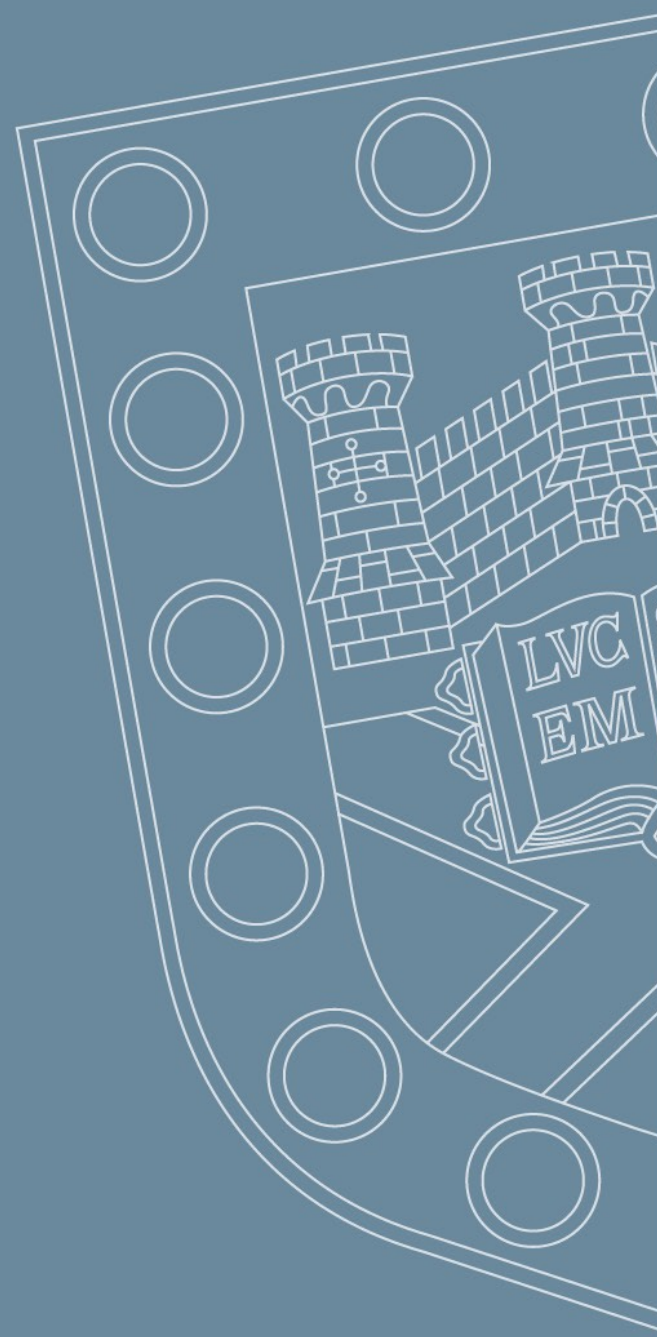
UNIVERSITY OF EXETER

The Information Age

ECM1407: Social and Professional Issues of the Information Age

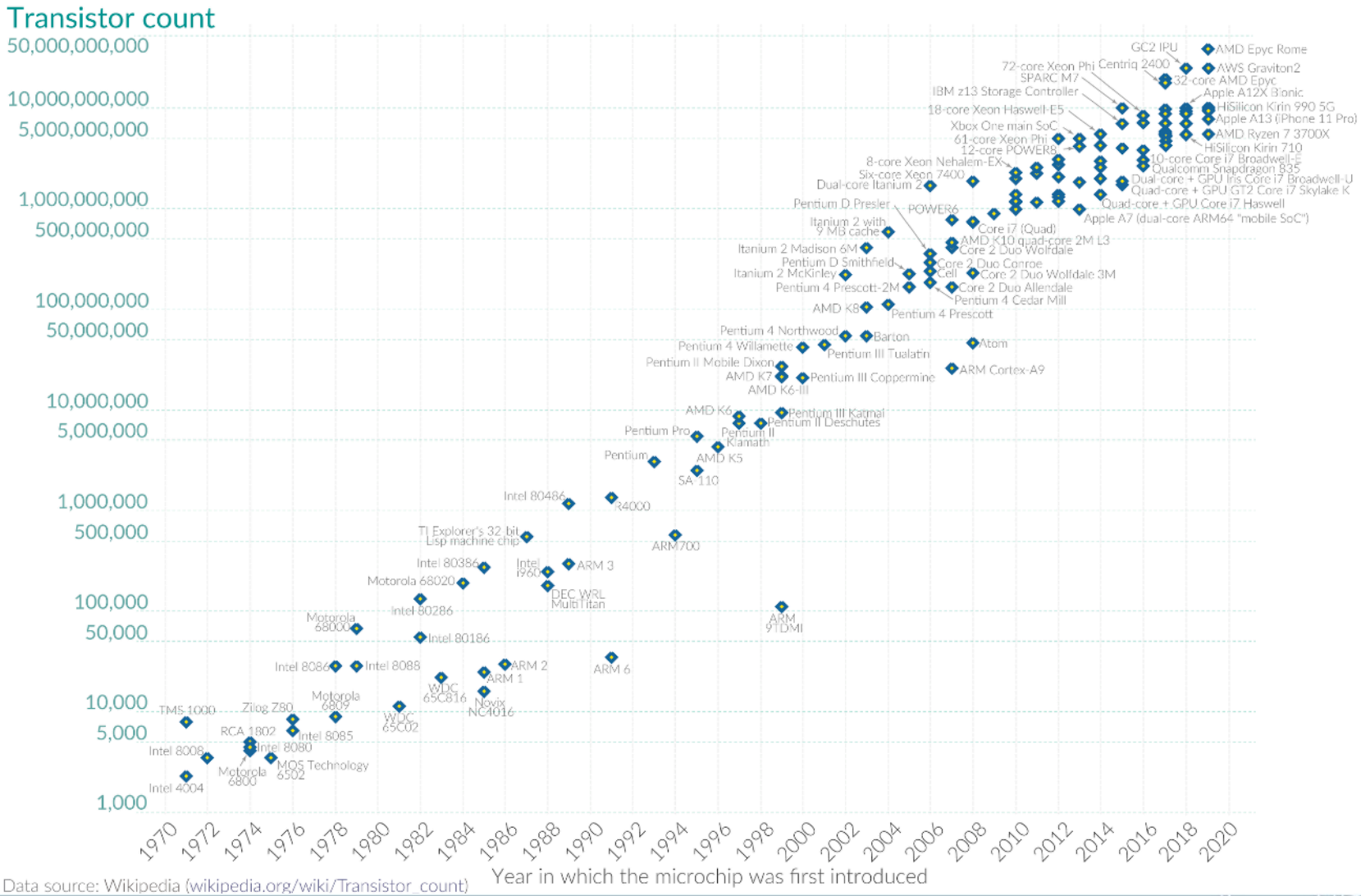
Marcos Oliveira



Moore's Law: The number of transistors on microchips doubles every two years

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important for other aspects of technological progress in computing – such as processing speed or the price of computers.

Our World in Data



Data source: Wikipedia (wikipedia.org/wiki/Transistor_count)

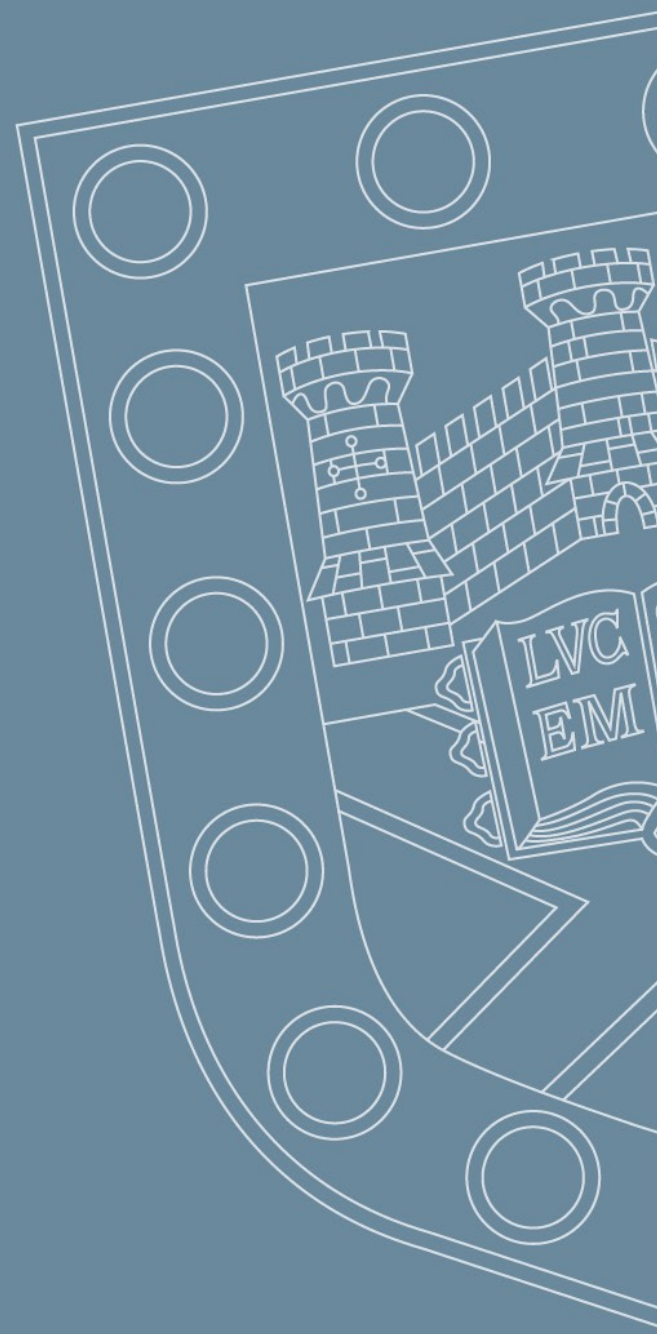
https://en.wikipedia.org/wiki/Moore's_law

UNIVERSITY OF EXETER

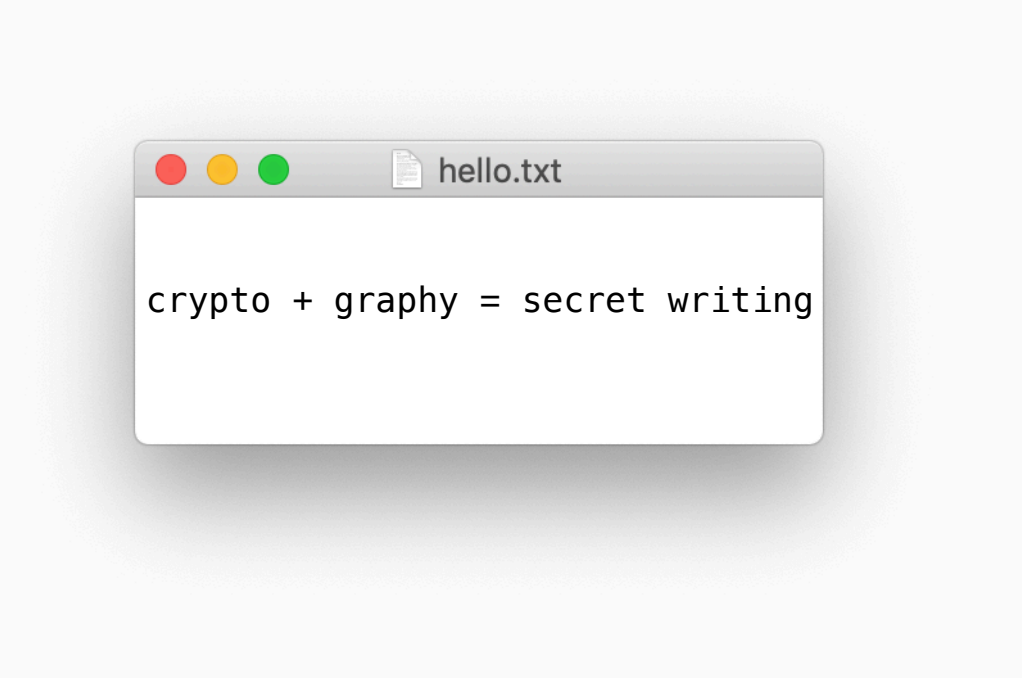
Cryptography and Society

ECM1407: Social and Professional Issues of the Information Age

Marcos Oliveira

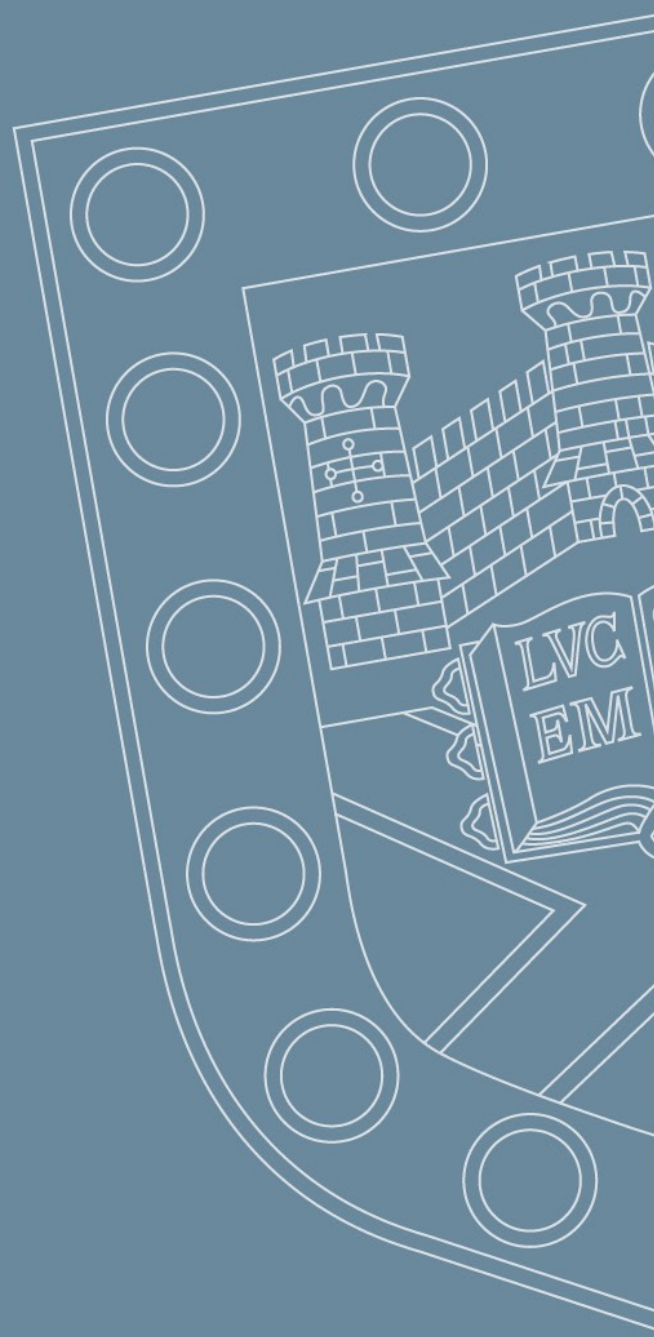


Cryptography and Society



Modern cryptography: The study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks.

UNIVERSITY OF EXETER



Week 3: Cryptography and Society

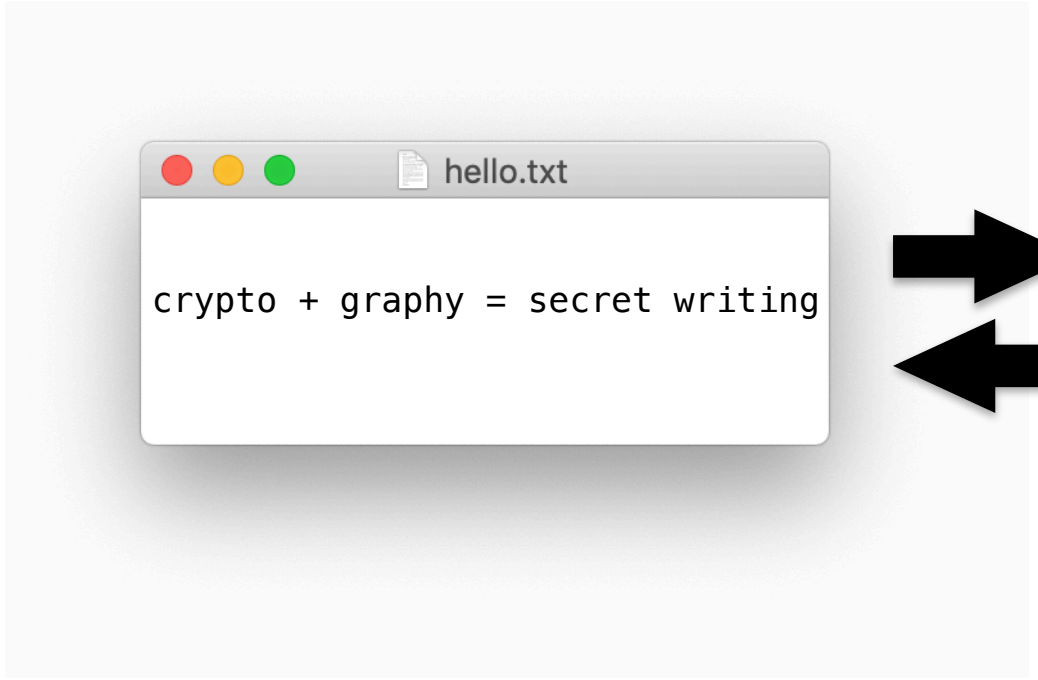
Cryptography

ECM1407: Social and Professional Issues of the Information Age

Marcos Oliveira

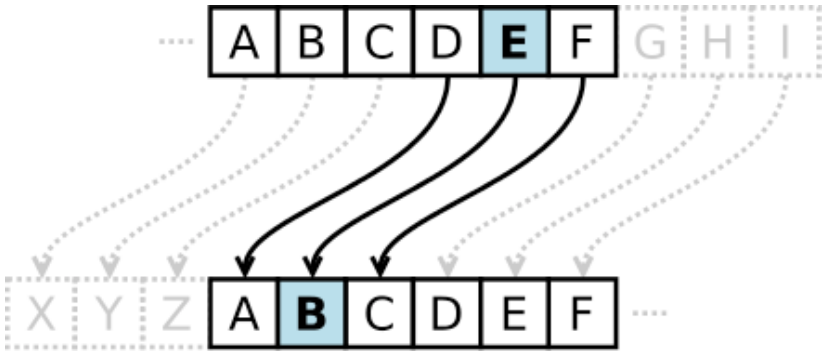
Cryptography

- Encryption / decryption.

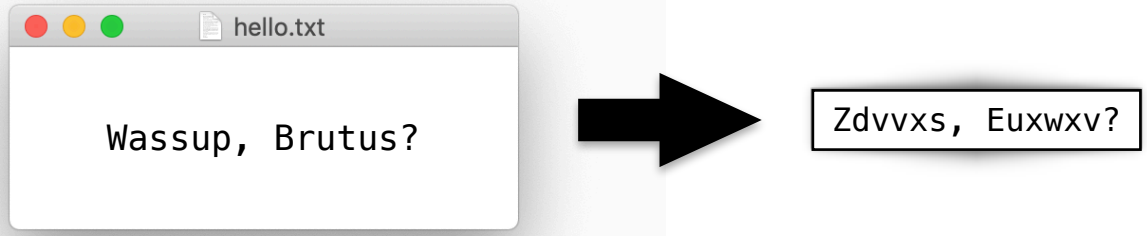


Cryptography

- Caesar's cipher: one of the oldest recorded ciphers.



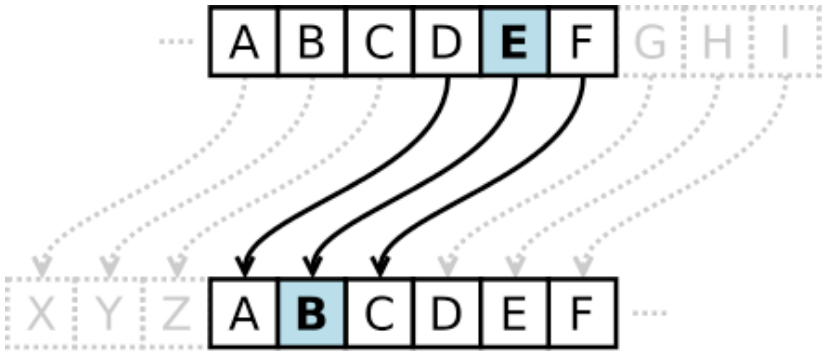
It shifts letters 3 places forward.



Katz, J., Lindell, Y. (2020). Introduction to Modern Cryptography. United Kingdom: Taylor & Francis Group.
Available online: http://www.cs.umd.edu/~jkatz/imc.html

Cryptography

- Shift cipher with key **k**



`Qummoj, Vlonom?`

It shifts letters **k** places forward.

Katz, J., Lindell, Y. (2020). Introduction to Modern Cryptography. United Kingdom: Taylor & Francis Group.
Available online: http://www.cs.umd.edu/~jkatz/imc.html

Cryptography

- The mono-alphabetic substitution cipher
  - It defines a map from each letter to some letter of the alphabet, where the map is arbitrary, instead of a fixed shift.

Plain alphabet	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution alphabet	NBAJYFOWLZMPXIKUVCDEGRQSTH

```
Lg Sgfu, afr Miafql ygk Ass mit Yoli!
```

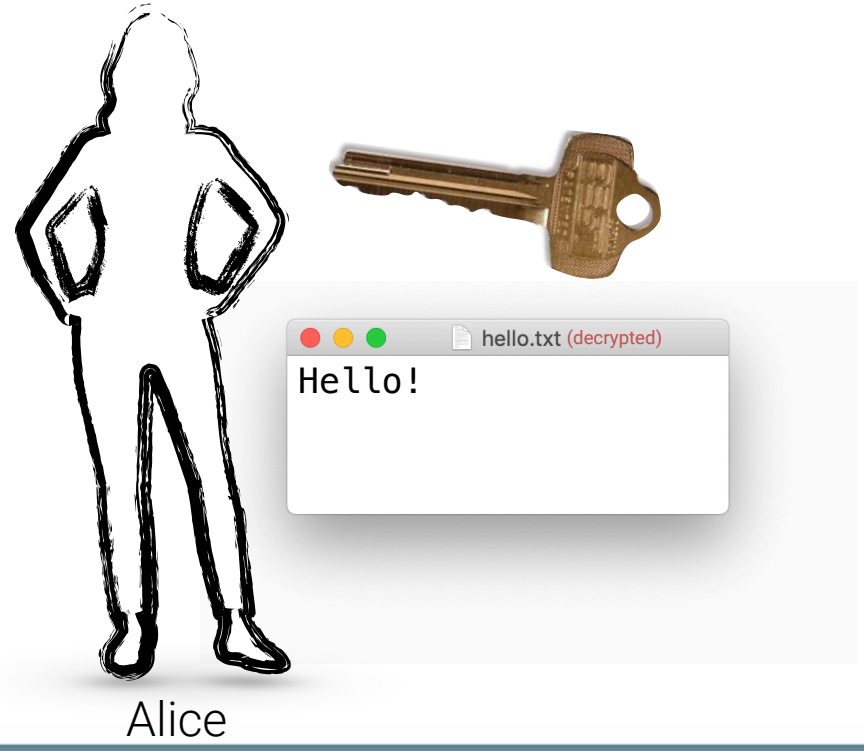
The size of the key space is **$26! \approx 2^{88}$**

Katz, J., Lindell, Y. (2020). Introduction to Modern Cryptography. United Kingdom: Taylor & Francis Group.
Available online: http://www.cs.umd.edu/~jkatz/imc.html

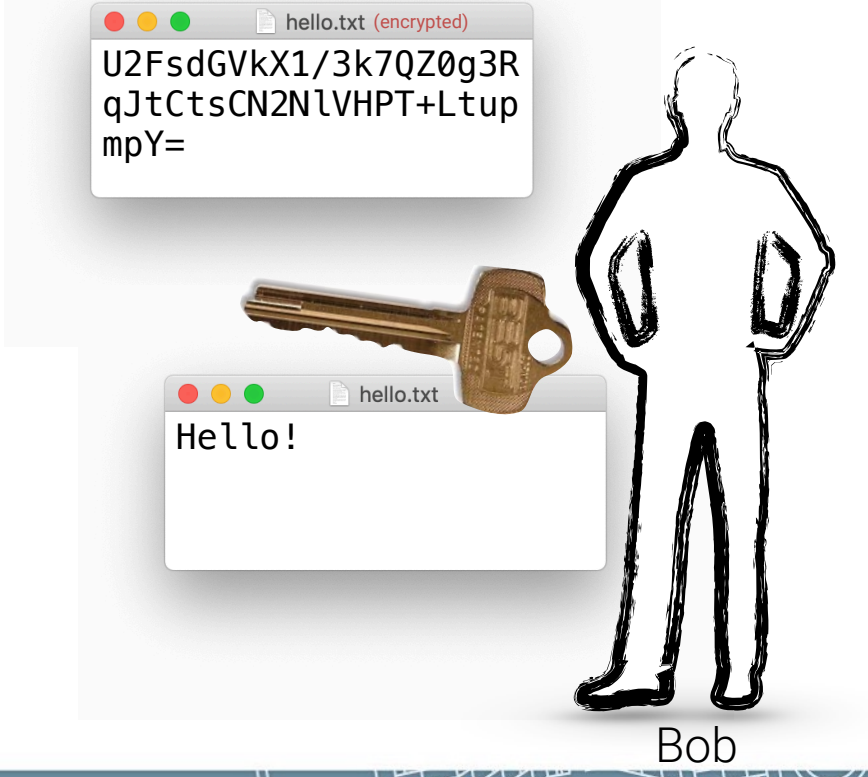
Cryptography

- Symmetric
- Asymmetric

Symmetric Cryptography



Alice

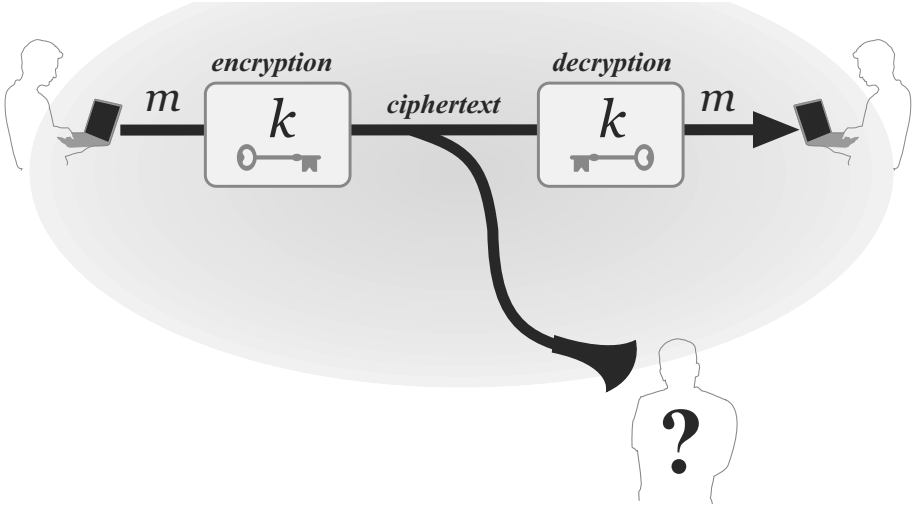


Bob

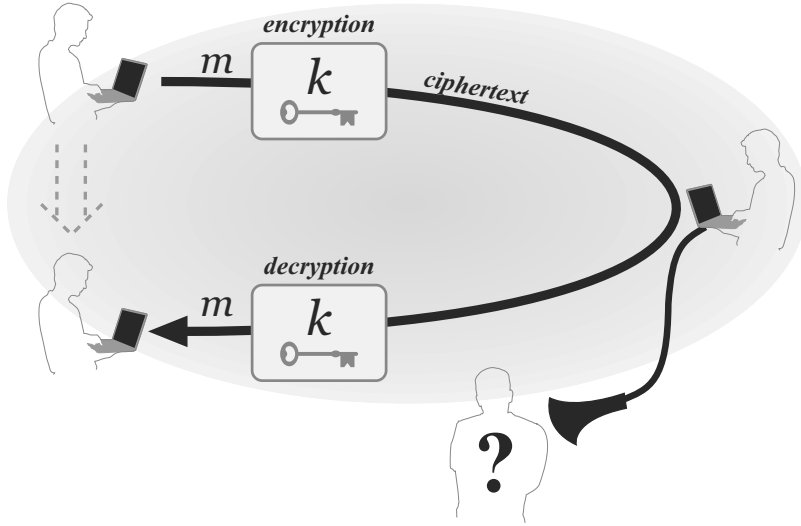
Symmetric Cryptography

- Private-key encryption/decryption: both parties share a key.

- Common use:



Space

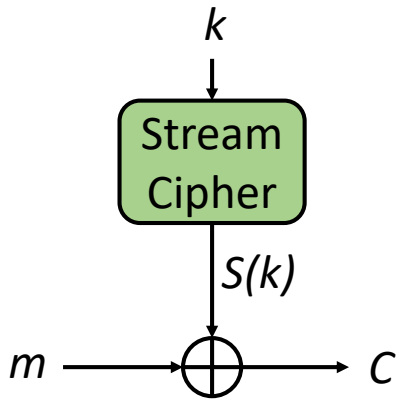


Time

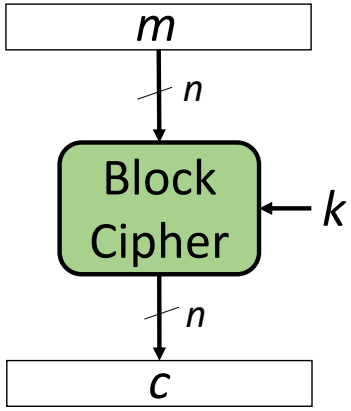
Katz, J., Lindell, Y. (2020). Introduction to Modern Cryptography. United Kingdom: Taylor & Francis Group.
Available online: http://www.cs.umd.edu/~jkatz/imc.html

Symmetric cryptography

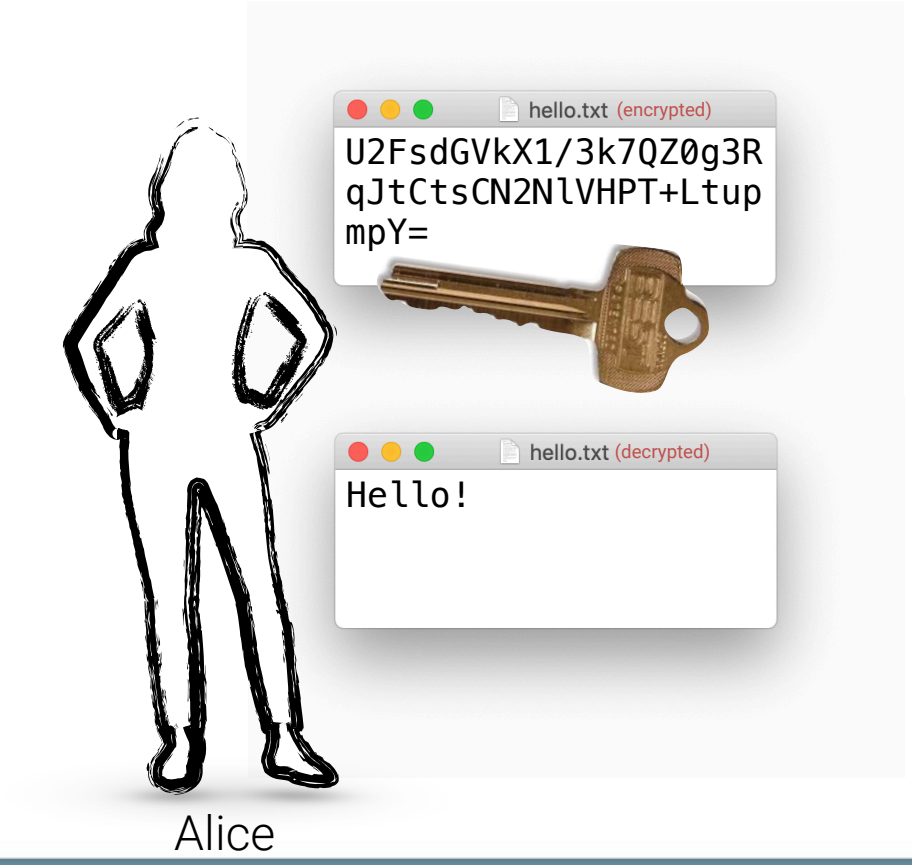
- Stream cipher



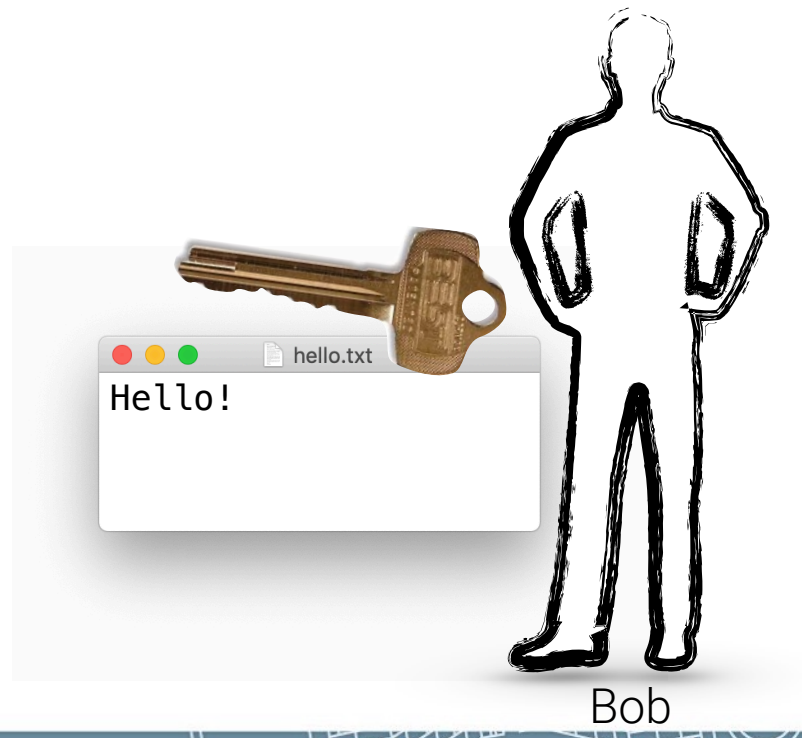
- Block cipher



Symmetric Cryptography



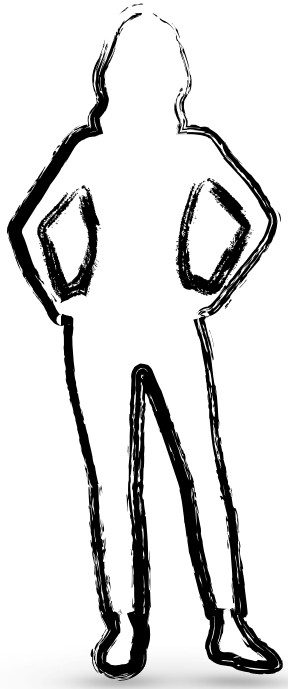
Alice



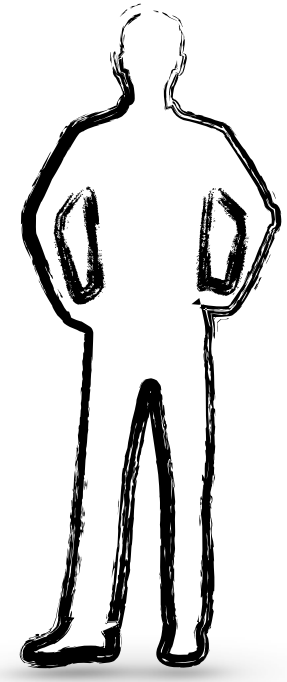
Bob

Symmetric Cryptography

- The key distribution problem.



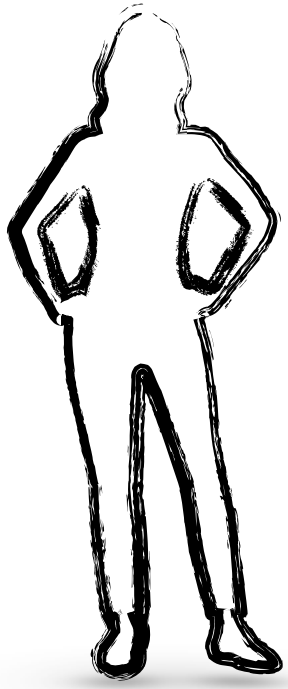
Alice



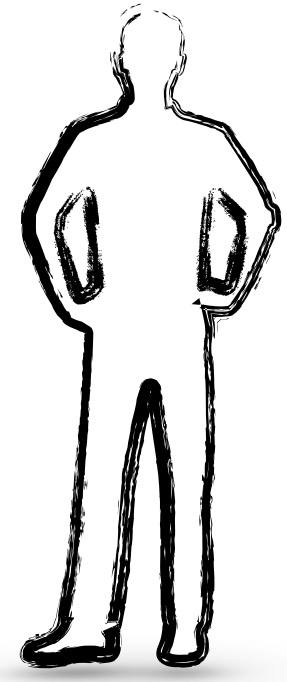
Bob

Symmetric Cryptography

- The key distribution problem.



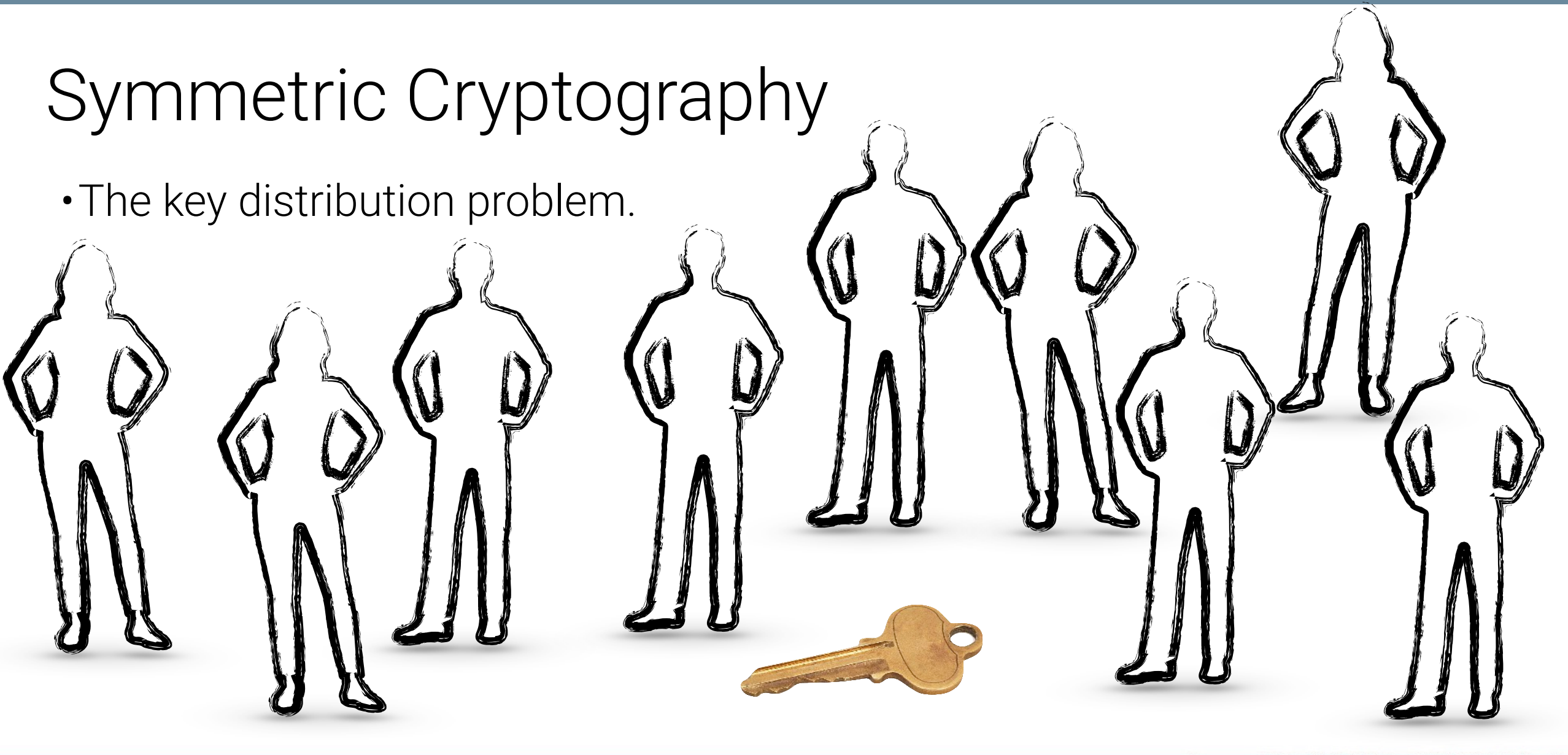
Alice



Bob

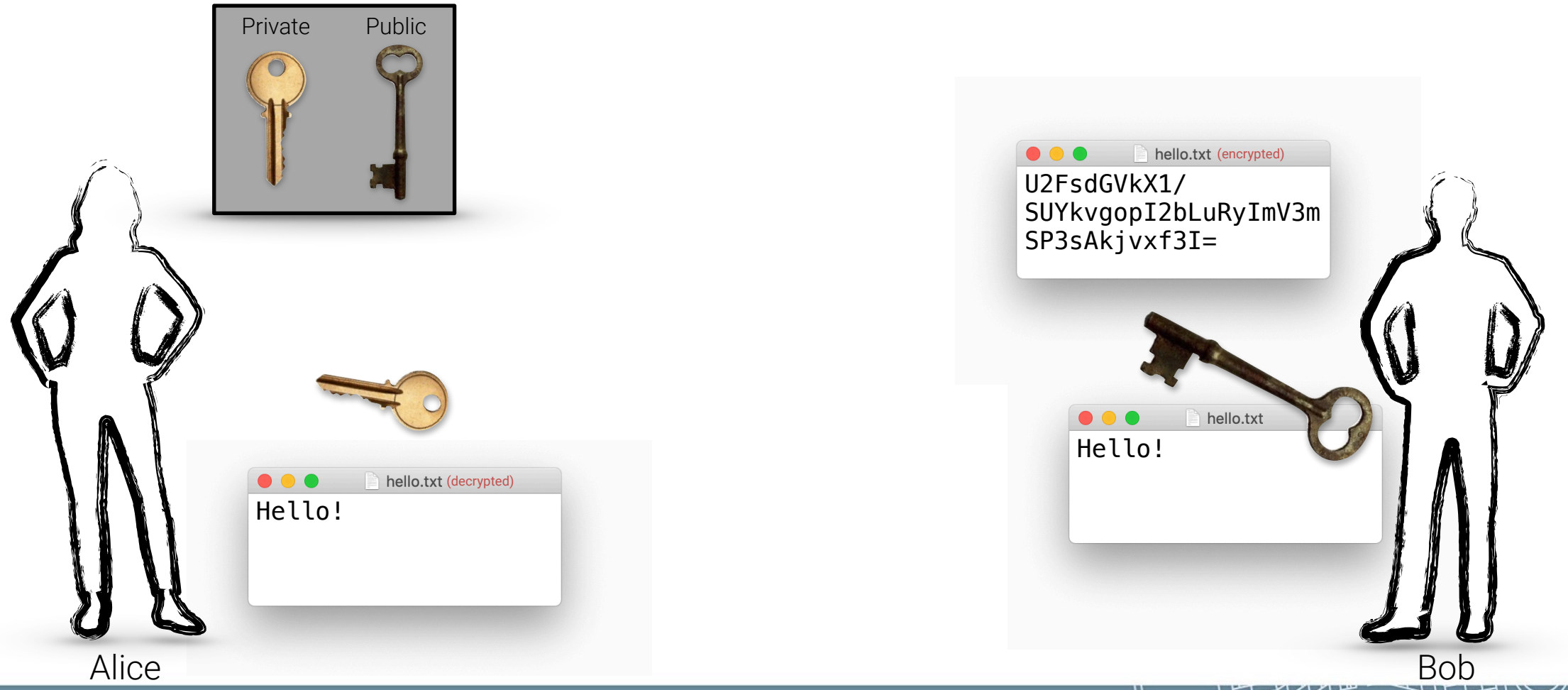
Symmetric Cryptography

- The key distribution problem.



Asymmetric Cryptography

Asymmetric Cryptography



Asymmetric Cryptography: RSA

Private	Public
(d, n)	(e, n)

1. Choose two large prime numbers p and q
2. Calculate $n = p \times q$
3. Calculate $z = (p - 1) \times (q - 1)$
4. Choose e to be relatively prime to z
5. Choose d such that $d \times e \mod z = 1$

Asymmetric Cryptography: RSA

Private	Public
(d, n)	(e, n)

1. Choose two large prime numbers p and q
2. Calculate $n = p \times q$
3. Calculate $z = (p - 1) \times (q - 1)$
4. Choose e to be relatively prime to z
5. Choose d such that $d \times e \mod z = 1$

Encrypted block

$$C = M^e \mod n$$

Encryption

$$M$$

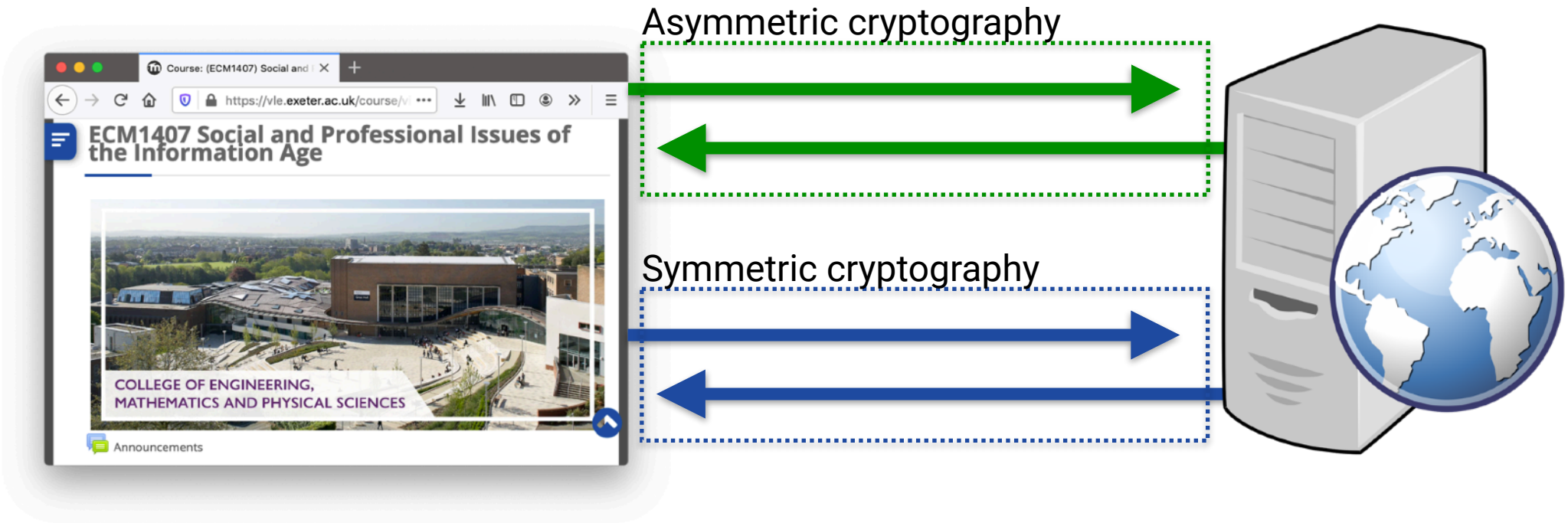
Plaintext block

$$M = C^d \mod n$$

Decryption

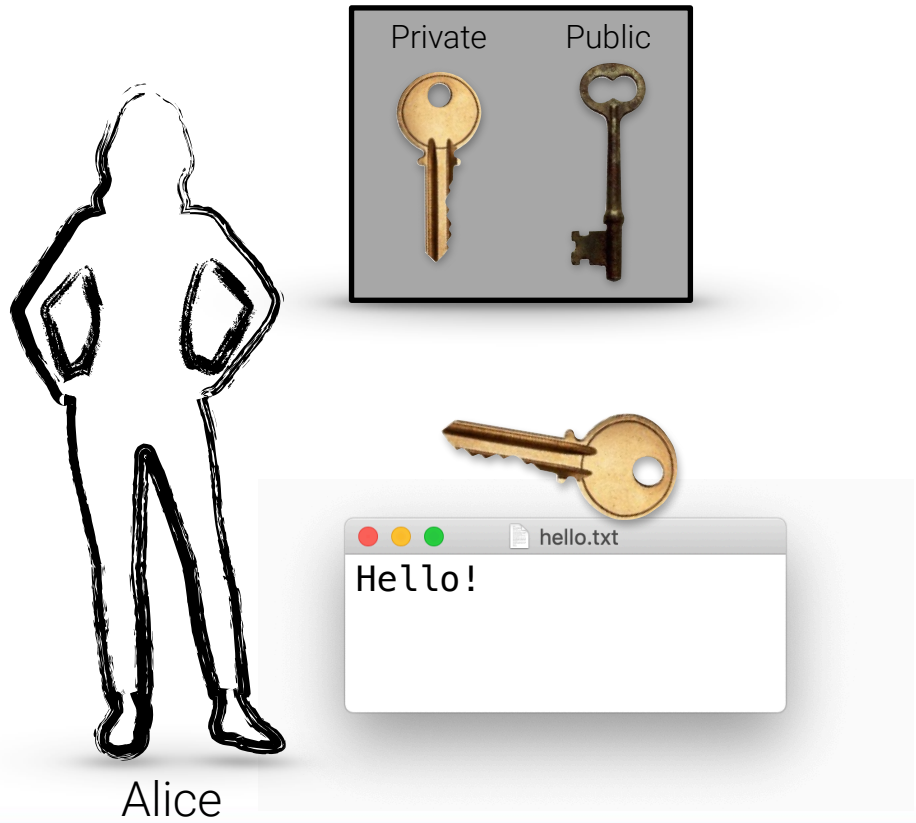
Asymmetric Cryptography

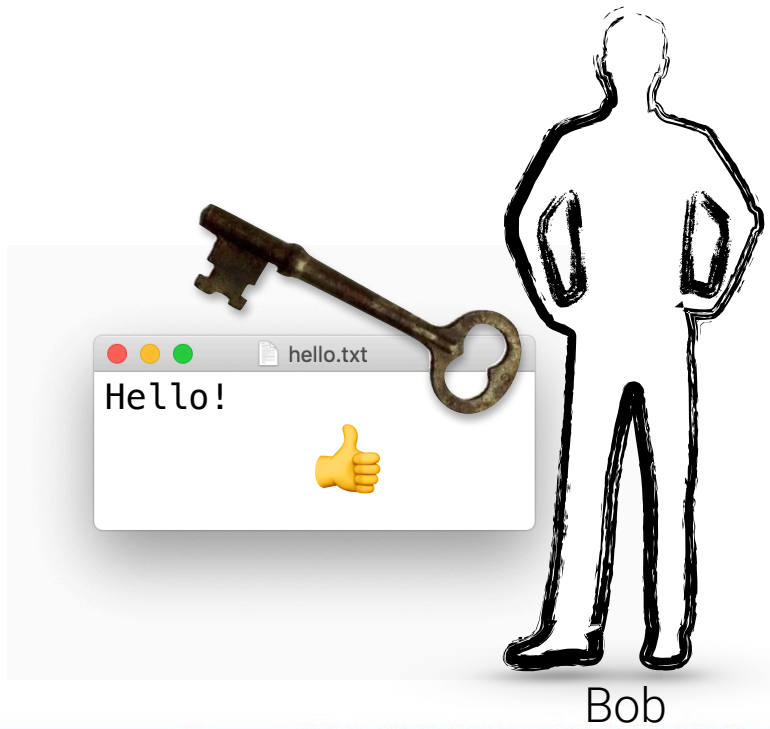
- It solves the key distribution problem. For example:



Digital signature

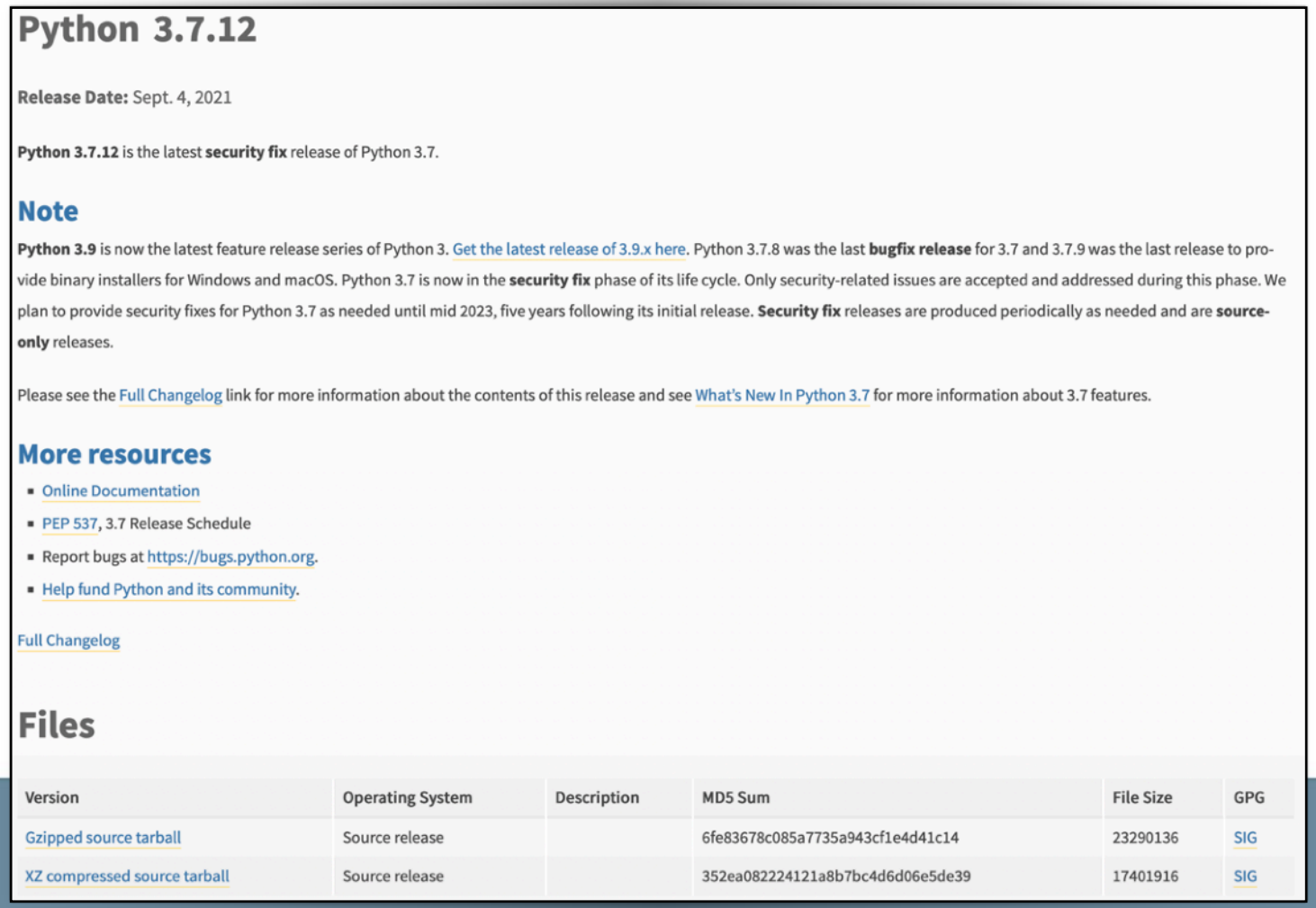
- Authentication, integrity, and accountability (non-repudiation):





Digital signature

- Integrity; similarly, with a hash function:



Python 3.7.12

Release Date: Sept. 4, 2021

Python 3.7.12 is the latest **security fix** release of Python 3.7.

Note

Python 3.9 is now the latest feature release series of Python 3. Get the latest release of 3.9.x here. Python 3.7.8 was the last **bugfix release** for 3.7 and 3.7.9 was the last release to provide binary installers for Windows and macOS. Python 3.7 is now in the **security fix** phase of its life cycle. Only security-related issues are accepted and addressed during this phase. We plan to provide security fixes for Python 3.7 as needed until mid 2023, five years following its initial release. **Security fix** releases are produced periodically as needed and are **source-only** releases.

Please see the Full Changelog link for more information about the contents of this release and see What's New In Python 3.7 for more information about 3.7 features.

More resources

- Online Documentation
- PEP 537, 3.7 Release Schedule
- Report bugs at https://bugs.python.org.
- Help fund Python and its community.

Full Changelog

Files

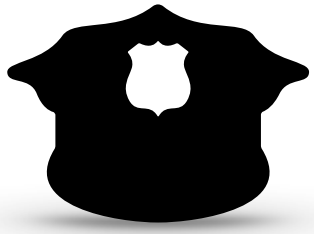
Version	Operating System	Description	MD5 Sum	File Size	GPG
Gzipped source tarball	Source release		6fe83678c085a7735a943cf1e4d41c14	23290136	SIG
XZ compressed source tarball	Source release		352ea082224121a8b7bc4d6d06e5de39	17401916	SIG

```
marcos@mac ~ % wget python.org/ftp/python/3.7.12/Python-3.7.12.tgz
marcos@mac ~ % md5 Python-3.7.12.tgz
MD5 (Python-3.7.12.tgz) = 6fe83678c085a7735a943cf1e4d41c14
```

https://www.python.org/downloads/release/python-3712/

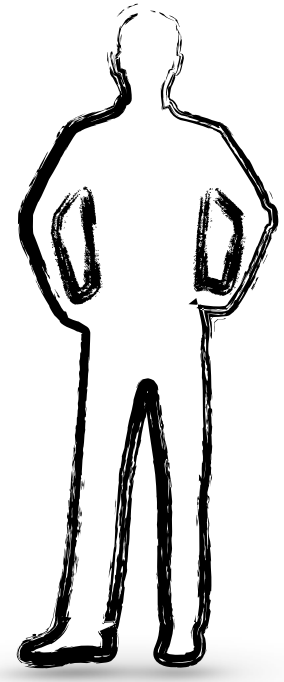
Digital certificate

- A certificate authority can issue a digital certificate to prove the ownership of a public key.



Certificate Authority

Alice



Bob

How to break it?

- Cryptography relies on the lack of an efficient factorization algorithm.

- Quantum computing
  - Shor's algorithm: polynomial-time quantum computer algorithm for integer factorization.

Encrypted block

$$C = M^e \mod n$$

Encryption

$$M = C^d \mod n$$

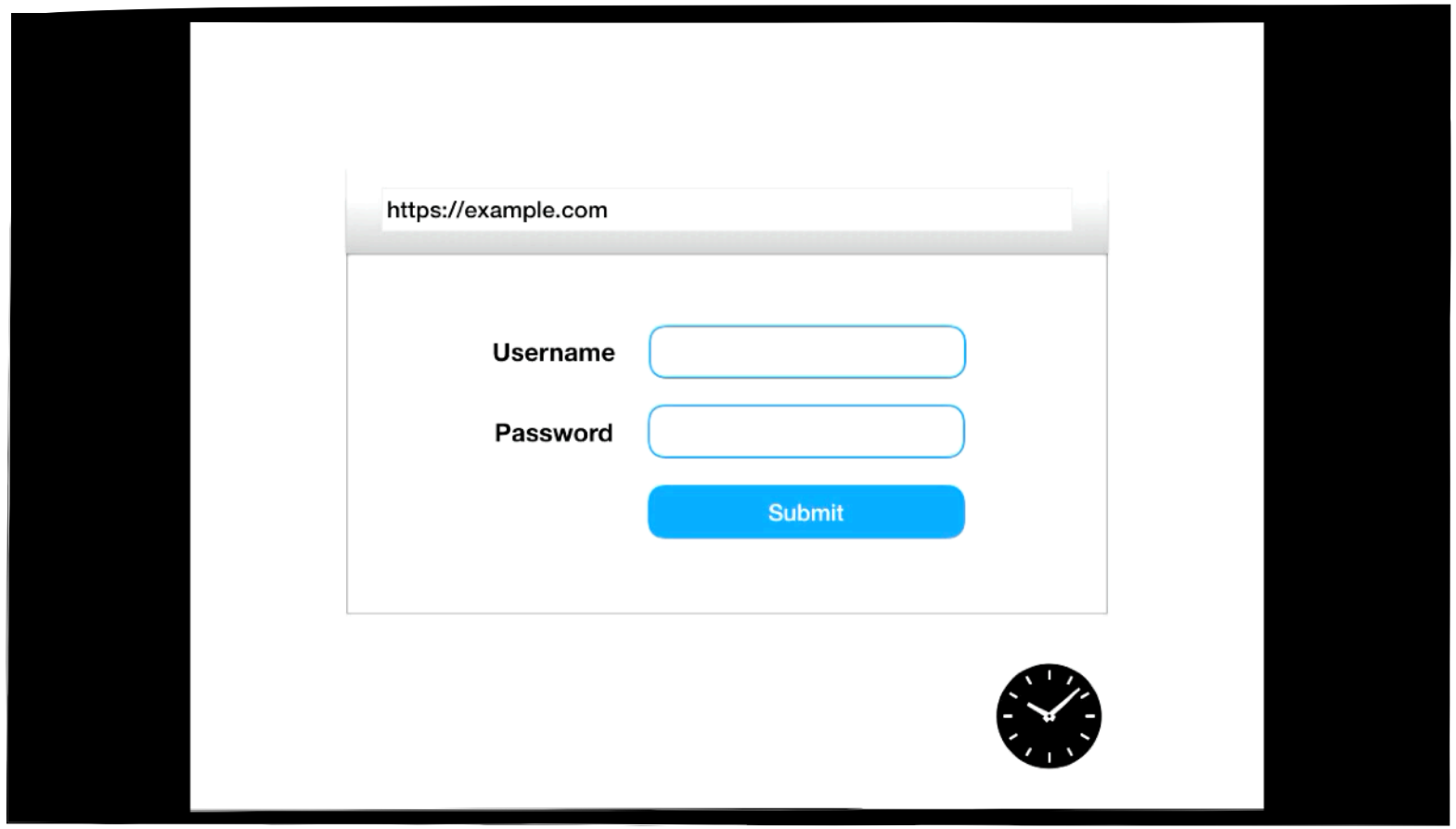
Decryption

$$M$$

Plaintext block

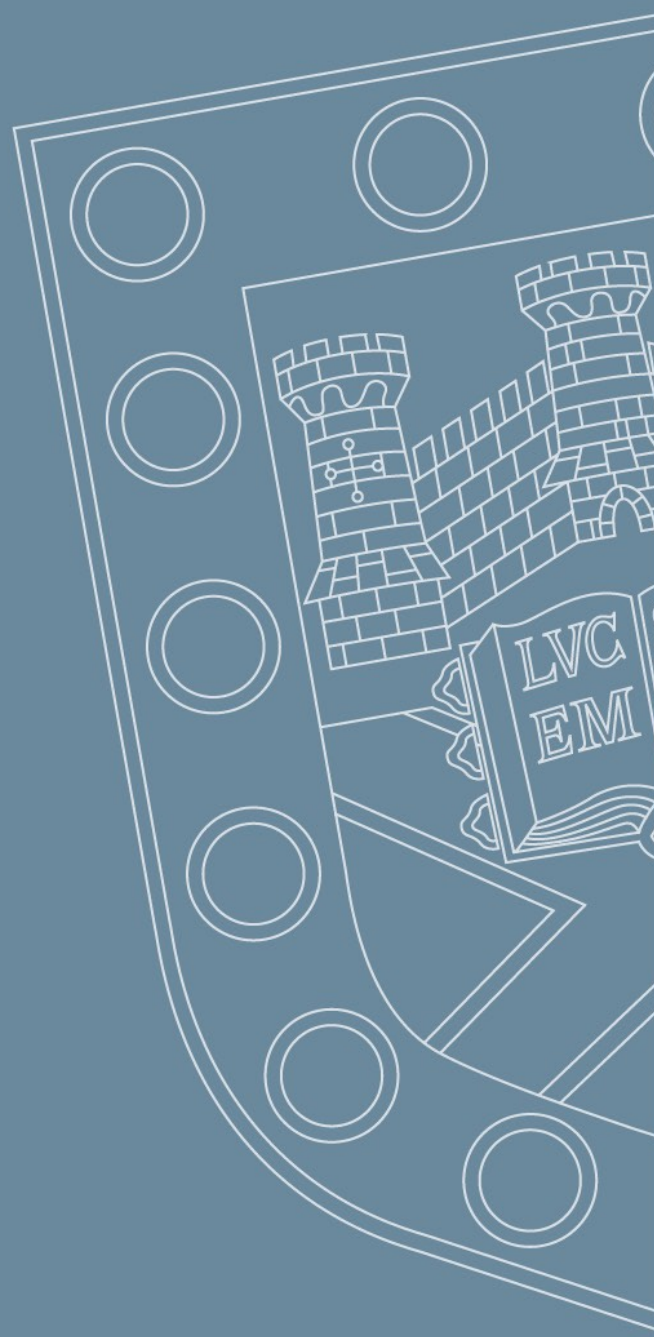
How to attack it?

- Brute force
- Differential cryptanalysis
- Side-channel attack
  - Timing
  - Power-monitoring
- among others.



https://www.youtube.com/watch?v=JW81H0R4Chg

UNIVERSITY OF EXETER



Week 3: Cryptography and Society

Cryptography

ECM1407: Social and Professional Issues of the Information Age

Marcos Oliveira