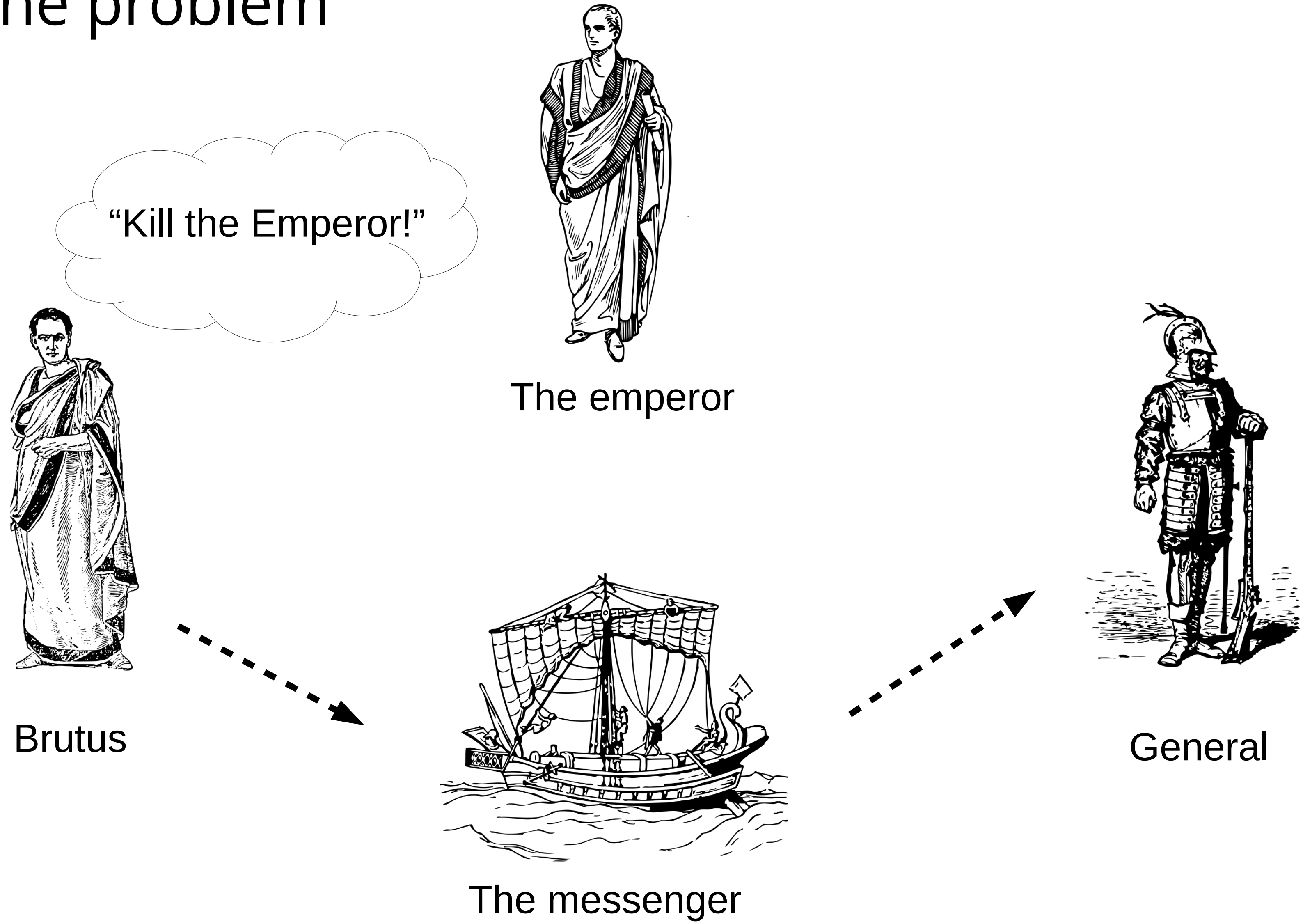
Cryptography

101

https://padlet.com/matthew_john_edwards/omuzpo0axjsj

The problem



"Kill the Emperor!"

The emperor

Brutus

The messenger

General

Solutions (that aren’t cryptography)

1. Encoding
2. Steganography
3. One-way functions (Not really a solution)

Encoding

(Not the same as encrypting)

Solution	Works...
Write it down!	✗ Unless the emperor can read
Write it down in French	✗ Unless the emperor speaks French
Write it down in Navaho	✗ Unless the emperor speaks Navaho
Use Morse code	✗ Unless the emperor knows Morse
Base64-encode it	✗ Unless the emperor has an email client!

Risk: Anybody can learn these systems!

Once the system is known, the message is exposed.

Assume your adversary can know anything that is public

Steganography (hiding that there are messages)

Solution

Invisible ink
Secret tattoos
Ninja delivery service
{Extremely complex and original delivery system}

Risk: *Somebody could* learn these systems!

Once the system is known, the message is exposed.

Assume your adversary knows how you send messages

One-way functions (neither a cipher nor a solution!)

“Solution”

e.g., *N*th letter of *nth* word scheme.

Kill the Emperor → **Khp**

Kill the Emperor

Khp?

Khp?
er...
Kiss the cupboard?
Kill showoff captain?

One-way functions (neither a cipher nor a solution!)

“Solution”

Good: Not enough information in message for the adversary to reconstruct the original, even <u>knowing the system.</u>

Bad: No way for the recipient to reconstruct the message!

Khp?
er...
Kiss the cupboard?
Kill showoff captain?

Solutions (that aren’t cryptography)

1. Encoding

Assume your adversary can know anything that is public

2. Steganography

Assume your adversary knows how you send messages

3. One-way functions

Recipient needs to be able to understand the message

Cryptographic solution

Shared Secret

k

Brutus

General

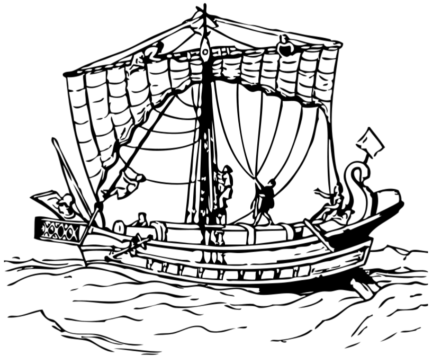
?

?

The emperor

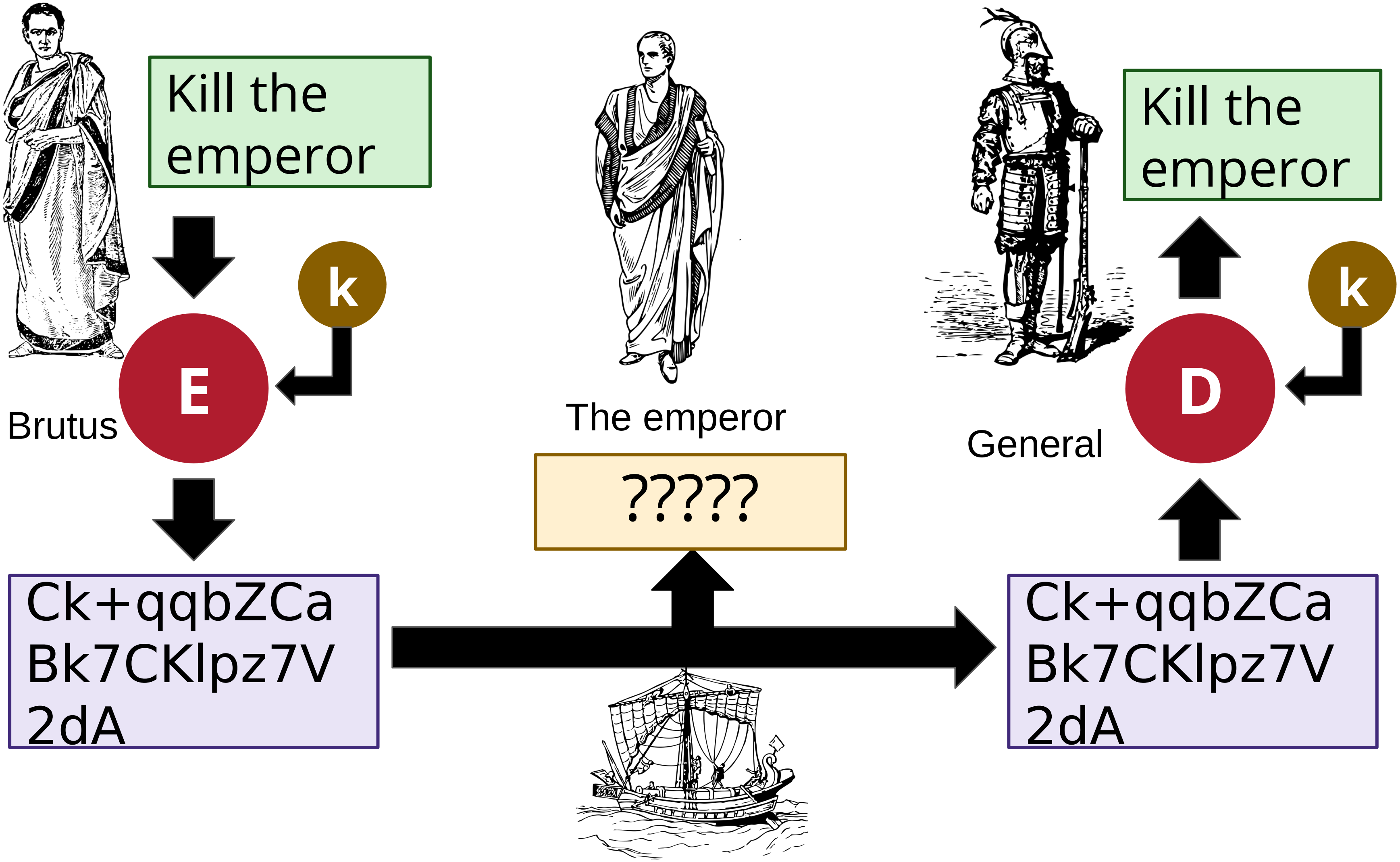
?

?



The messenger

Cryptographic solution



Brutus

Kill the emperor

k

E

Ck+qqbZCa
Bk7CKlpz7V
2dA

The emperor

?????

General

Kill the emperor

k

D

Ck+qqbZCa
Bk7CKlpz7V
2dA

Kerchoffs’ principle

Assume that the enemy knows all about your *system*.

Security must rest solely on secrecy of the *keys*.

Historical ciphers

Caesar’s cipher

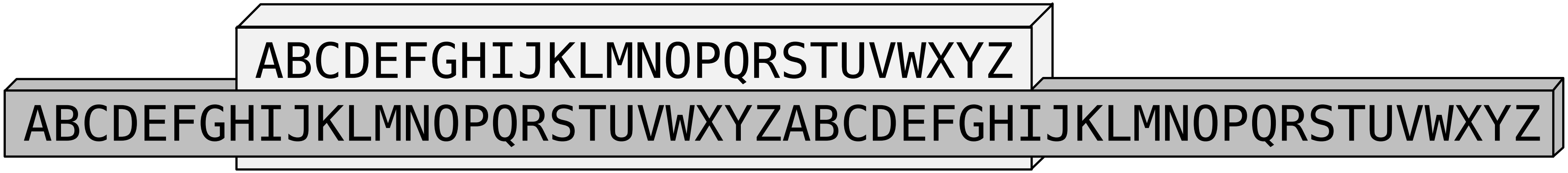
Caesar’s cipher

system: increment/decrement each letter of ***message*** by ***key*** places (wrapping around the alphabet)

a = 0, b = 1 … z = 25

message + key (mod 26)

addition is **modulo 26**, i.e. it wraps around:



ABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

cipher disks

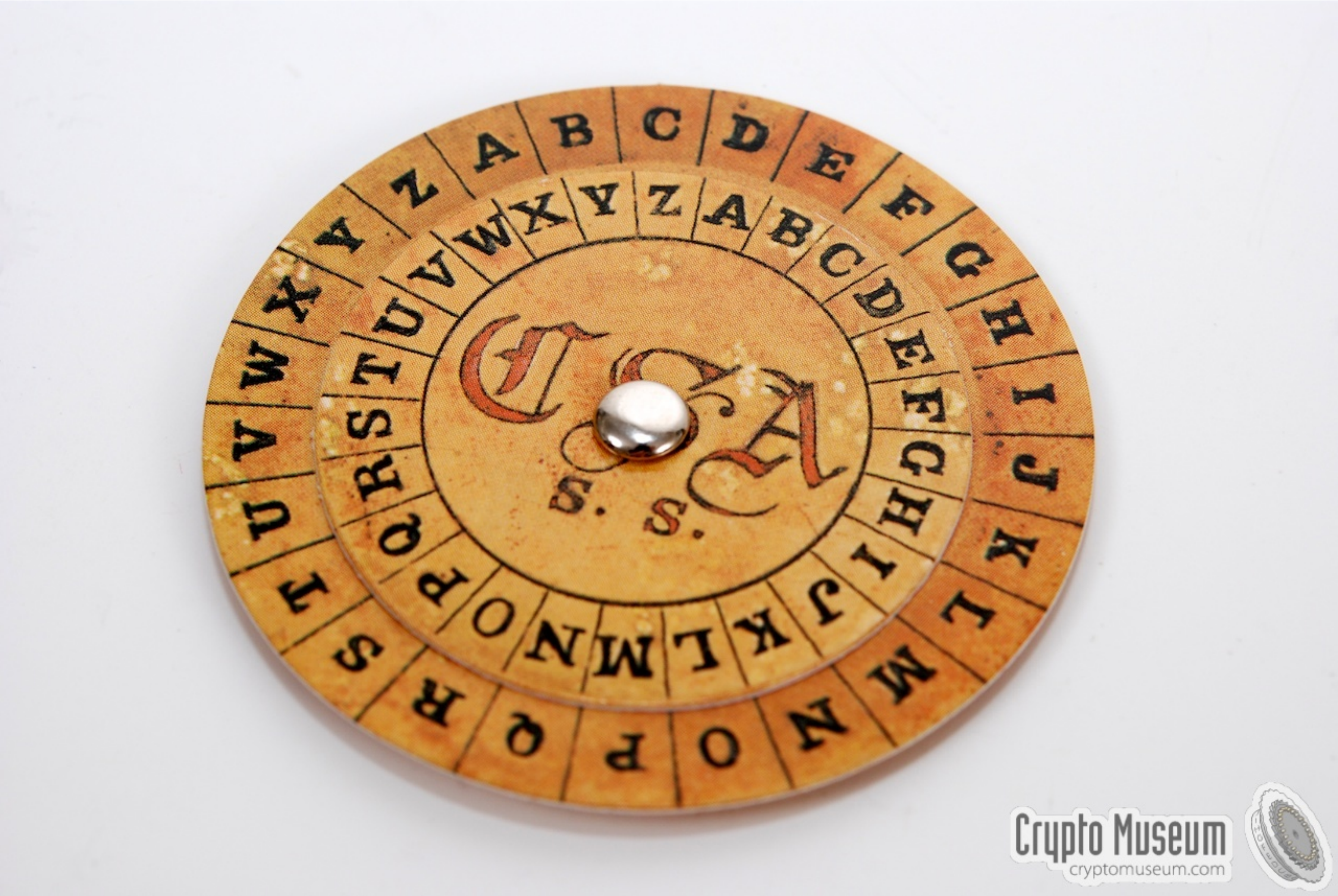


image: cryptomuseum.com

Caesar’s cipher

system:

ciphertext = message + key (mod 26)
message = ciphertext – key (mod 26)

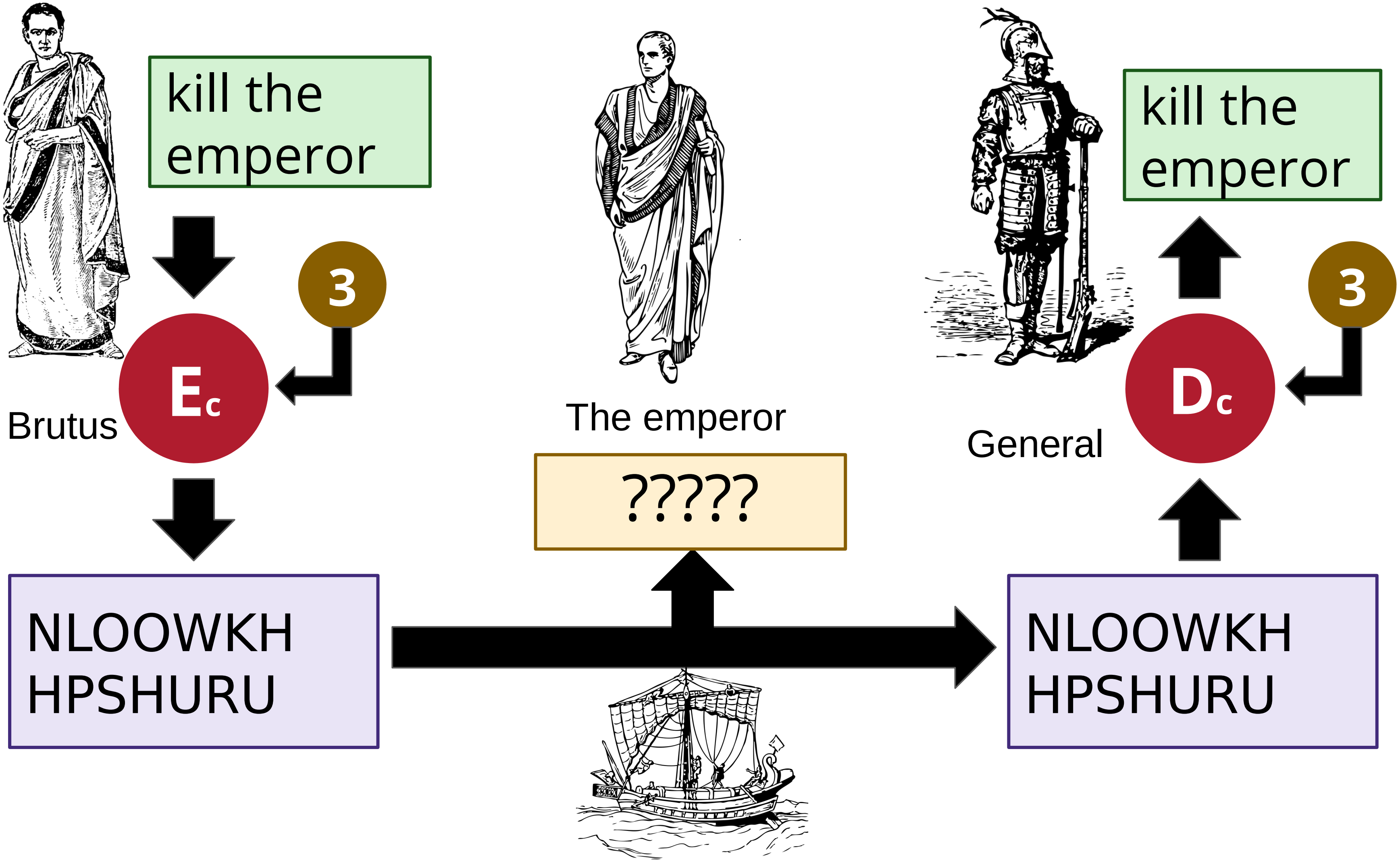
key: 3

message: `attack at dawn`

ciphertext: `DWWDFN DW GDZQ`

(Convention for examples:
plaintext is lower-case,
ciphertext is upper-case)

Caesar’s cipher



kill the emperor

3

E_c

Brutus

NLOOWKH HPSHURU

The emperor

?????

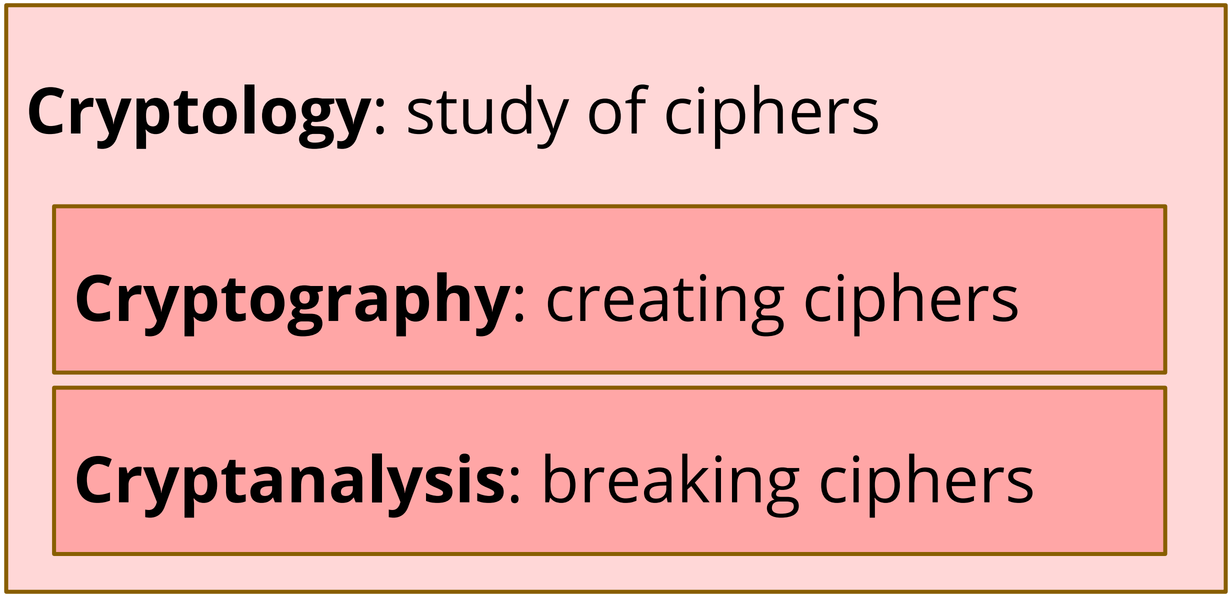
General

D_c

3

kill the emperor

NLOOWKH HPSHURU



Cryptology: study of ciphers

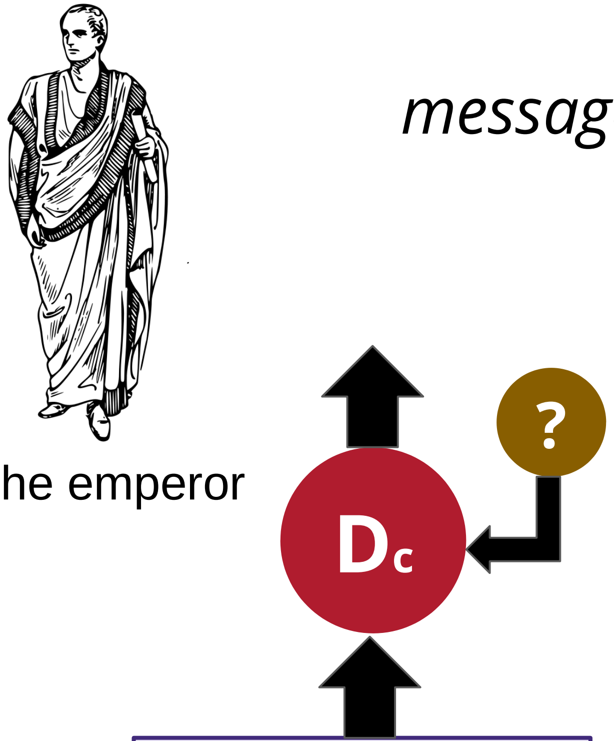
Cryptography: creating ciphers

Cryptanalysis: breaking ciphers

Caesar's cipher: cryptanalysis

Kerchoffs' principle

message = ciphertext – key (mod 26)



NLOOWKH
HPSHURU

What possible values could **k** take?

Caesar’s cipher: cryptanalysis

The emperor

Only **26** possible keys… very simple for a **brute force** attack: try all possibilities.

cipher: NLOOWKHHPSHURU

-1:mknnvjggorgtqt

-2:ljmmuiffnqfsps

-3:killtheemperor

-4:jhkksgddlodqnq

A good cipher needs a large number of possible keys

Historical ciphers

Monoalphabetic ciphers

Monoalphabetic cipher

Caesar-rotating: 26 possibilities

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
```

Random shuffle: 26! possibilities

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
VAHDBLKGZRYSQUFNXJWOPCMITE
```

26! = 403291461126605650322784256

Monoalphabetic cipher

OYR KMJEFRG VAOY NAGKFR CAKYRMN AN OYSO OYRX UJ HJO YAUR KSOORMHN AH OYR GRNNSTR: AO AN RSNX OJ NRR NYJMO VJMUN, MRKROAOAJH JI FROORMN SHU GSHX JOYRM IRSOPMRN.

S TJJU CAKYRM GPNO YAUR SFF KSOORMHN AH OYR GRNNSTR NJ OYSO FJJDAHT SO OYR CAKYRMORWO UJRN HJO TAQR XJP SHX PNRIPF AHIJMGSOAJH SEJPO OYR GRNNSTR, RWCRKO KRMYSKN AON FRHTOY.

Short words in English

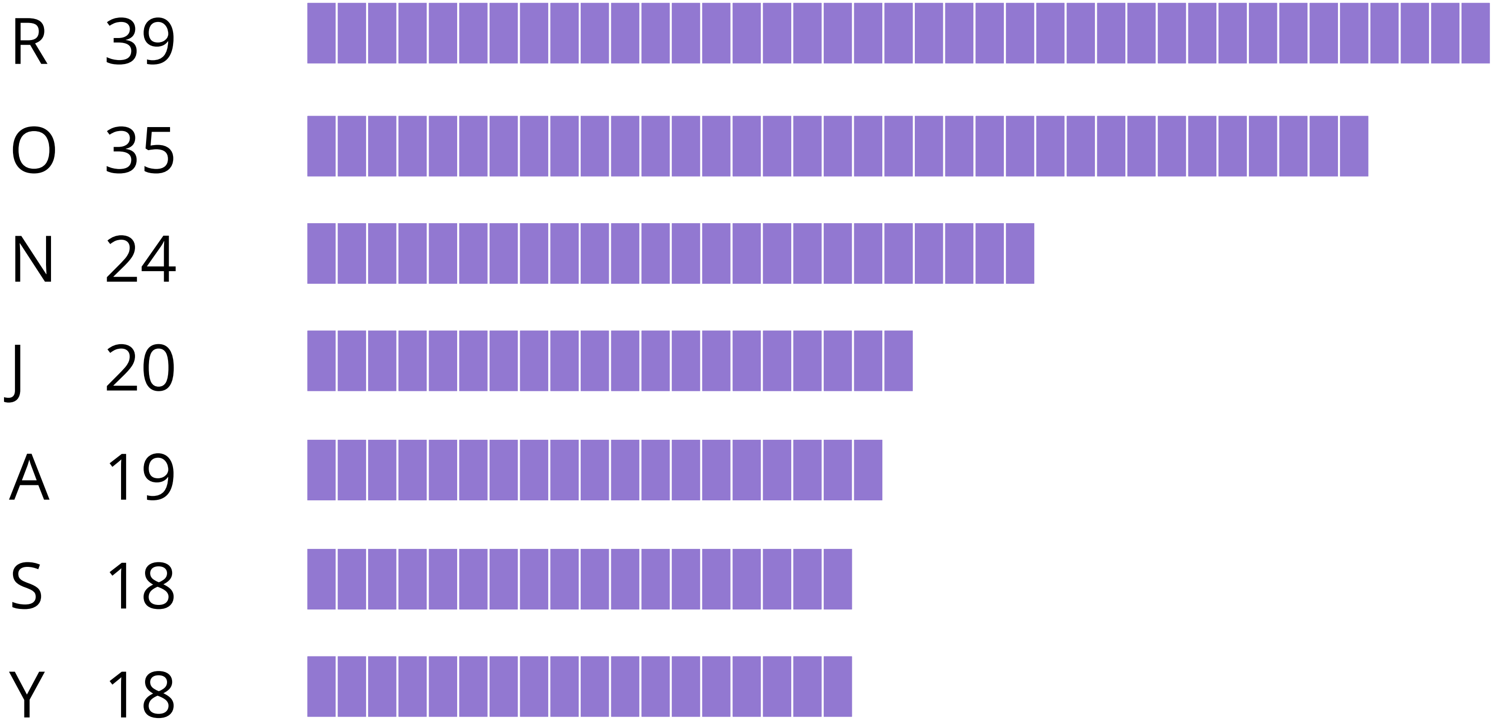
a, I, (O)

of, to, in, it, is, be, as, at, so, we, he, by, or, on, do, if, me, my, up, an, go, no, us, am

a_ => am, an, as, at; o_ => of, or, on, (oh); i_ => in, it, is, if
_o => to, do, no, go, so; _s => is, as, us; _n => in, on, an,
_e => be, we, he, me

the, and, for, are, but, not, you, all, any, can, had, her, was, one, our, out, day, get, has, him, his, how, man, new, now, old, see, two, way, who, boy, did, its, let, put, say, she, too, use

Letter frequencies



Most common in English: ETAOIN SHRDLU

Solution

the problem with simple ciphers is that they do not hide patterns in the message: it is easy to see short words, repetition of letters and many other features.

a good cipher must hide all patterns in the message so that looking at the ciphertext does not give you any useful information about the message, except perhaps its length.

Monoalphabetic cipher

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
SECURITYABDFGHJKLMNOPQVWXZ
```

Obviously not secure by today’s standards - we’ve just broken it!

A good cipher needs a large number of possible keys

A good cipher also needs to hide patterns in the message

Historical ciphers

Vignère cipher

Vigenère: a *poly*alphabetic cipher

Perhaps we can encrypt different letters with different keys …

Pick a secret word or phrase … for example **SECRET**.

```
message:   DEAR MR. AGENT ...
key:       SECR ET  SECRE ...
```

The alphabet square

```
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
A ABCDEFGHIJKLMNOPQRSTUVWXYZ
B BCDEFGHIJKLMNOPQRSTUVWXYZA
C CDEFGHIJKLMNOPQRSTUVWXYZAB
D DEFGHIJKLMNOPQRSTUVWXYZABC
E EFGHIJKLMNOPQRSTUVWXYZABCD
F FGHIJKLMNOPQRSTUVWXYZABCDE
G GHIJKLMNOPQRSTUVWXYZABCDEF
  ...
```

The alphabet square

	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

...

Encrypting D with key letter S: D + S = V

Vigenère: a polyalphabetic cipher

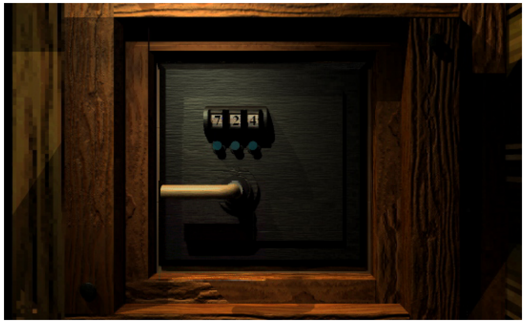
```
message:    DEAR MR. AGENT ...
 +  key:    SECR ET. SECRE ...
-------------------------------
sum:        VICI QK. SKGEX ...


cipher:     VICIQKSKGEX…
```

Cryptanalysis: your lab exercise!

bits of security

Bits of security



A safe with an n-digit code:

- You (the owner) need to remember $D = n$ digits.
- A burglar has to try $B = 10^n$ combinations.

A cryptographic system with ***n* bits of security**:

you need some "efficient" function of n steps/time to operate it (e.g. n^2).

to break the system takes 2^n steps/time.

n *bits of security* = breaking the system takes $\mathbf{2^n}$ steps.

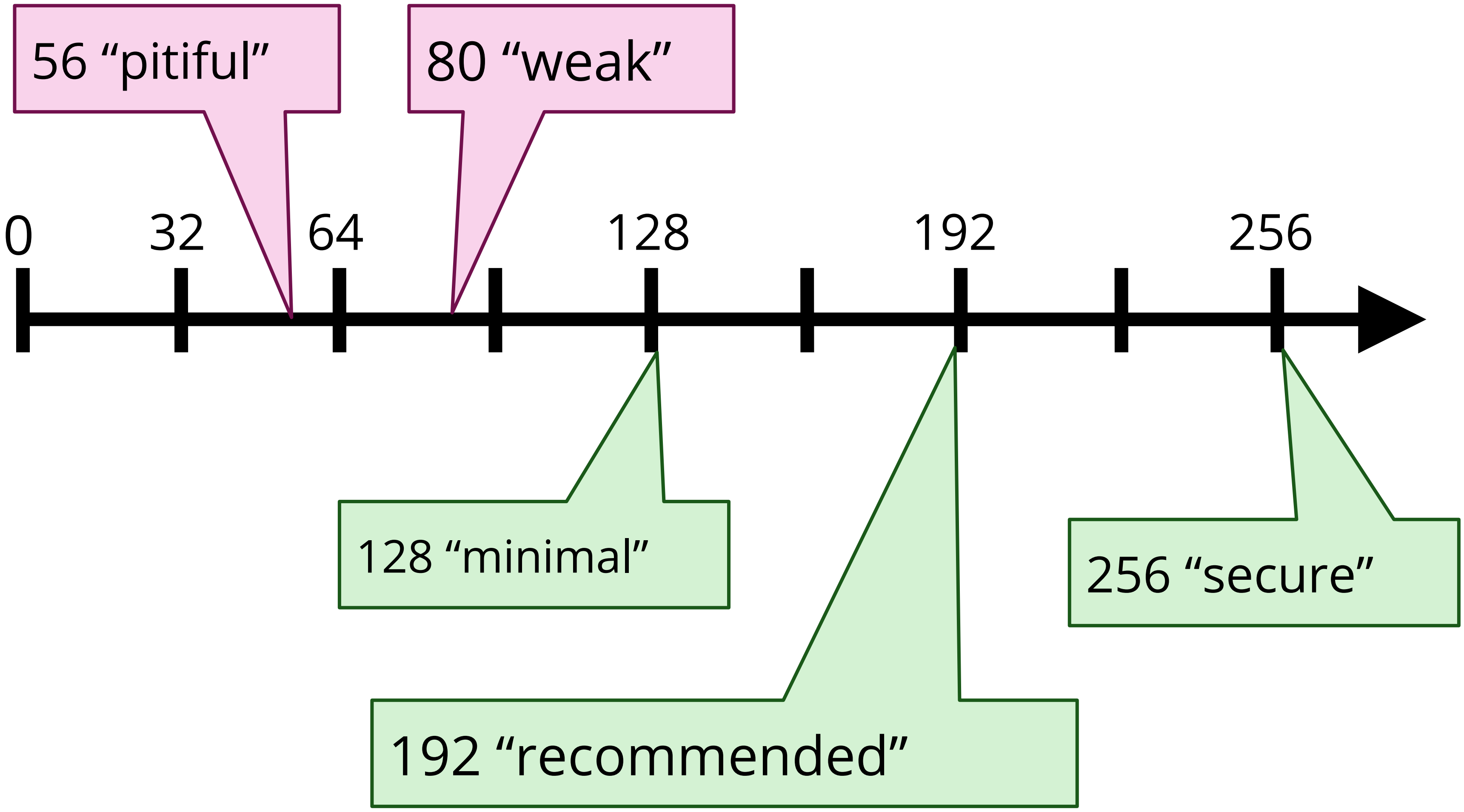
$$\log_2(26!) = 88.38 = 89$$

Nowadays 128 bits is the minimum requirement.

Key length is not the same thing as security level!

80 bits of key are usually *less* than 80 bits of security.

Security recommendations



56 “pitiful”

80 “weak”

128 “minimal”

192 “recommended”

256 “secure”

Cryptography and mathematics

Modern cryptography is based on (fairly) advanced mathematics - CS students can take Crypto A/B (COMS30002, COMSM00007) to find out more.

Any cipher not designed according to the latest mathematical principles is generally easy to break using the lastest mathematical principles -

Never try and create your own crypto until you have at least a PhD in the subject!