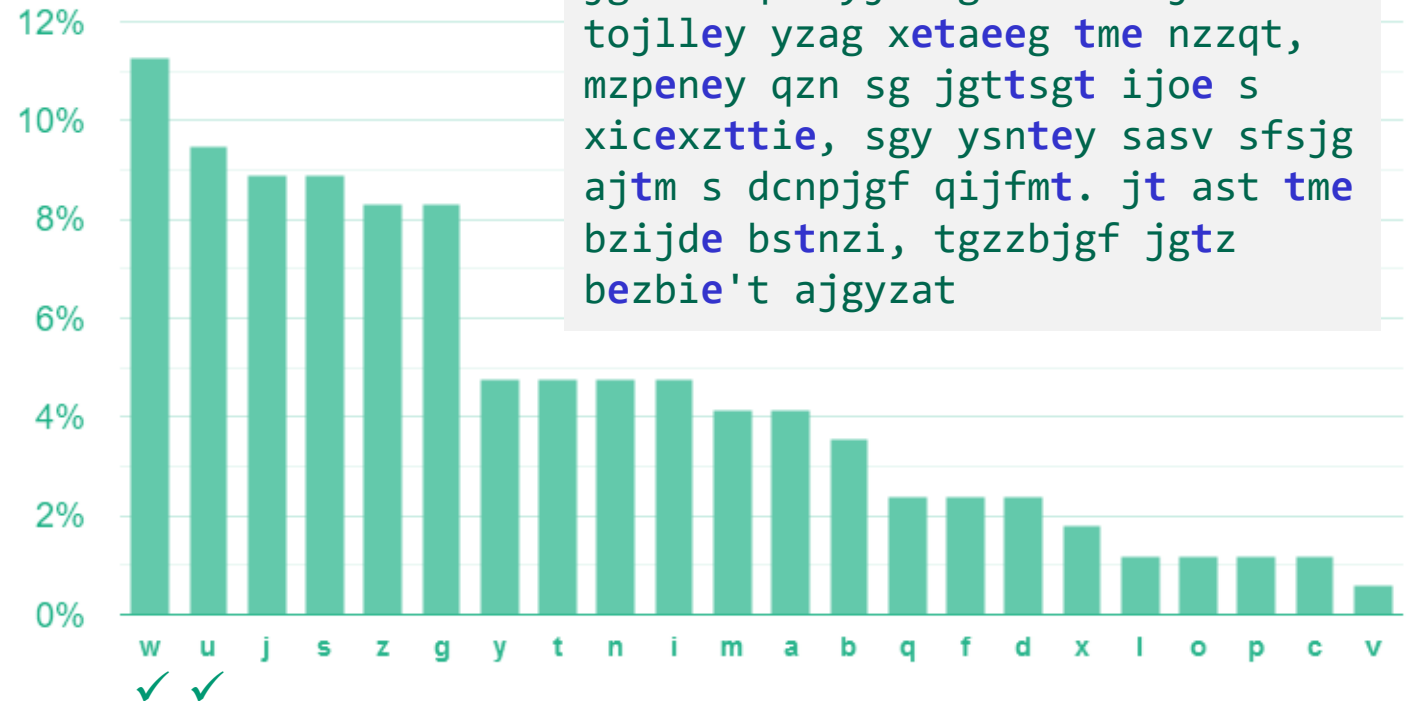
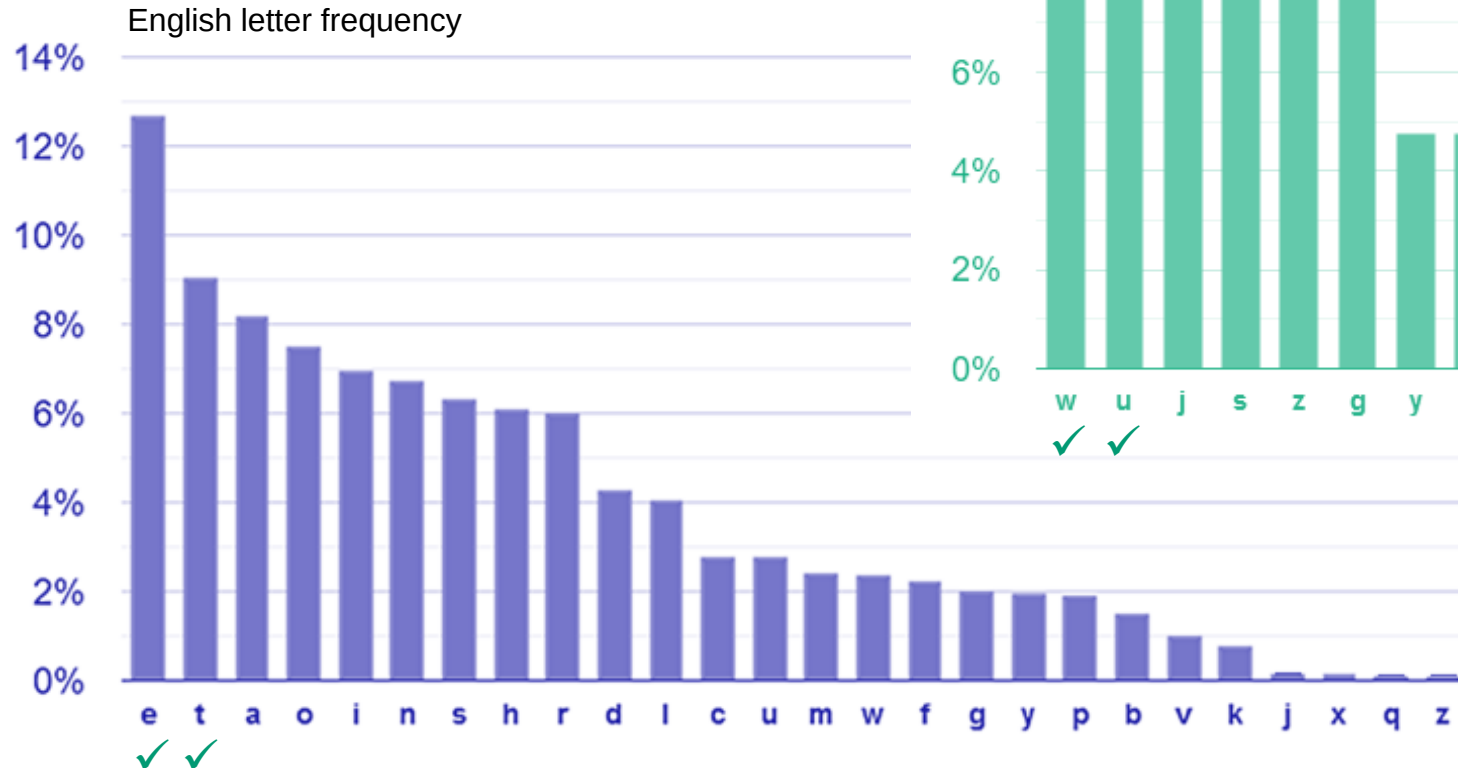
$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$



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

Attacking the substitution cipher

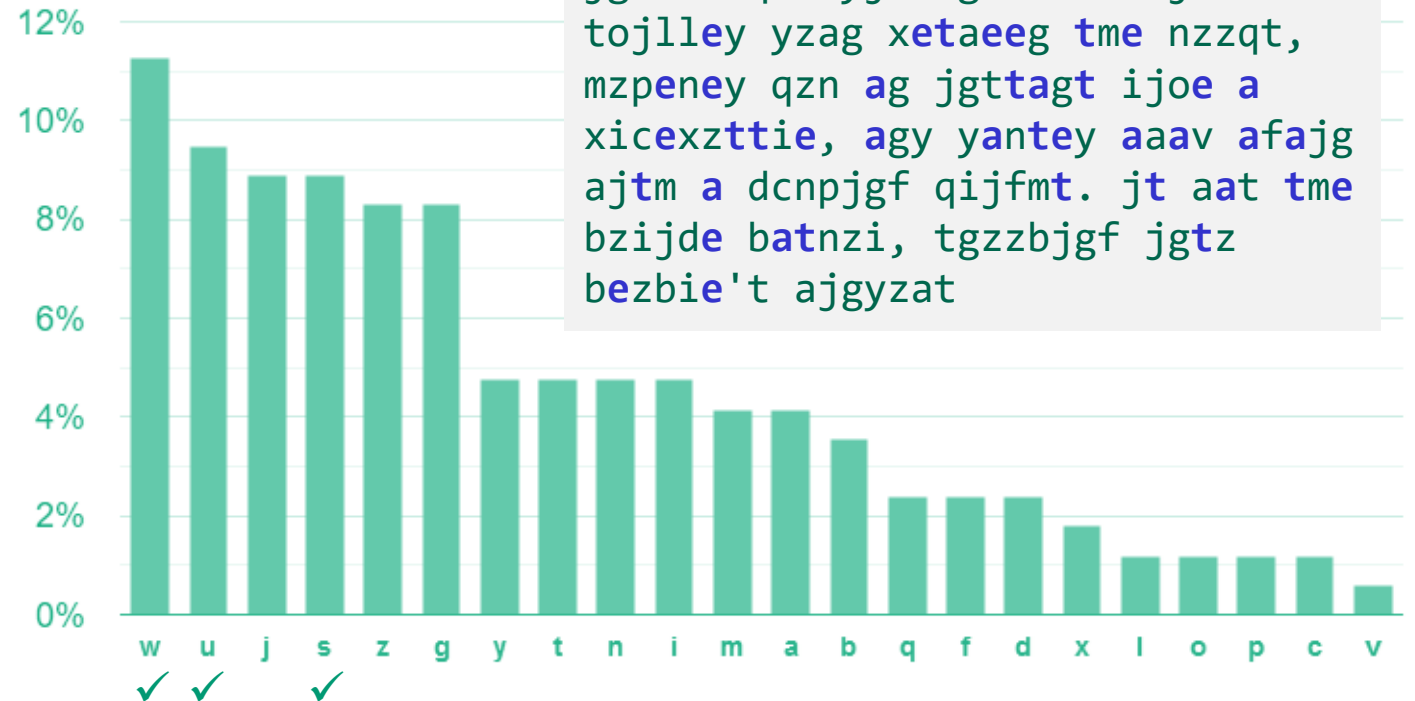
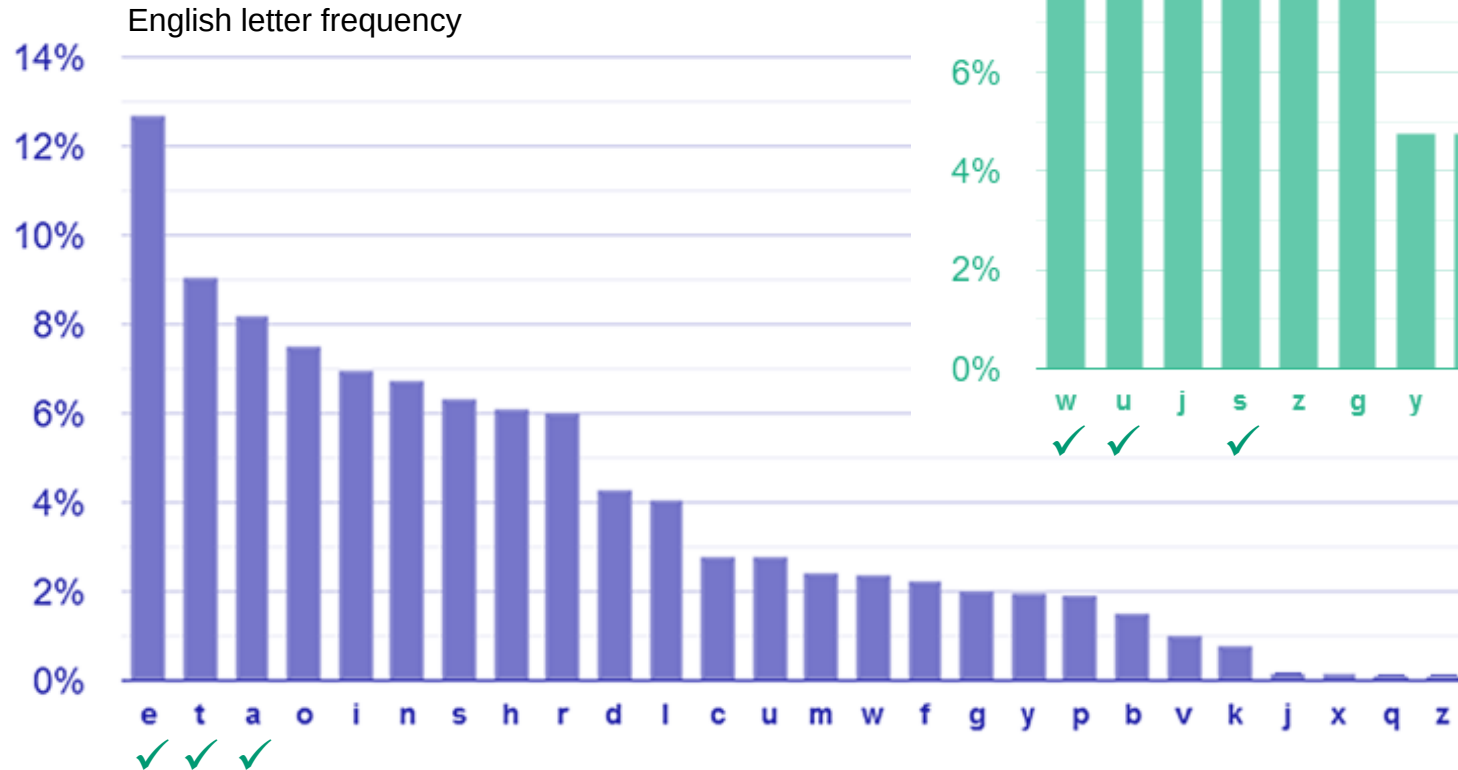
$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$



jg tme qsn yjttsge s meijdzbt
 tojlley yzag xetaeeg tme nzzqt,
 mzpeneey qzn sg jgttsge ijoe s
 xicexztie, sgy ysney sasv sfsjg
 ajtm s dcnpgf qijfmt. jt ast tme
 bzijde bstnzi, tgzzbjgf jgtz
 bezbie't ajgyzat

Attacking the substitution cipher

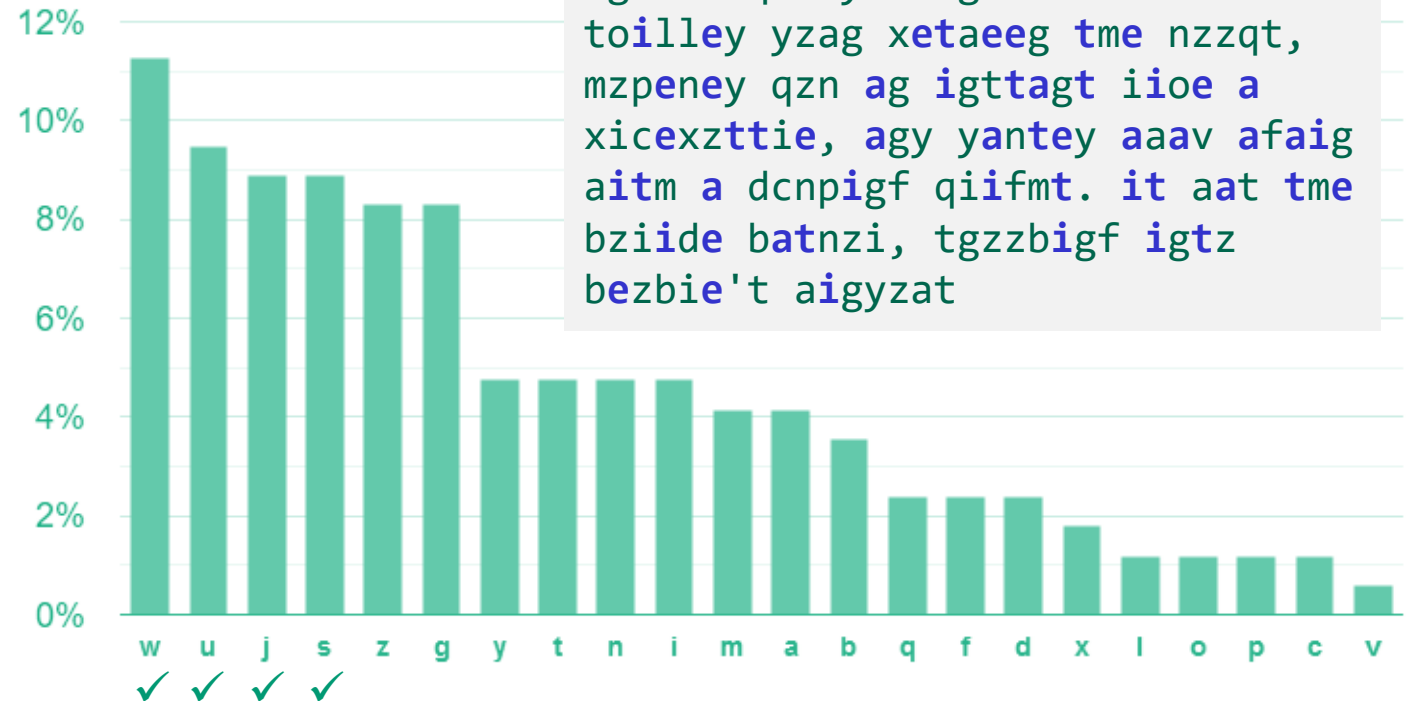
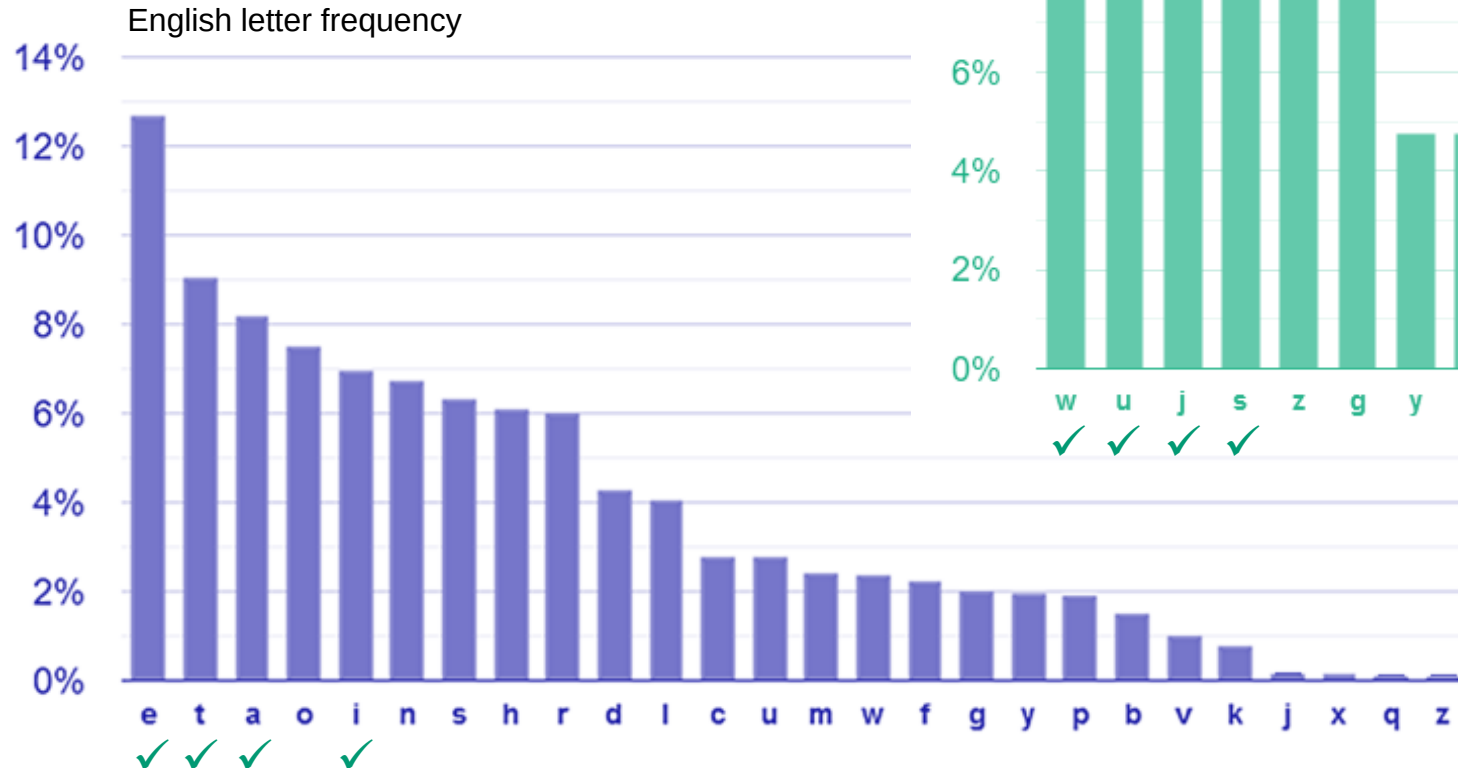
$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$



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

Attacking the substitution cipher

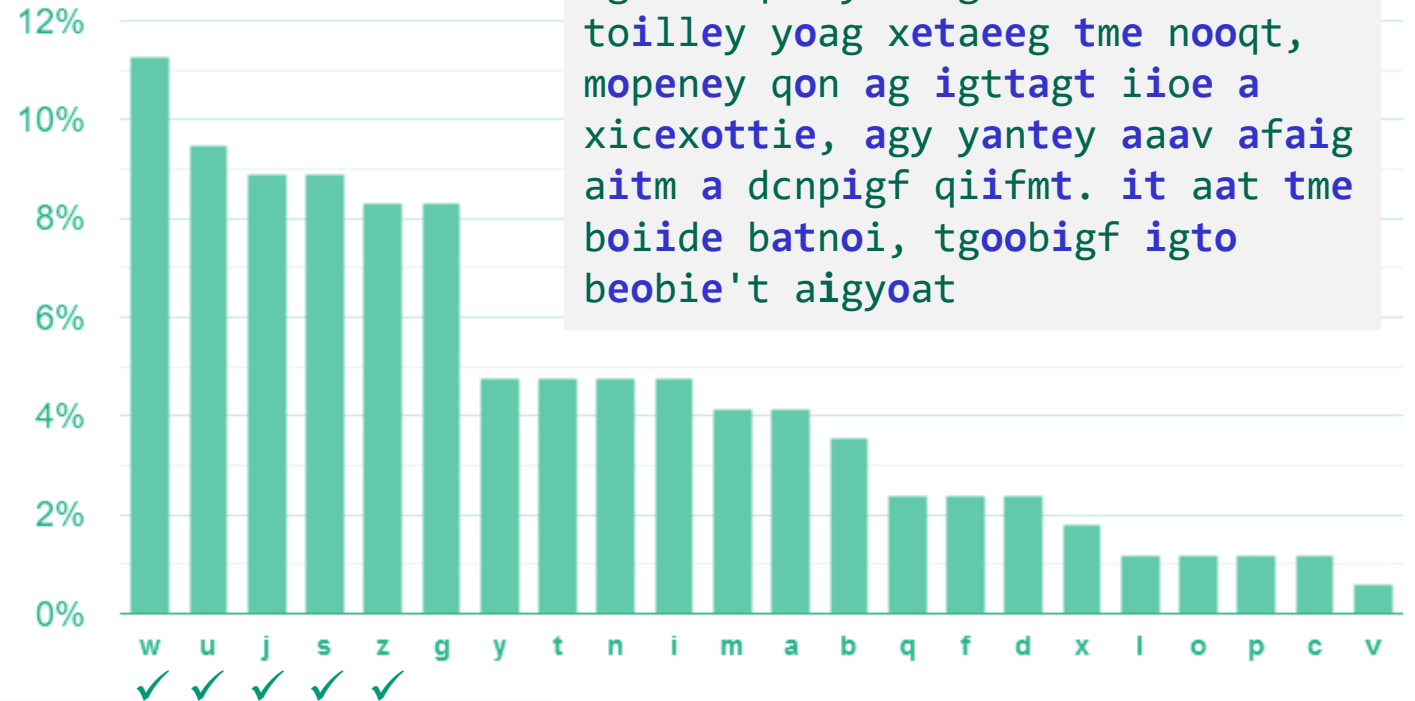
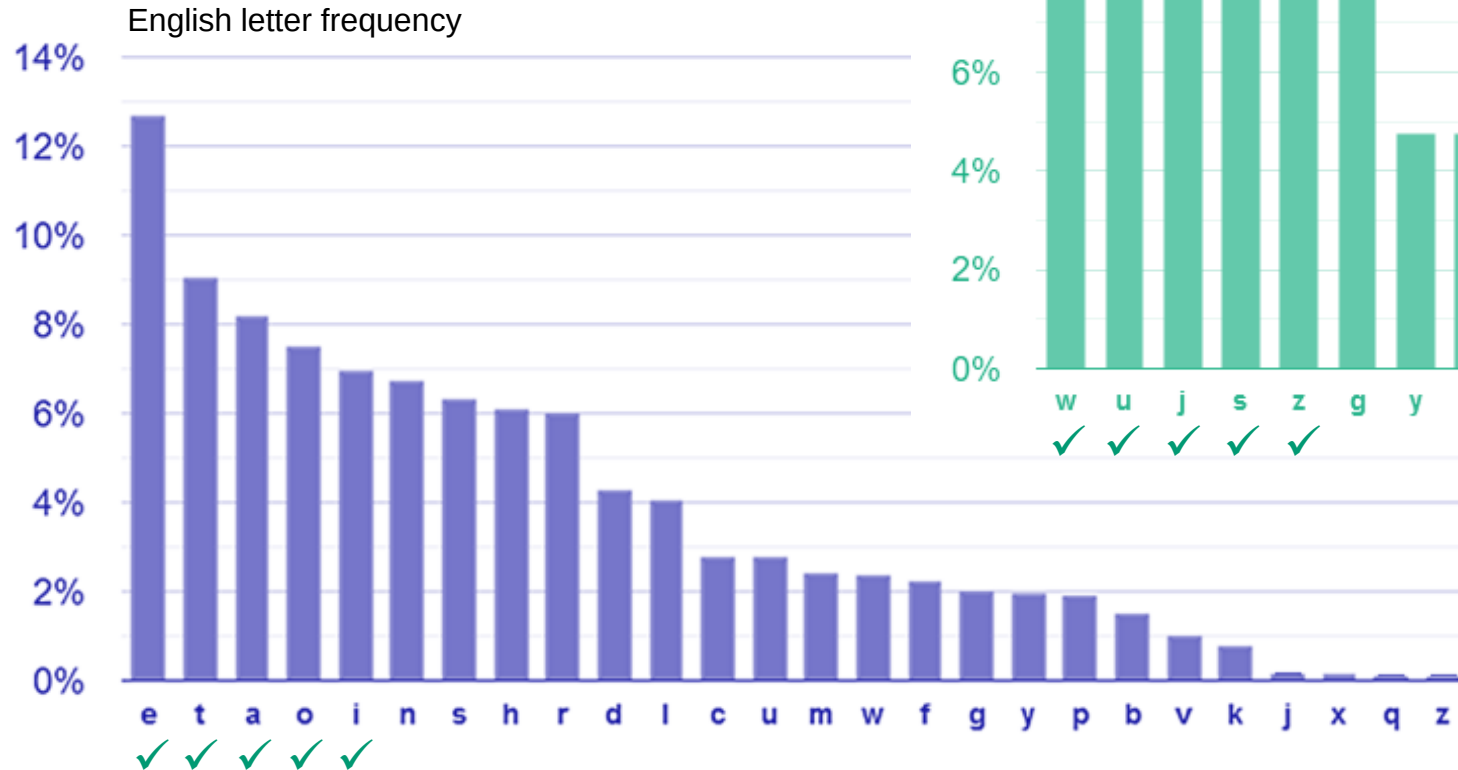
$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$



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

Attacking the substitution cipher

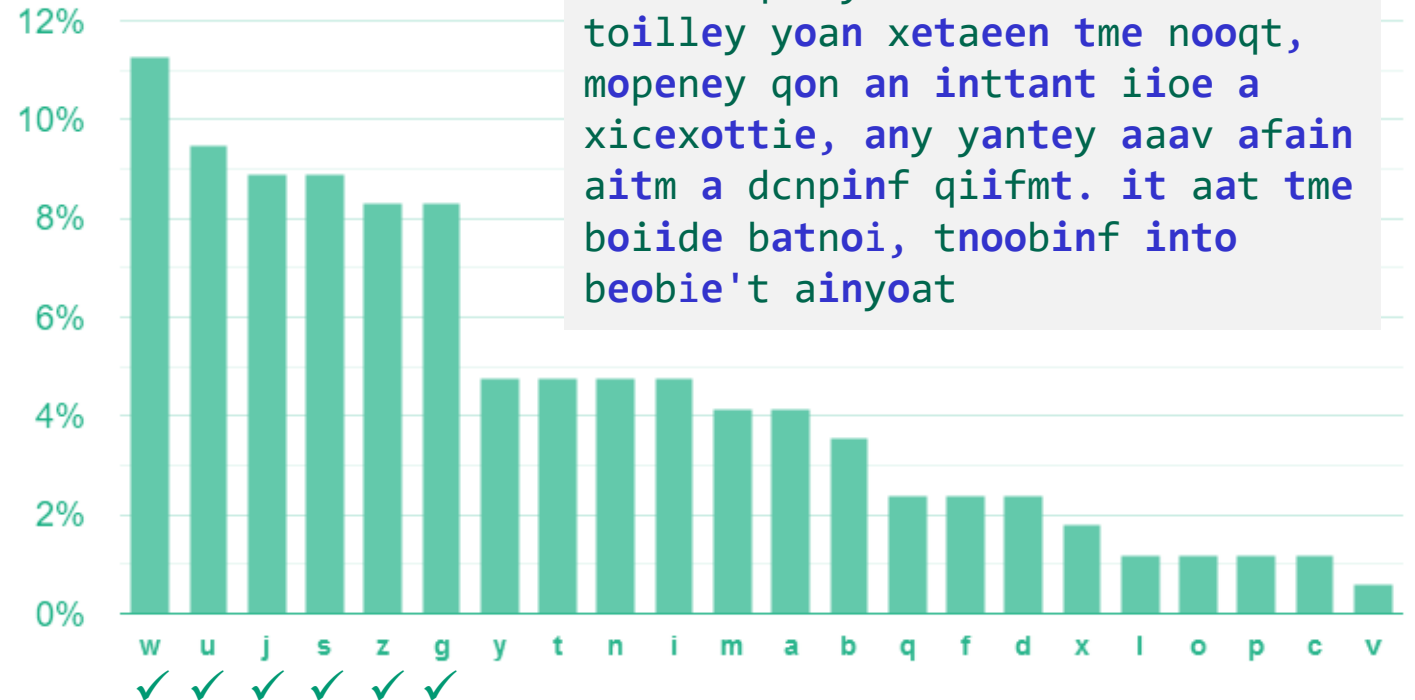
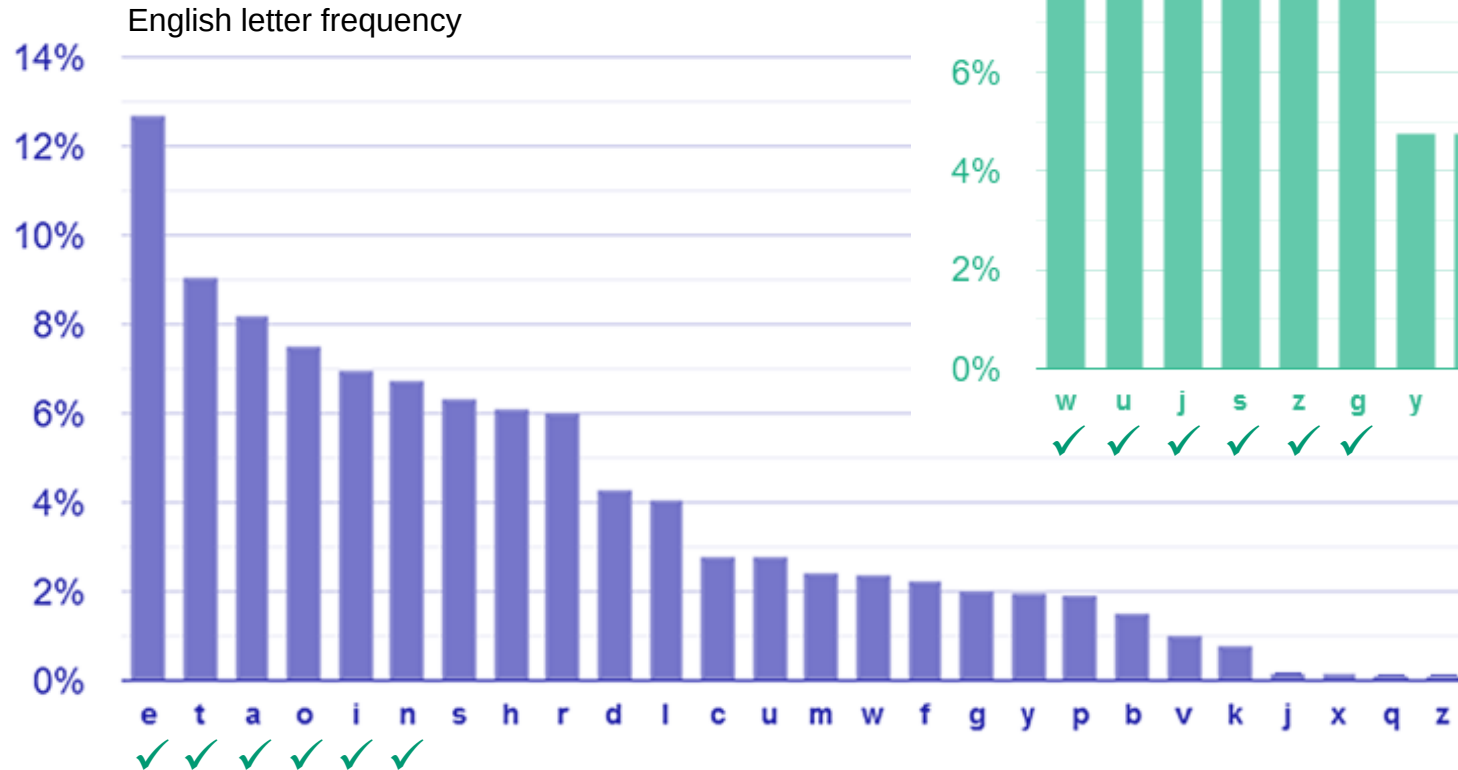
$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$



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

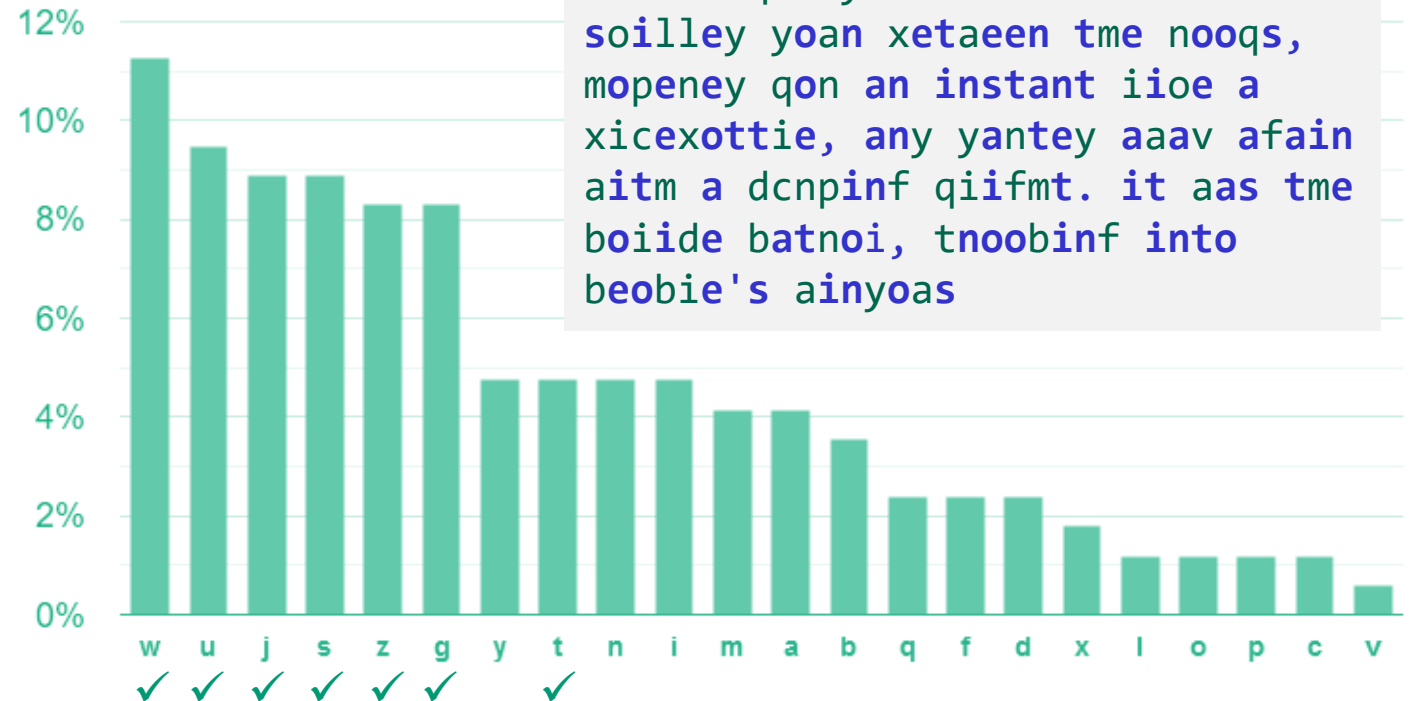
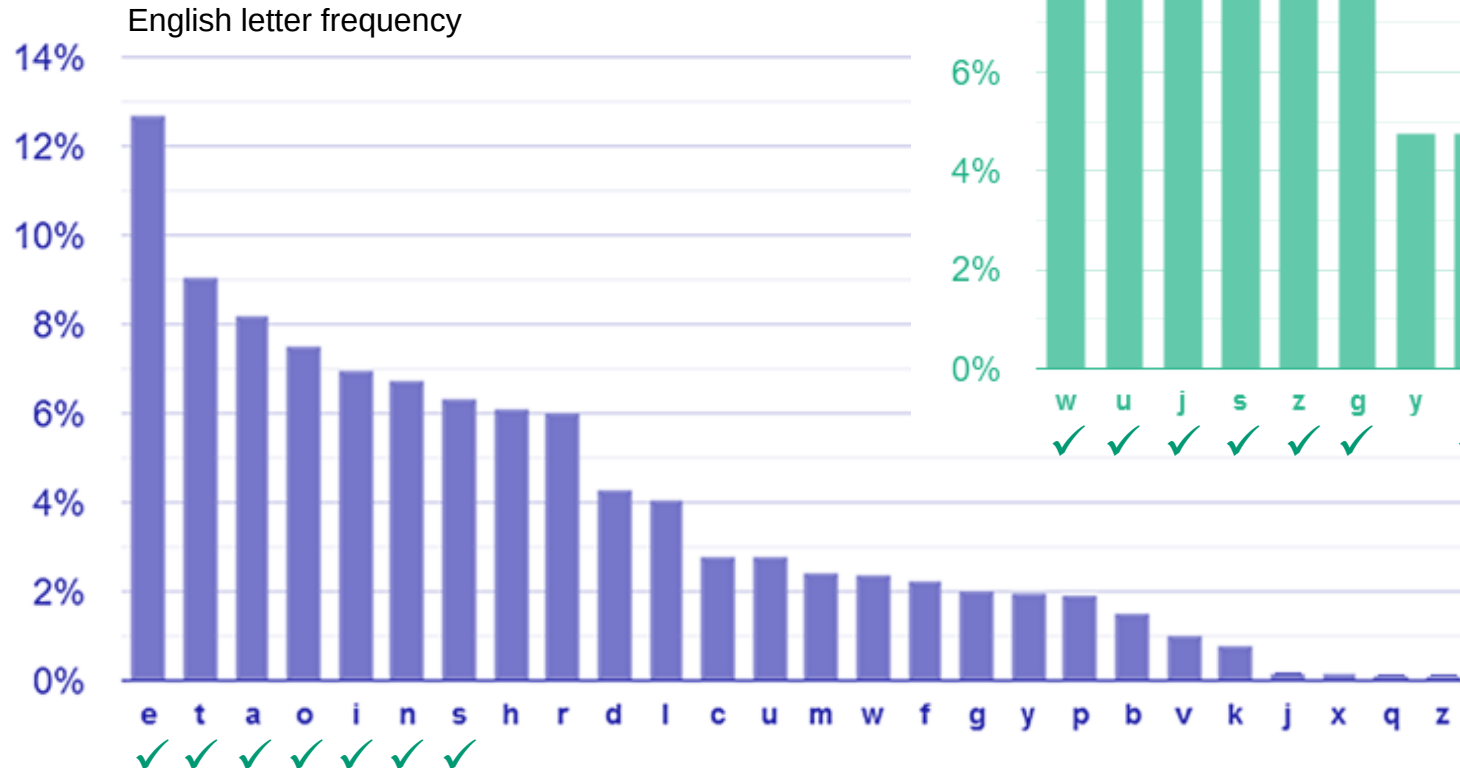
$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$



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

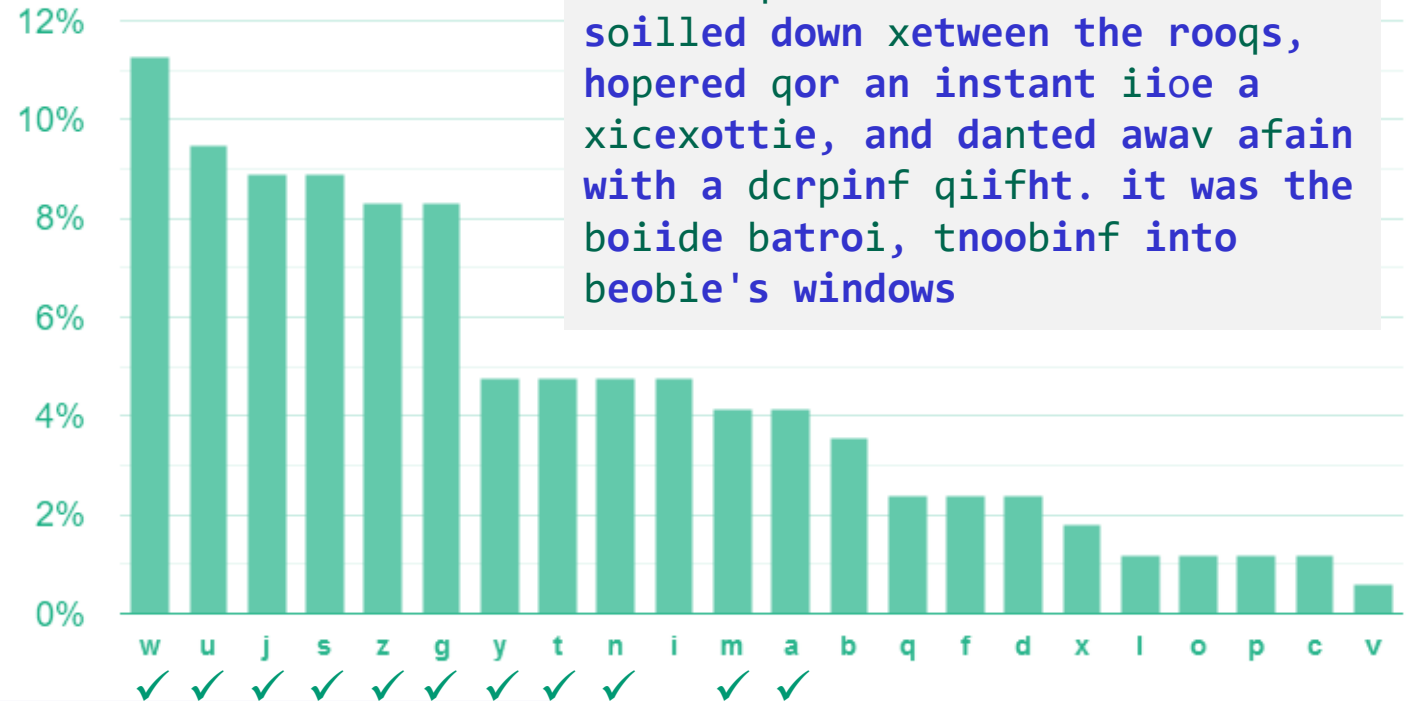
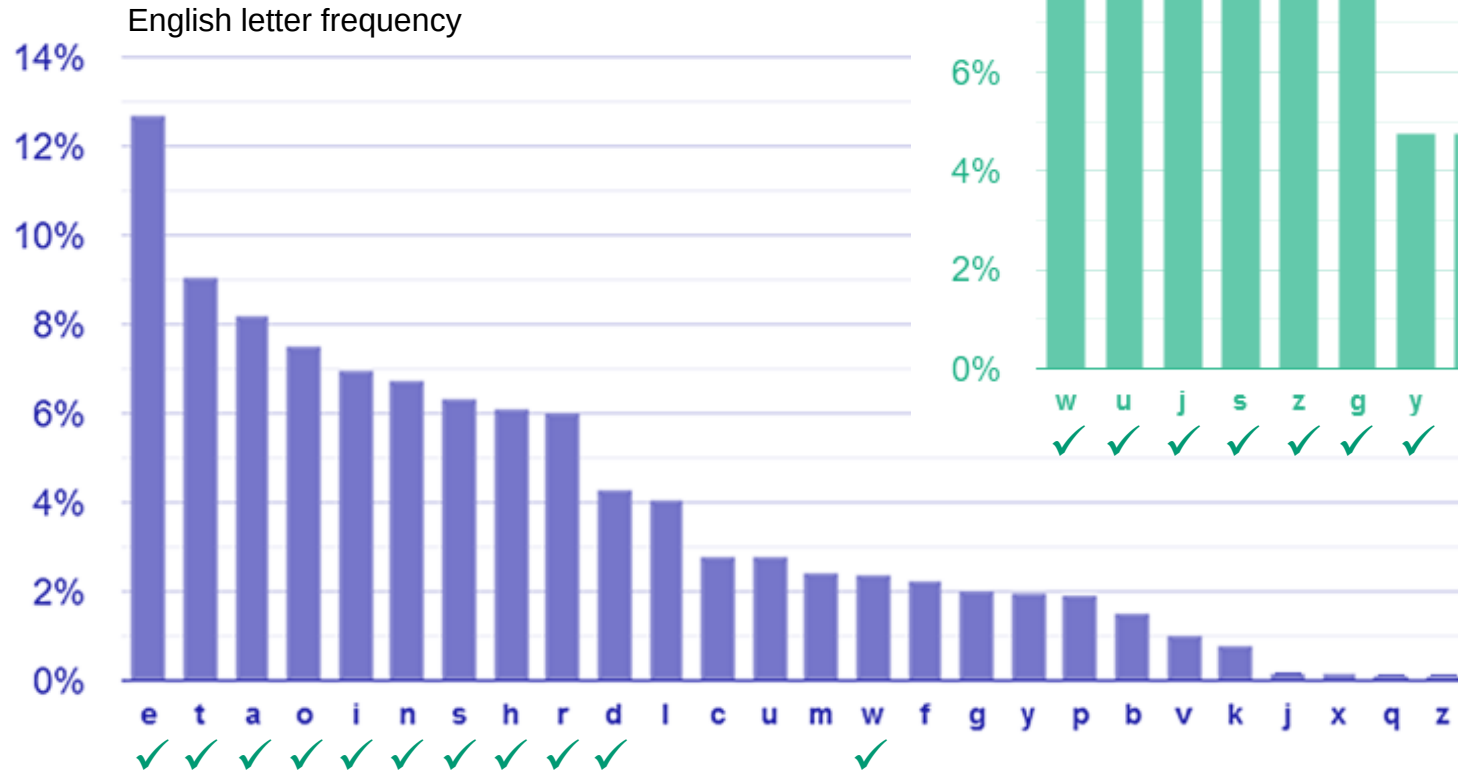
$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$



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

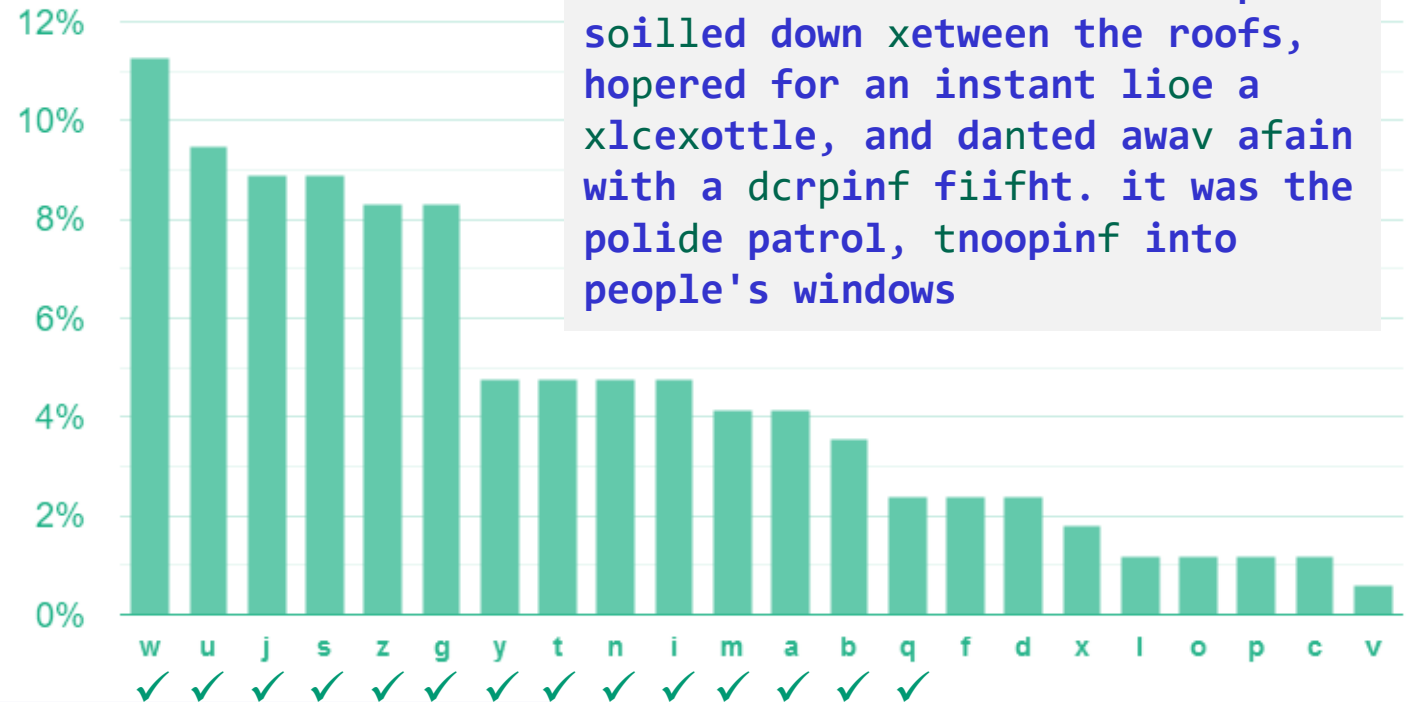
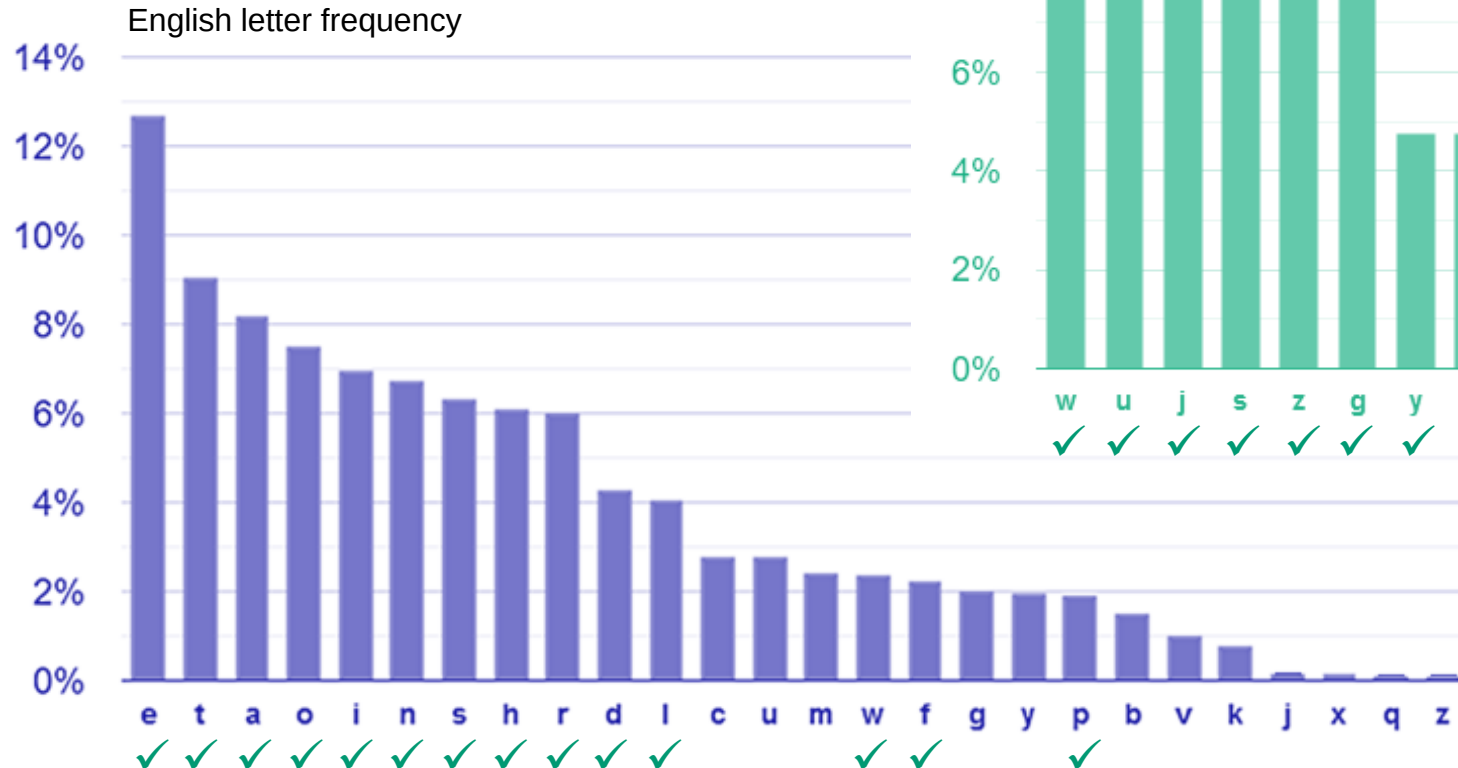
$$|\mathcal{K}| = 26! \approx 10^{26} \approx 2^{88}$$



in the qar 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 the
boiide batroi, tnoobinf into
beobie's windows

Attacking the substitution cipher

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

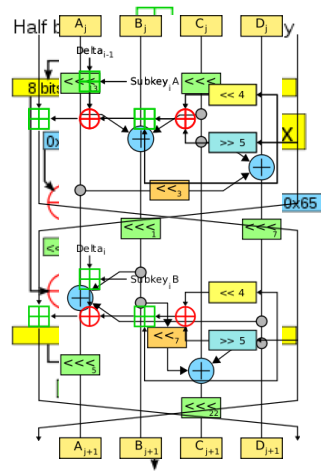


in the far distande a helidopter
soilled down xetween the roofs,
hopered for an instant lioe a
xlcexottle, and danted awav afain
with a dcrpinf fiifht. it was the
polide patrol, tnoopinf into
people's windows

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 $\rightarrow$ break $\rightarrow$ fix $\rightarrow$ break $\rightarrow$ fix $\rightarrow$ break $\rightarrow$ 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)

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

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

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

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

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

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

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

Is the one-time pad secure?

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 $C \in \mathcal{C}$

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

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

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

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?

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

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

Wanted: security definition for symmetric encryption

computational

- ~~One-time perfect~~ privacy:

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

resource bounded

- Security holds for *any* adversary ~~(no limit on resource usage)~~
- Very strict requirements:
 - ~~Key needs to be as long as the message~~ ✓
 - ~~Key can only be used for one message~~ ✓

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

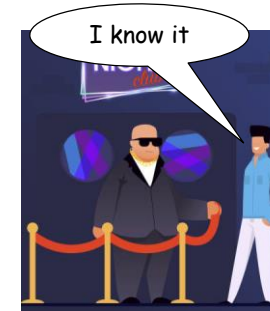
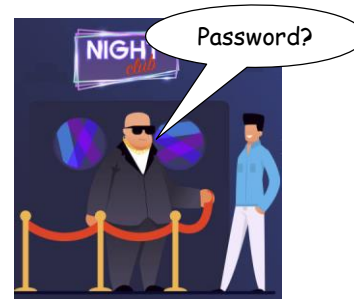
Outline of course

	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

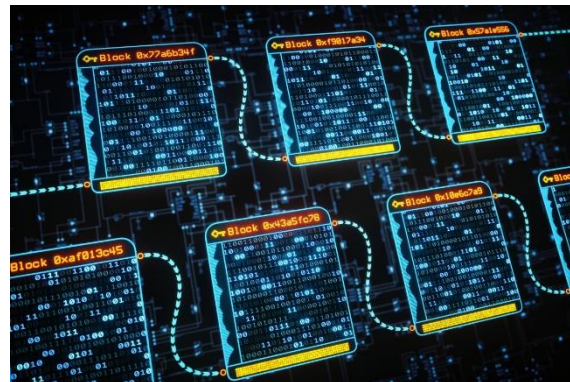
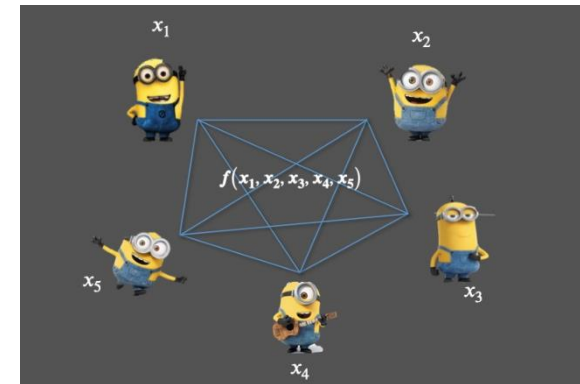
Part II

Much more to cryptography

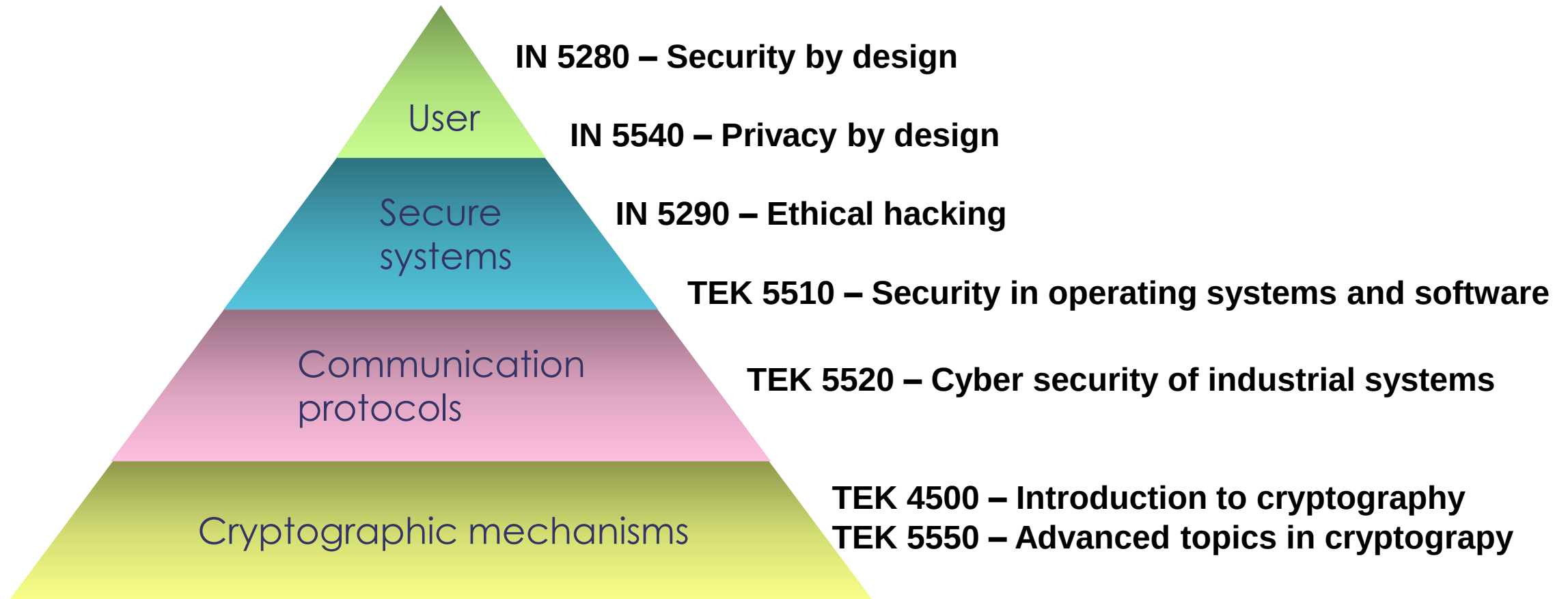
- Zero-knowledge proofs
- Fully-homomorphic encryption
- Multi-party computation
- Blockchains

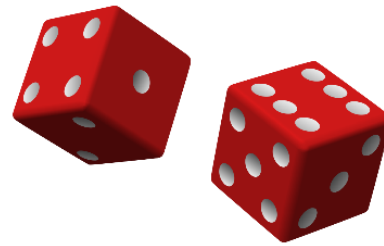


$$\text{Enc}(K, M_1 + M_2) = \text{Enc}(K, M_1) + \text{Enc}(K, M_2)$$



The security pyramid





Discrete probability

the bare minimum

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

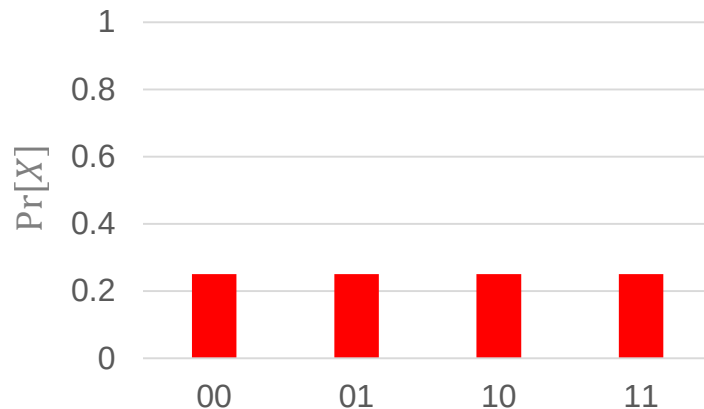
Discrete probability

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

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

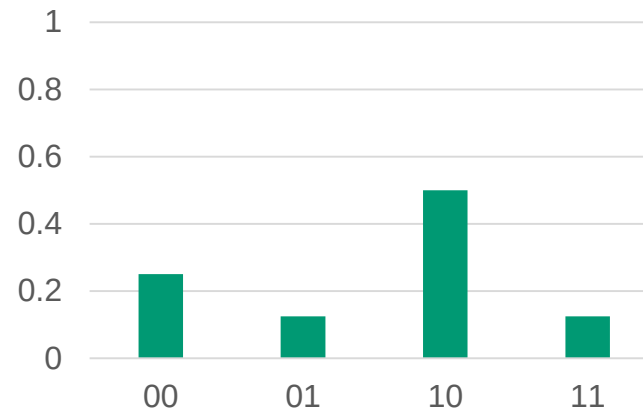
$$\sum_{X \in \mathcal{U}} \Pr[X] = 1$$

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

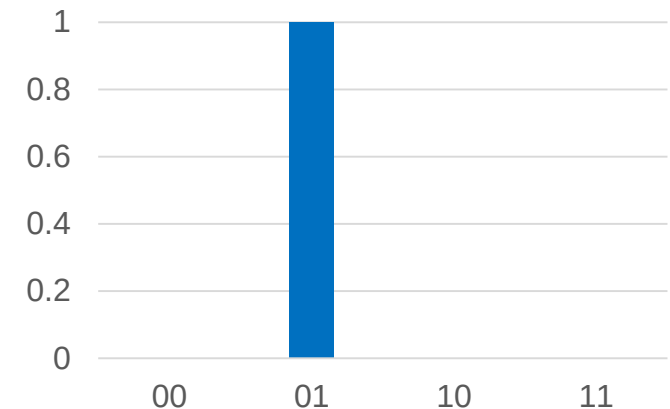


$$\begin{aligned}\Pr[00] &= 1/4 \\ \Pr[01] &= 1/4 \\ \Pr[10] &= 1/4 \\ \Pr[11] &= 1/4\end{aligned}$$

Uniform distribution



$$\begin{aligned}\Pr[00] &= 1/4 \\ \Pr[01] &= 1/8 \\ \Pr[10] &= 1/2 \\ \Pr[11] &= 1/8\end{aligned}$$



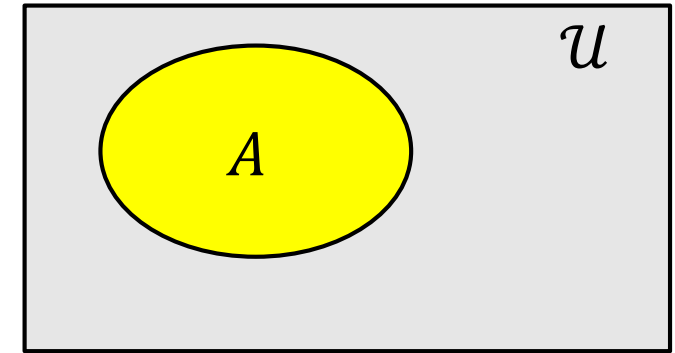
$$\begin{aligned}\Pr[00] &= 0 \\ \Pr[01] &= 1 \\ \Pr[10] &= 0 \\ \Pr[11] &= 0\end{aligned}$$

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

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

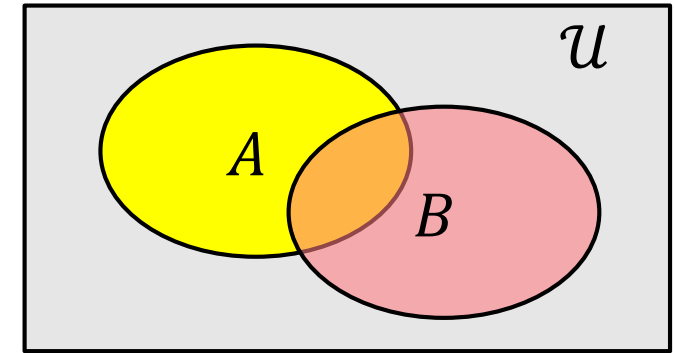
With the uniform distribution over $\mathcal{U}$, what is $\Pr[A]$?

- **Answer:** $\Pr[A] = \Pr[\text{1100 0000}] + \Pr[\text{1100 0001}] + \dots + \Pr[\text{1111 1111}]$
 $= 2^6 \cdot 1/2^8$
 $= 1/2^2$
 $= 1/4$

Union bound

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

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



- **Example:** suppose we have $N = 200$ computers, where each one fails with probability 0.001. What is the probability that *at least one* server fails?
- **Answer:** Let A_i be the event that server i fails. Then *at least one server fails* $= A_1 \cup A_2 \cup \dots \cup A_{200}$,

$$\Pr[A_1 \cup A_2 \cup \dots \cup A_{200}] \leq \Pr[A_1] + \Pr[A_2] + \dots + \Pr[A_{200}] = 0.001N = 0.2$$

Independence

- Events A and B are **independent** if $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$
- **Example:** Suppose we flip two fair coins. Let
 - A_1 : first coin is heads
 - A_2 : second coin is heads
 - A_3 : the coins are different
- $\Pr[A_1] = \Pr[A_2] = \Pr[A_3] = 1/2$
- $\Pr[A_1 \cap A_2] = 1/4$
- $\Pr[A_1 \cap A_3] = 1/4$
- $\Pr[A_2 \cap A_3] = 1/4$
- $\Pr[A_1 \cap A_2 \cap A_3] = 0$

Law of total probability

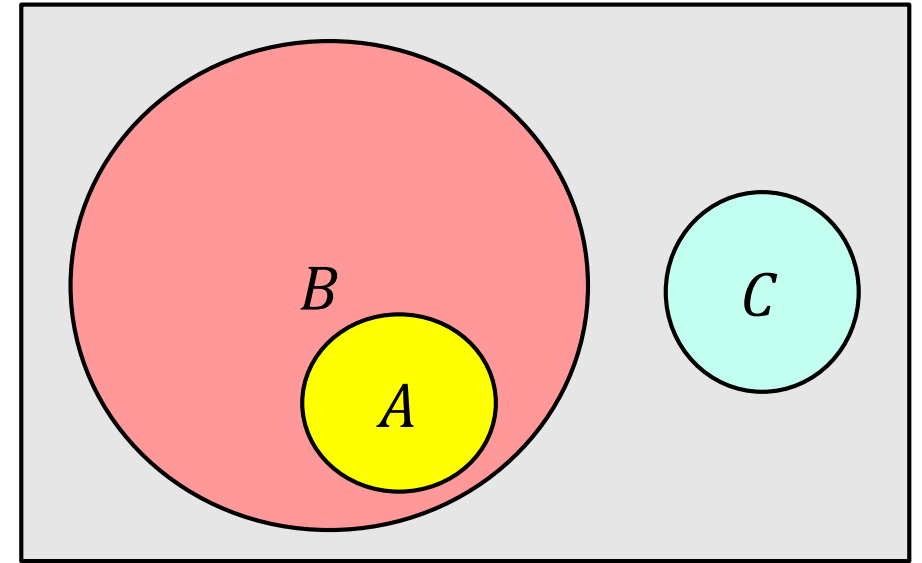
- Conditional probability

$$\Pr[X | Y] \stackrel{\text{def}}{=} \frac{\Pr[X \cap Y]}{\Pr[Y]}$$

assuming $\Pr[Y] > 0$

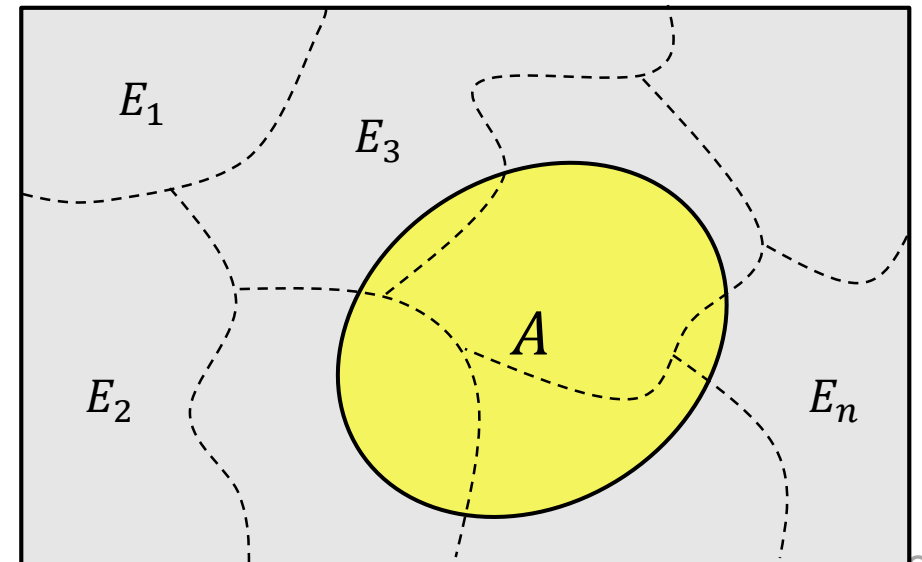
$$\Pr[A | B] > \Pr[A]$$

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



- Law of total probability

$$\begin{aligned} \Pr[A] &= \Pr[A | E_1] \cdot \Pr[E_1] \leq \Pr[E_1] \\ &\quad + \Pr[A | E_2] \cdot \Pr[E_2] \leq \Pr[A | E_2] \\ &\quad \vdots \\ &\quad + \Pr[A | E_n] \cdot \Pr[E_n] \leq \Pr[E_n] \end{aligned}$$



Law of total probability

See full problem here: <https://nitter.poast.org/littmath/status/1827447490683003234>

- **Example**

You have 10,000 coins. 9999 of them are fair; one is rigged so that it always lands on heads. You choose a coin at random and flip it 10 times. What is the probability that it comes up heads every time?

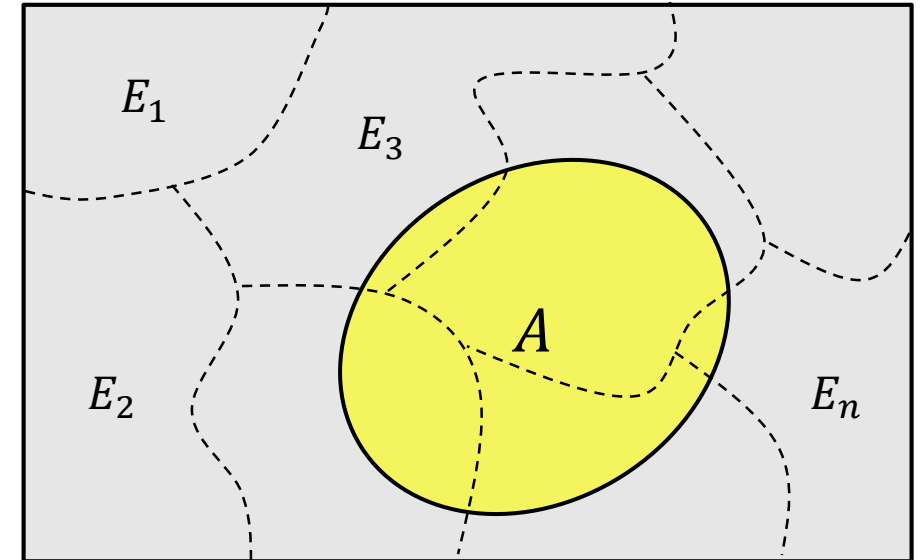
- **Answer**

Let R be the event that the coin is rigged. Let F be event that it is fair. Let H_{10} be the event that it comes up heads 10 times.

- $\Pr[R] = 1/10,000$
- $\Pr[F] = 1 - \Pr[R] = 1 - 1/10,000 = 9999/10,000$
- $\Pr[H_{10}] = \Pr[H_{10} \mid R] \cdot \Pr[R] + \Pr[H_{10} \mid F] \cdot \Pr[F]$

$$= 1 \cdot 1/10,000 + \frac{1}{2^{10}} \cdot 9999/10,000 \approx 0.00108$$

$$\frac{1}{2^{10}} \approx 0.00098$$



Random variables

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

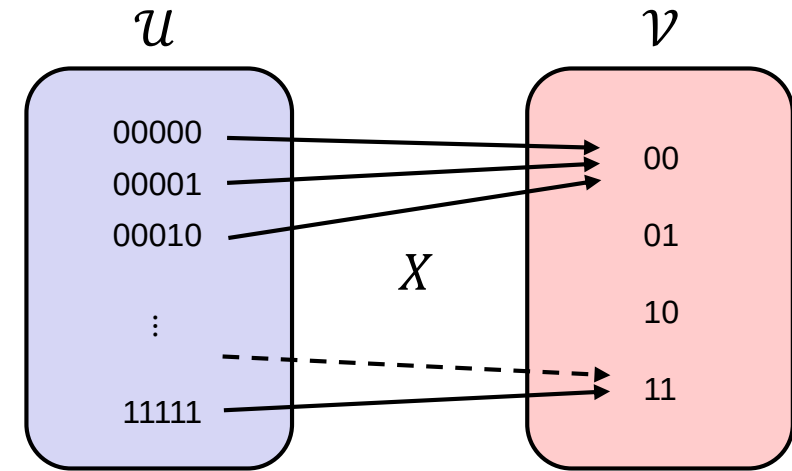
Example:

$$\begin{aligned} X : \overset{\mathcal{U}}{\{0,1\}^5} &\rightarrow \overset{\mathcal{V}}{\{0,1\}^2} \\ X(s) &\stackrel{\text{def}}{=} \text{msb}_2(s) \end{aligned}$$

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

↑
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:

$$X : \overset{\mathcal{U}}{\{0,1\}^5} \rightarrow \overset{\mathcal{V}}{[0,1,2,\dots,10]}$$
$$X(s) \stackrel{\text{def}}{=} s_1 + s_2 + s_3 + s_4 + s_5$$

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

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

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

$\vdots$

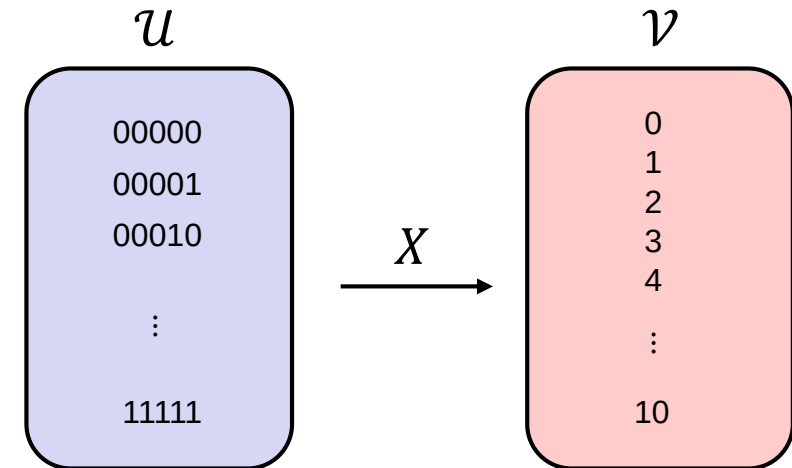
$$\Pr[X = 5] = 1/32$$

$$\Pr[X = 6] = 0$$

$\vdots$

$$\Pr[X = 10] = 0$$

Uniform distribution on $\mathcal{U}$
but not on $\mathcal{V}$!



Random variables

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

Example:

$$X : \overset{\mathcal{U}}{\{0,1\}^5} \rightarrow \overset{\mathcal{V}}{[0,1,2,\dots,10]}$$
$$X(s) \stackrel{\text{def}}{=} s_1 + s_2 + s_3 + s_4 + s_5$$

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

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

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

$\vdots$

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

$$\Pr[X = 6] = 0$$

$\vdots$

$$\Pr[X = 10] = 0$$

Uniform distribution on $\mathcal{U}$
but not on $\mathcal{V}$!

$\mathcal{V}$	
X	0 1/32
	1 5/32
	2 10/32
	3 10/32
	4 5/32
	$\vdots$
	10 0

Randomized algorithms

- Deterministic algorithm:

$$y \leftarrow A(x)$$

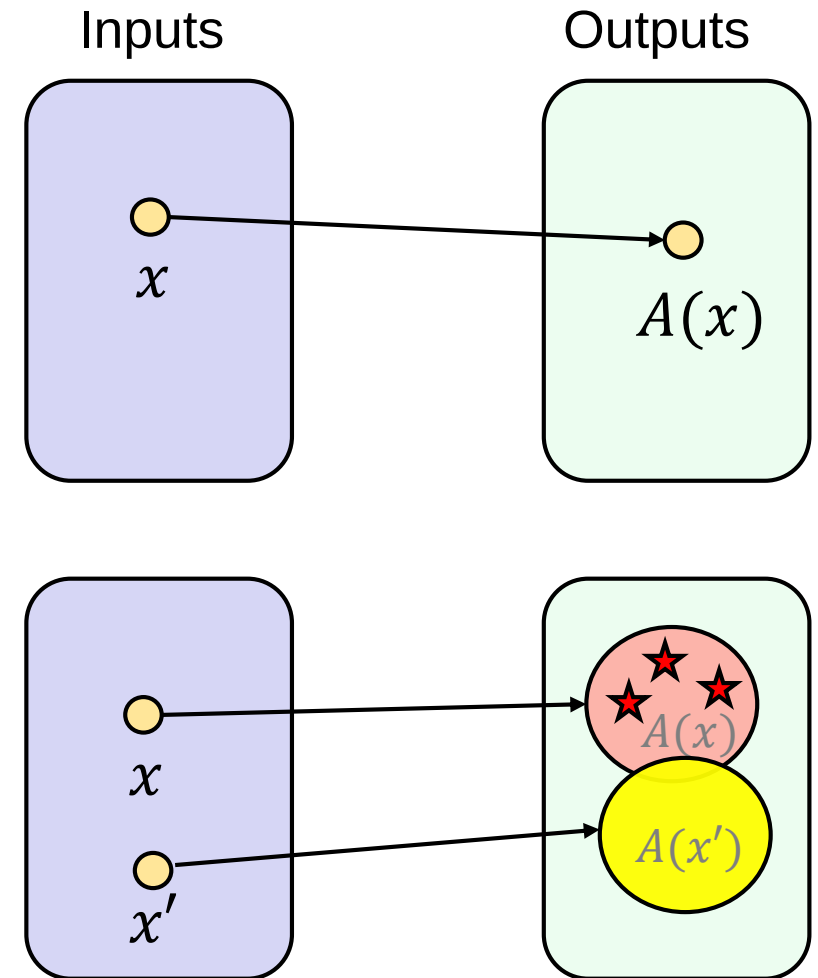
- Randomized algorithm:

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

$$y \stackrel{\$}{\leftarrow} A(x) \quad \textcolor{red}{A(x) \text{ is a random variable!}}$$

- Example:**

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



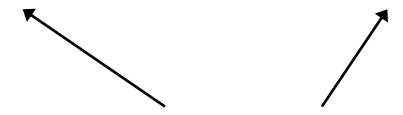
Randomized algorithms

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

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

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

- What does "*where the probability is over the random choice $K \overset{\$}{\leftarrow} \mathcal{K}$* " mean?
 - Notice that M_1 and M_2 are *fixed* in the definition
 - What *varies* is the choice of the key K (assuming $\mathcal{E}$ is deterministic)
 - Thus, formally we have a *random variable* $\mathcal{E}(\cdot, M) : \mathcal{K} \rightarrow \mathcal{C}$ (sample space: $\mathcal{K}$)
 - The probability that $\mathcal{E}(\cdot, M) = C$ is thus "*all $K \in \mathcal{K}$ such that $\mathcal{E}(K, M) = C$* " / " *$|\mathcal{K}|$* "


 $|\mathcal{X}|$ = size of set $\mathcal{X}$

Next week

- Block ciphers
- Pseudorandom functions and pseudorandom permutations
- AES