Information Security

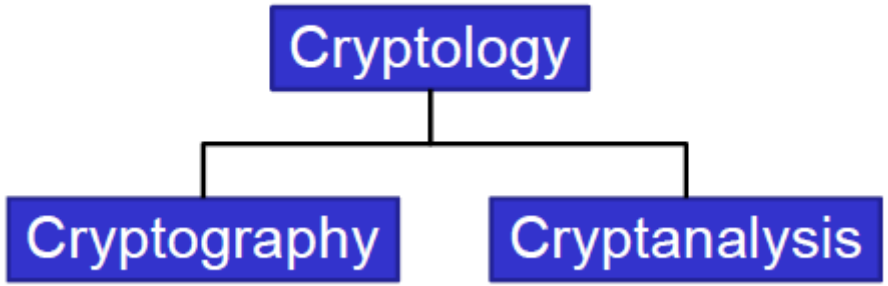
Lecture 2: Cryptography

Mona Taghavi

LaSalle College
Montréal

Terminology

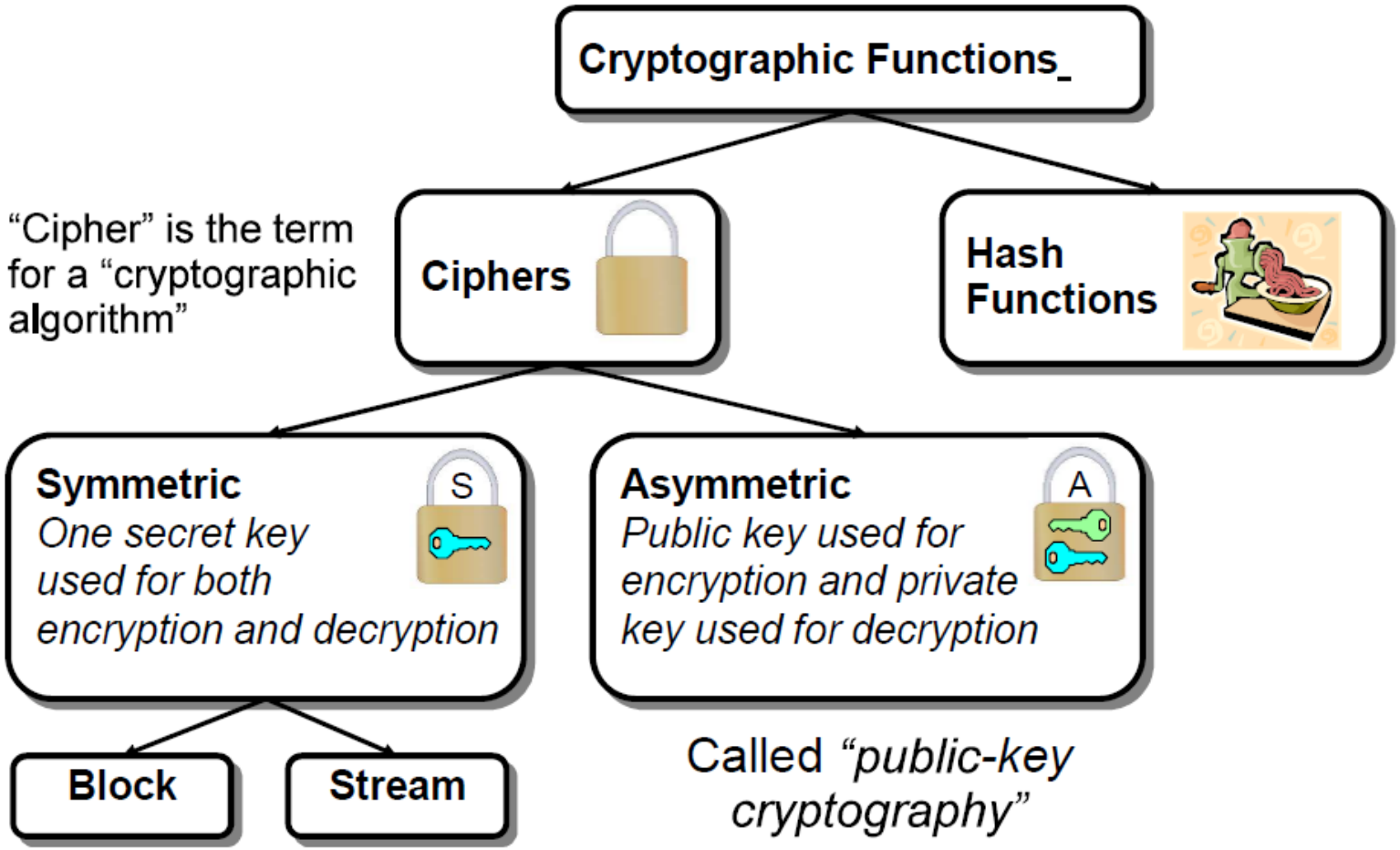
- **Greek Word**: “Krypto” = Hidden / Secret
- Cryptography is the science of secret writing with the goal of hiding the meaning of a message.
- Cryptanalysis is the science of breaking cryptography.
- Cryptology covers both cryptography and cryptanalysis.



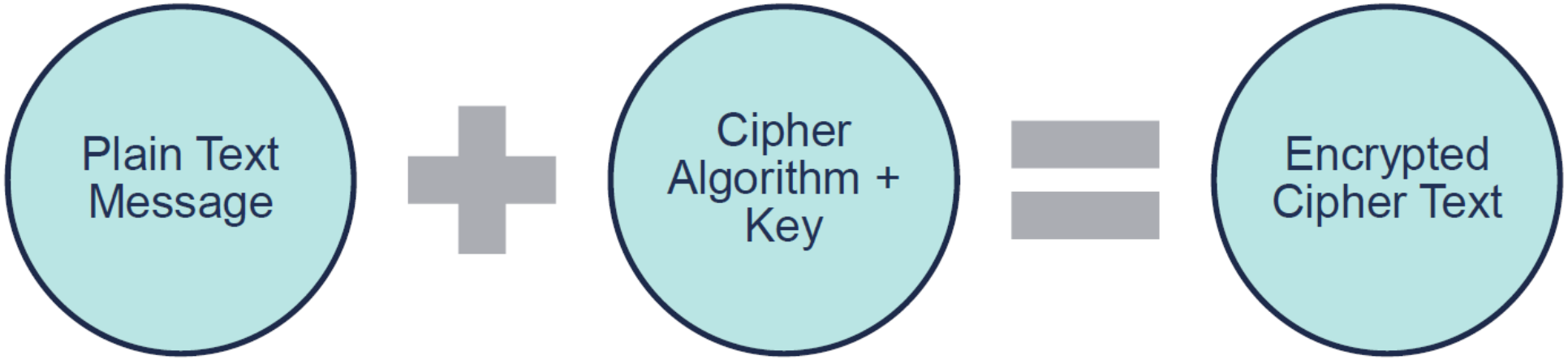
What can cryptography do?

- Crypto can provide the following security services:
- Confidentiality:
  - Makes data unreadable to entities who do not have the appropriate cryptographic keys, even if they have the data.
- Data Integrity:
  - Entities with the appropriate cryptographic keys can verify that data is correct and has not been altered, either deliberately or accidentally.
- Authentication:
  - Entities who communicate can be assured that the other user/entity or the sender of a message is what it claims to be.
- Digital Signature and PKI (Public-Key Infrastructure):
  - Strong proof of data origin which can be verified by 3rd parties.
  - Scalable (to the whole Internet) distribution of cryptographic keys.

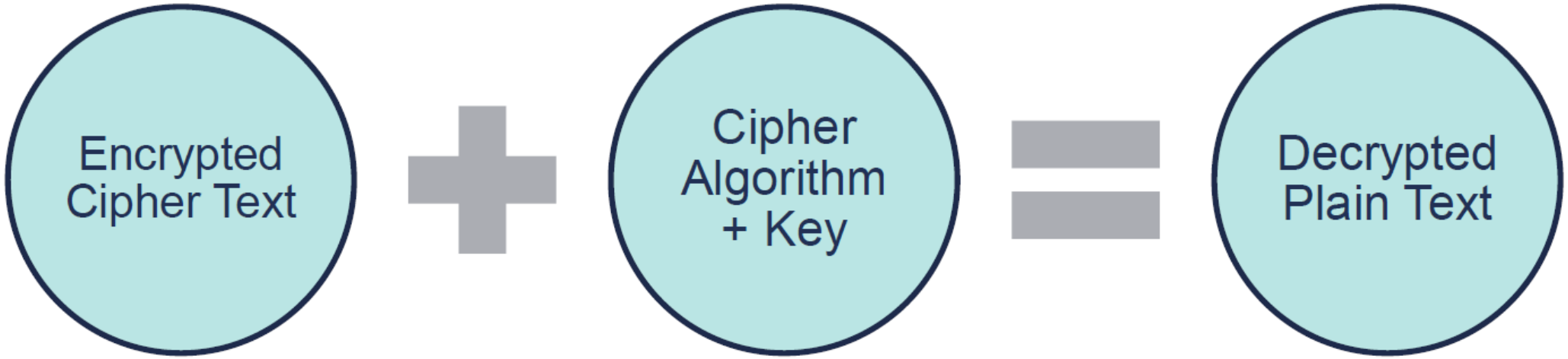
Taxonomy of cryptographic functions



Encrypting a Message

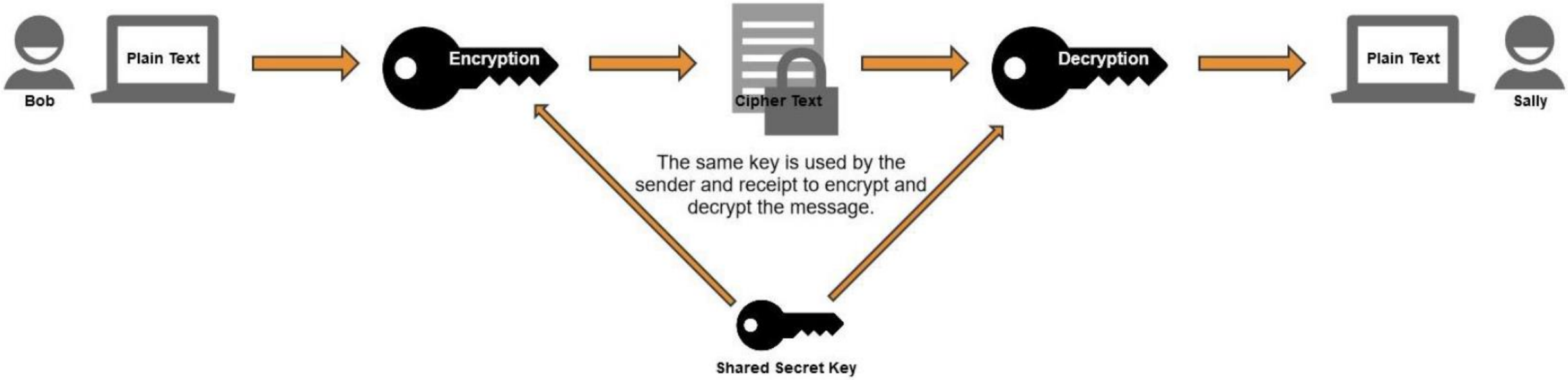


Decrypting a Message



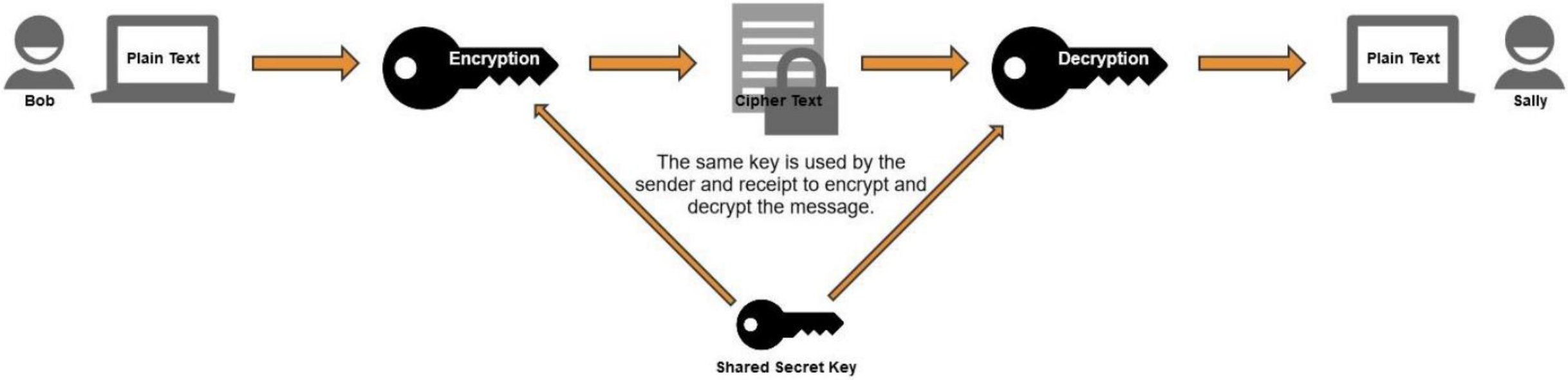
Symmetric (Private Key) Encryption

- Symmetric encryption uses a **single key** for **encryption** and **decryption**.
- Both the **sende**r and **receiver** have the **same key**and use it to encrypt and decrypt all messages.
- It’s also known as **secret-key encryption** or **private-key** encryption.

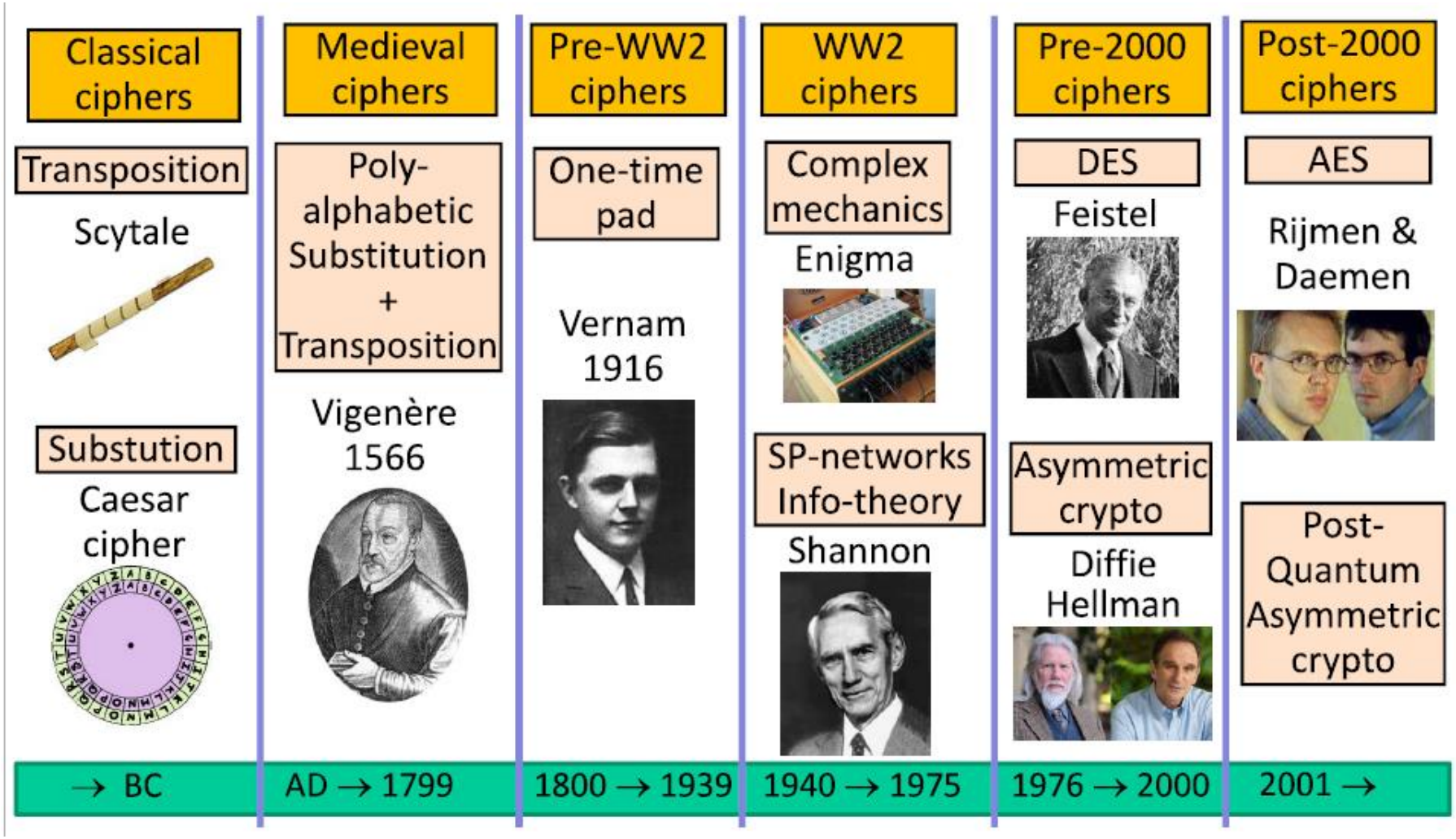


Symmetric (Private Key) Encryption

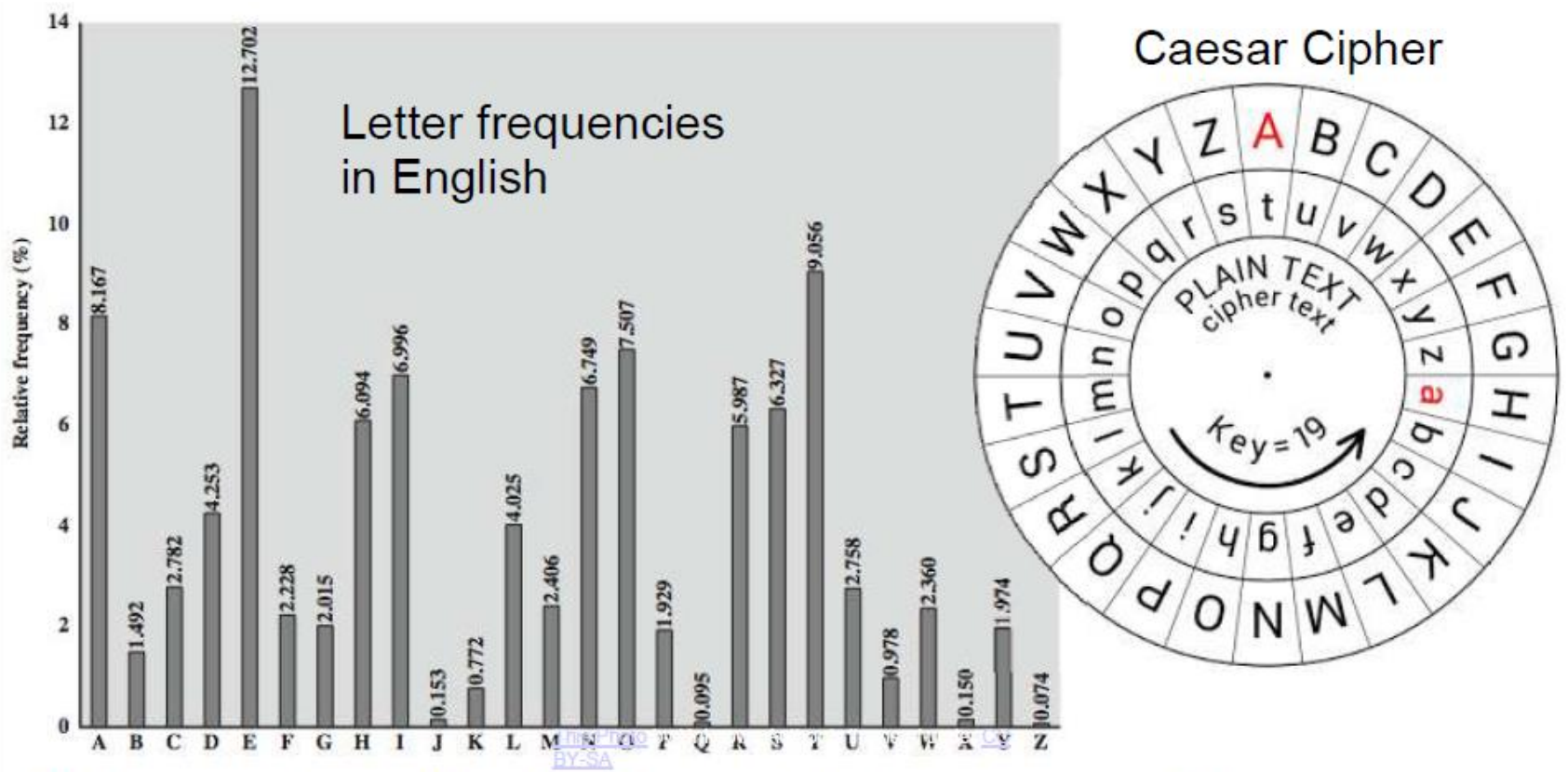
- **Symmetric encryption** is much more efficient at encrypting large amounts of data than its counterpart, **asymmetric encryption**.
- The downside of symmetrical encryption is that it makes it hard to initiate communication the first time.



Evolution of Ciphers



Letter Frequencies



Historic ciphers, like the Caesar Cipher, are weak because they fail to hide statistical regularities in the ciphertext.