

# Classical Cryptography

Thierry Sans

# Example and definitions of a cryptosystem

# Caesar Cipher - the oldest cryptosystem

A *shift* cipher – attributed to Julius Caesar (100-44 BC)

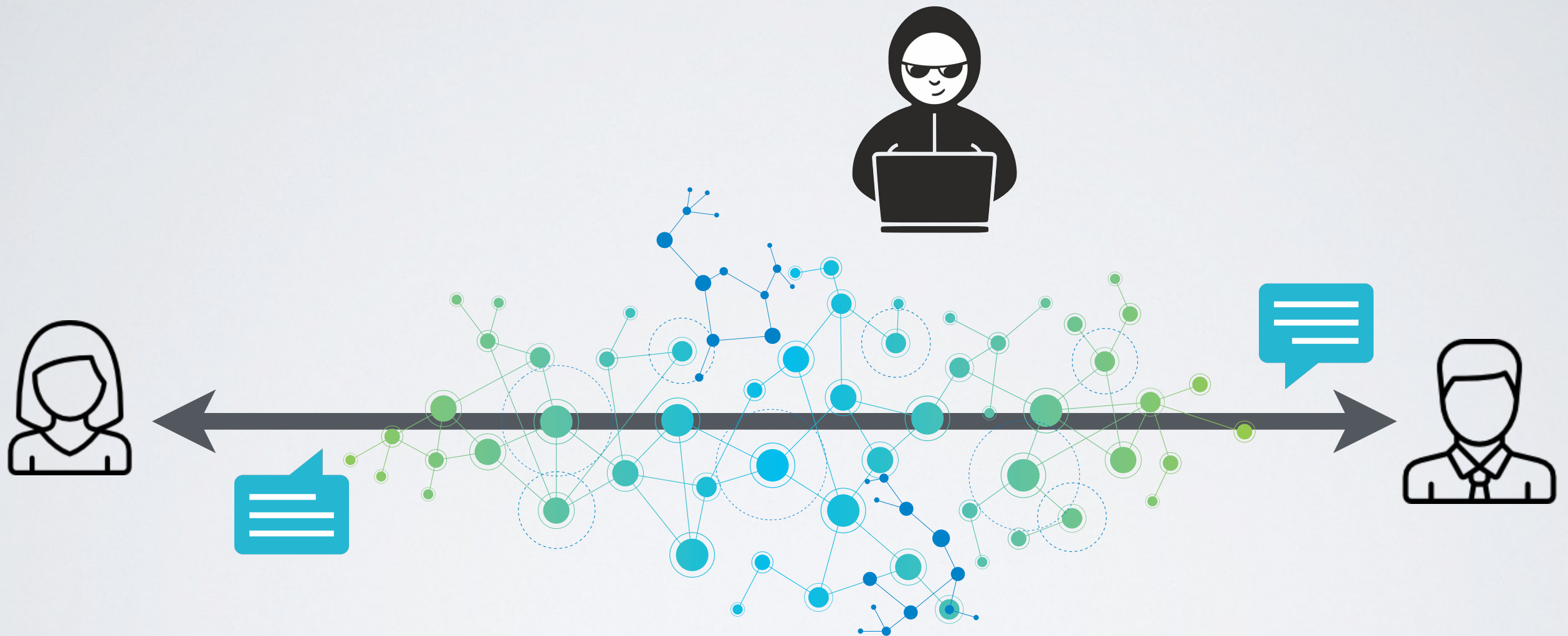
MEET ME AFTER THE TOGA PARTY

PHHW PH DIWHU WKH WRJD SDUWB

Shift the alphabet 23 places to the right and substitute letters

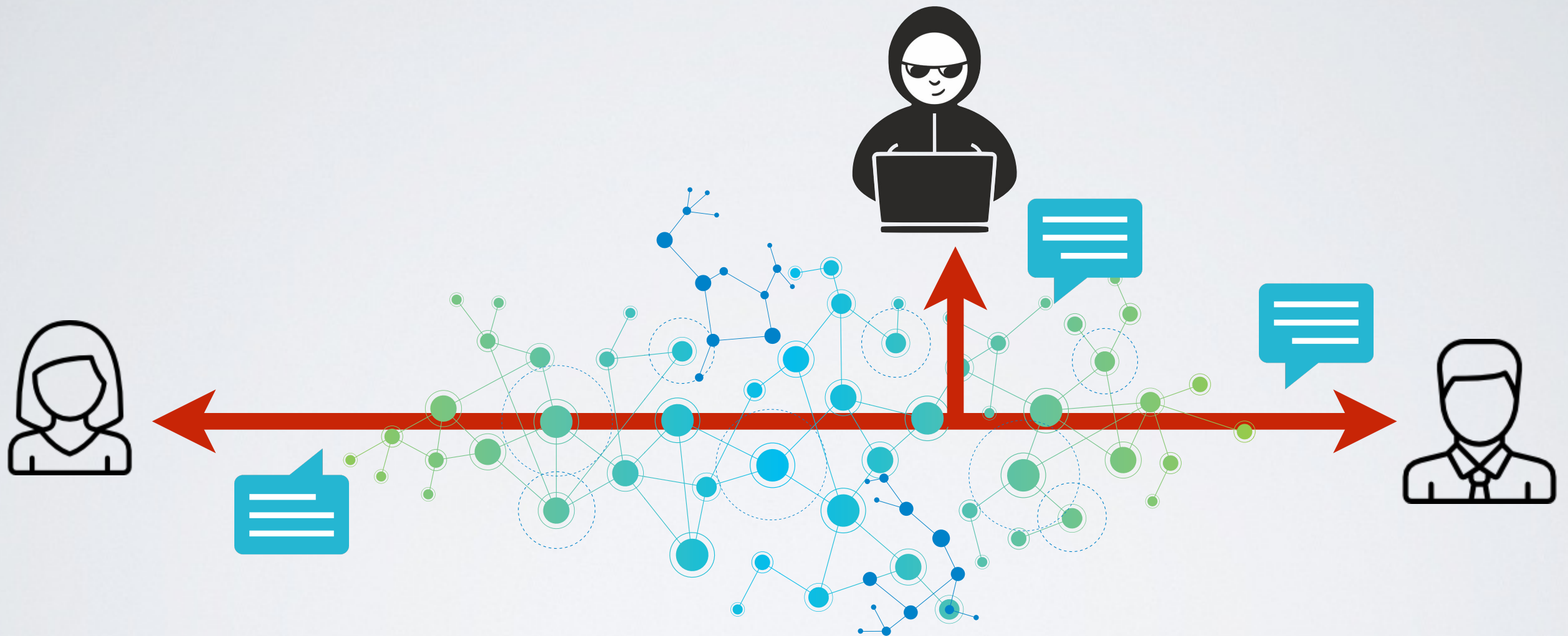
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

# Communication over an **insecure** medium



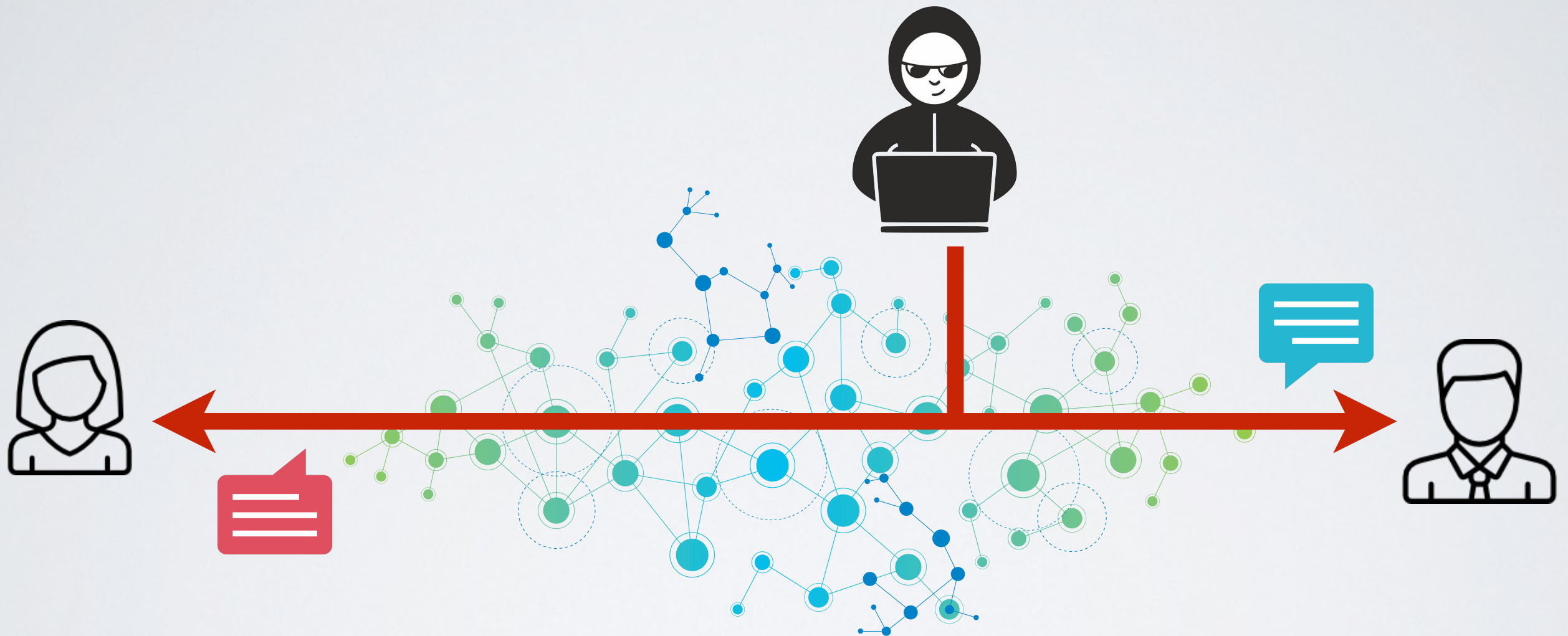


# Threat I - **Interception**



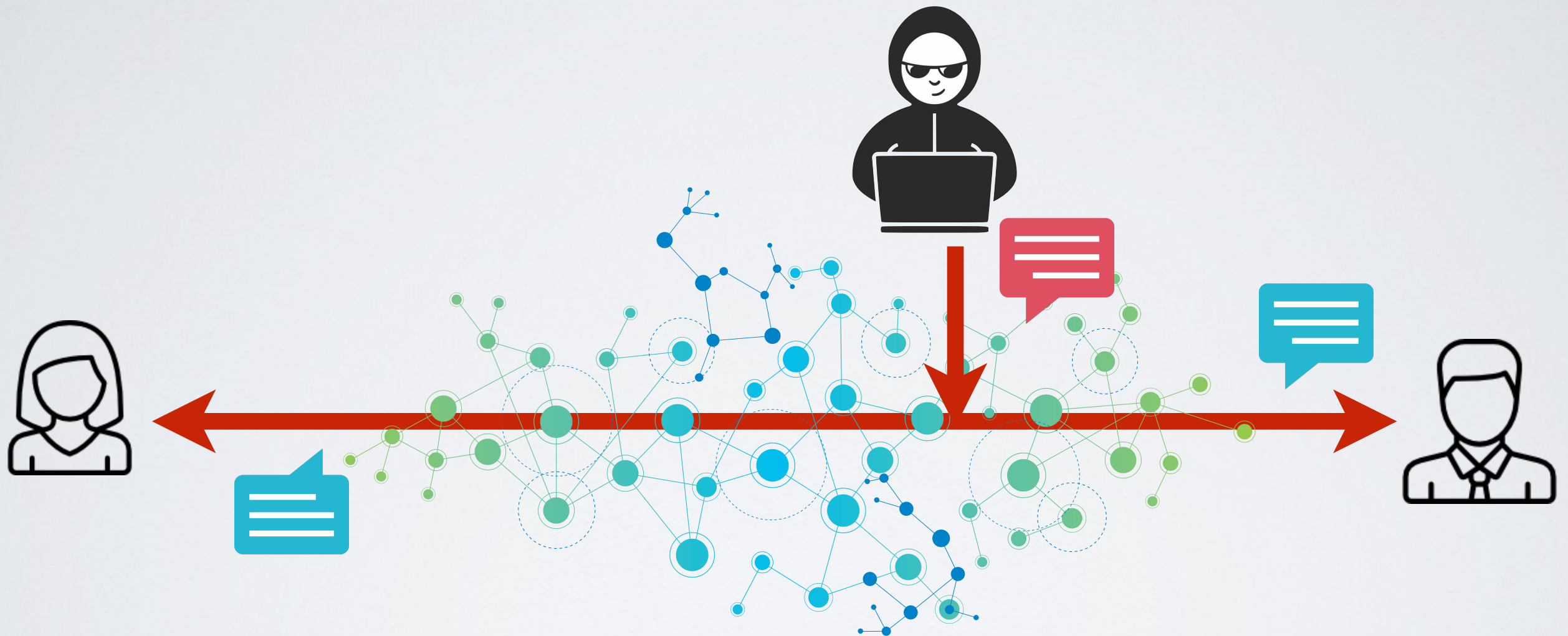
- **Interception** : an attacker can read messages

## Threat 2 - **Modification**



- **Modification** : an attacker can modify messages

## Threat 3 - **Fabrication**



- **Fabrication** : an attacker can inject messages

## Threat 4 - **Interruption**



- **Interruption** : an attacker can block messages



# Confidentiality and Integrity of communications



➡ Implement a **virtual trusted channel**  
over an insecure medium

# Definitions

## **Plaintext**

The message in its clear form (the original message)

## **Ciphertext**

The message in its ciphered form (the encrypted message)

## **Encryption**

Transform a plaintext into ciphertext

## **Decryption**

Transform a ciphertext into a plaintext

# Definitions

## **Cryptographic algorithm**

The method to do encryption and decryption

## **Cryptographic key**

An input variable used by the algorithm for the transformation

## **N-bit security entropy** (a.k.a. the key space)

The number of bits necessary to encode the number of possible keys (could be different than the key length)

# Representing data as numbers

Cryptographic algorithms are mathematical operations

- ➡ messages and keys must be represented as numbers  
for instance : ASCII encoding



# Back to Caesar Cipher

**Algorithm :** shift the alphabet of a certain number of positions

**Key :** the number of positions to shift

**Key space :** 25 possible rotations (  $\sim$  5 bits security )

**Encoding :**

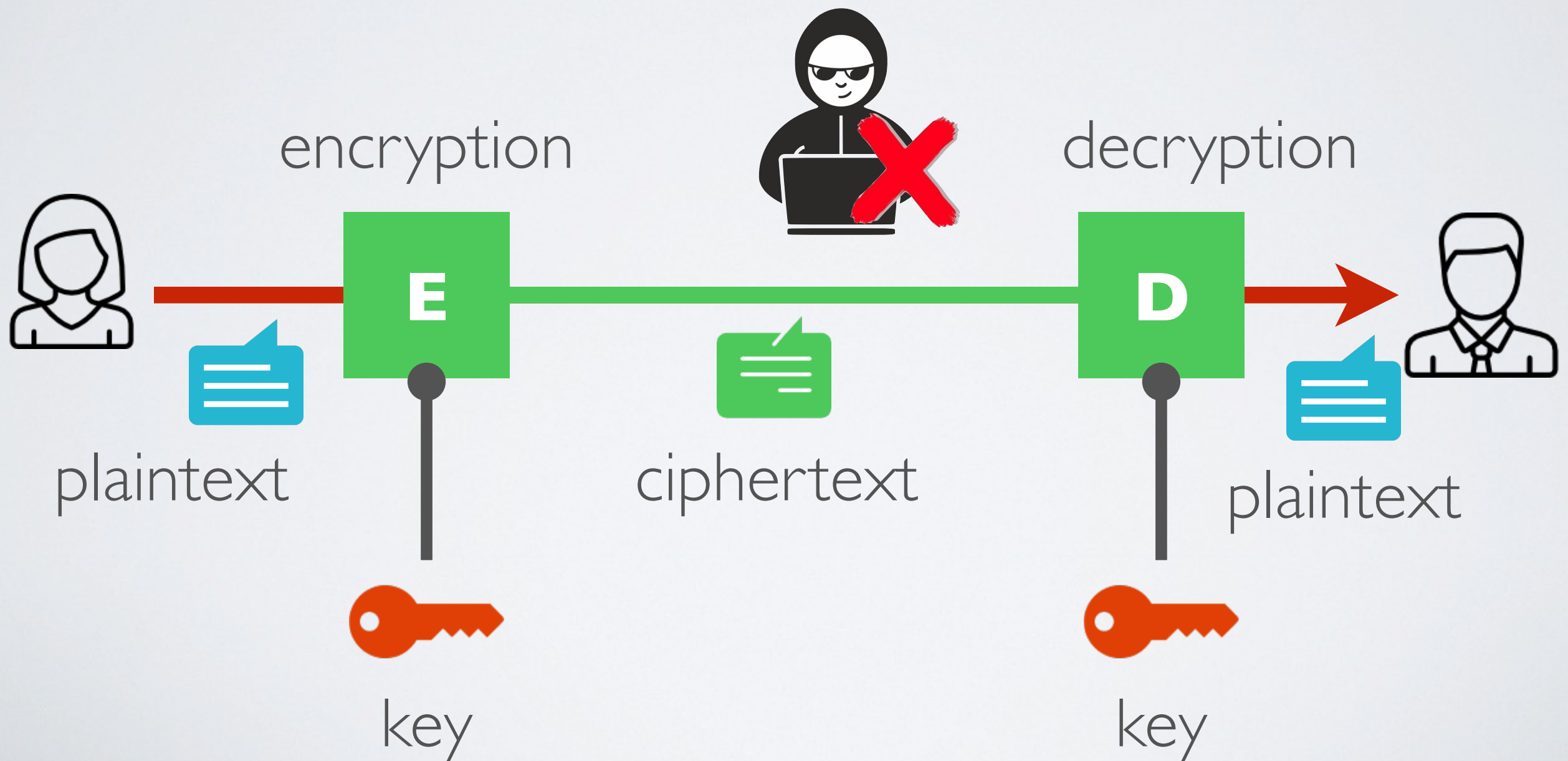
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Encrypting and decrypting one character is obtained as follows:

$$c = E(k, p) = (p + k) \bmod 26$$

$$p = D(k, c) = (c - k) \bmod 26$$

# The big picture



Breaking the cipher

# The Kerckhoffs' principle (1883)

*“The enemy knows the system”* - the security of a communication should not rely on the fact that the algorithms are secrets

- ➡ A cryptosystem should be secure even if everything about the system, except the key, is public knowledge

**No security by obscurity**



# Breaking the cipher - the attacker's model

- **Exhaustive Search** (a.k.a brute force)  
Try all possible  $n$  keys (in average it takes  $n/2$  tries)
  - **Ciphertext only**  
You know one or several random ciphertexts
  - **Known plaintext**  
You know one or several pairs of random plaintext and their corresponding ciphertexts
  - **Chosen plaintext**  
You know one or several pairs of chosen plaintext and their corresponding ciphertexts
  - **Chosen ciphertext**  
You know one or several pairs of plaintext and their corresponding chosen ciphertexts
- ➔ **A good crypto system resists all attacks**

# Breaking Caesar cipher

Exhaustive search	Yes
ciphertext only	Statistical Analysis
known plaintext	Look at the first letter and get the shift
chosen plaintext	Choose “A” and get the shift
chosen ciphertext	Choose “A” and get the shift

# Statistical Cryptanalysis

- ➔ Monoalphabetic ciphers do not change the relative frequency of letters in a message

# Evolution of cryptosystems



# A brief history of cryptography

~ 2000 years ago	Substitution ciphers (a.k.a mono alphabetic ciphers)
few centuries later	Transposition ciphers
Renaissance	Polyalphabetic ciphers
1844	Mechanization
1976	Public key cryptography

# Substitution ciphers (a.k.a mono alphabetic ciphers)

➔ Improvement over Caesar cipher

**Algorithm :** allow an arbitrary permutation of the alphabet

**Key :** set of substitutions

**Key space :**  $26!$  possible substitutions (  $4 \times 10^{26} \sim 89$  bits)

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

if we wish to replace letters

WI RF RWAJ UH YFTSDVF SFUUFYA

# Breaking substitution ciphers

Exhaustive search	Doable with a computer
ciphertext only	Statistical analysis
known plaintext	Match letters together
chosen plaintext	Choose ABCDE ... and match letters
chosen ciphertext	Choose ABCDE ... and match letters

# Polyalphabetic ciphers (a.k.a Renaissance Cipher)

➡ Vigenere cipher

**Algorithm :** combine the message and the key

**Key :** a word

**Key space :** the length of the word

$$\begin{array}{r} \text{wearediscoveredsaveyourself} \\ + \text{deceptivedeceptivedeceptive} \quad (\text{mod } 26) \\ \hline \text{ZICVTWQNGRZGVTWAVZHCQYGLMGJ} \end{array}$$

**Advantage :** Encryption of a letter is context dependent



# Breaking Polyalphabetic Ciphers

exhaustive search	Small key length only
ciphertext only	Statistical analysis for small key length and significant amount of ciphertext
known plaintext	Subtract plaintext from ciphertext
chosen plaintext	Choose AAAAAA ... and match letters
chosen ciphertext	Choose AAAAAA ... and match letters

# OTP - One Time Pad

➔ Improvement over Vigenere cipher

**Algorithm :** combine the message and the key

**Key :** an infinite random string

**Key space :** infinite

$$\begin{array}{r} \text{whatanicedaytoday} \\ \oplus \text{yksuftgoarfwfwel} \\ \hline \text{ZZZJUCLUDTUNNWGQS} \end{array}$$

**Advantage :** **this is the perfect cipher !**

**Disadvantage :** hard to use in practice, how to transmit the key ?

# The impossibility of breaking OTP

The ciphertext bears no statistical relationship to the plaintext

➡ No statistical analysis

For any plaintext and ciphertext, there exists a key mapping one to the other, and all keys are equally probable

➡ A ciphertext can be decrypted to any plaintext of the same length

# Transposition Cipher

**Algorithm :** switch letters around a permutation

**Key :** a set of permutation

**Key space :** the set of permutations

helloworld

LOLHERDLWO



# Breaking Transposition ciphers

brute force	Small key length only
ciphertext only	Hard for large permutations
known plaintext	Match letters together
chosen plaintext	Choose ABCDE ... and match letters
chosen ciphertext	Choose ABCDE ... and match letters

# The seeds of modern cryptography

## 1. **Diffusion**

Mix-up symbols

*Transposition Cipher*

## 2. **Confusion**

Replace a symbol with another

*Polyalphabetic Cipher*

## 3. **Randomization**

Repeated encryption of the same text are different

*OTP*

# Mechanization

# Mechanization

1844

Invention of the telegraph

1939

World War II  
The Enigma Machine



# The cryptography toolbox

# Cryptography is not just about confidentiality

## **Integrity**

digital signatures, hash functions

## **Non-repudiation**

contract-signing

## **Anonymity**

electronic cash, electronic voting

...

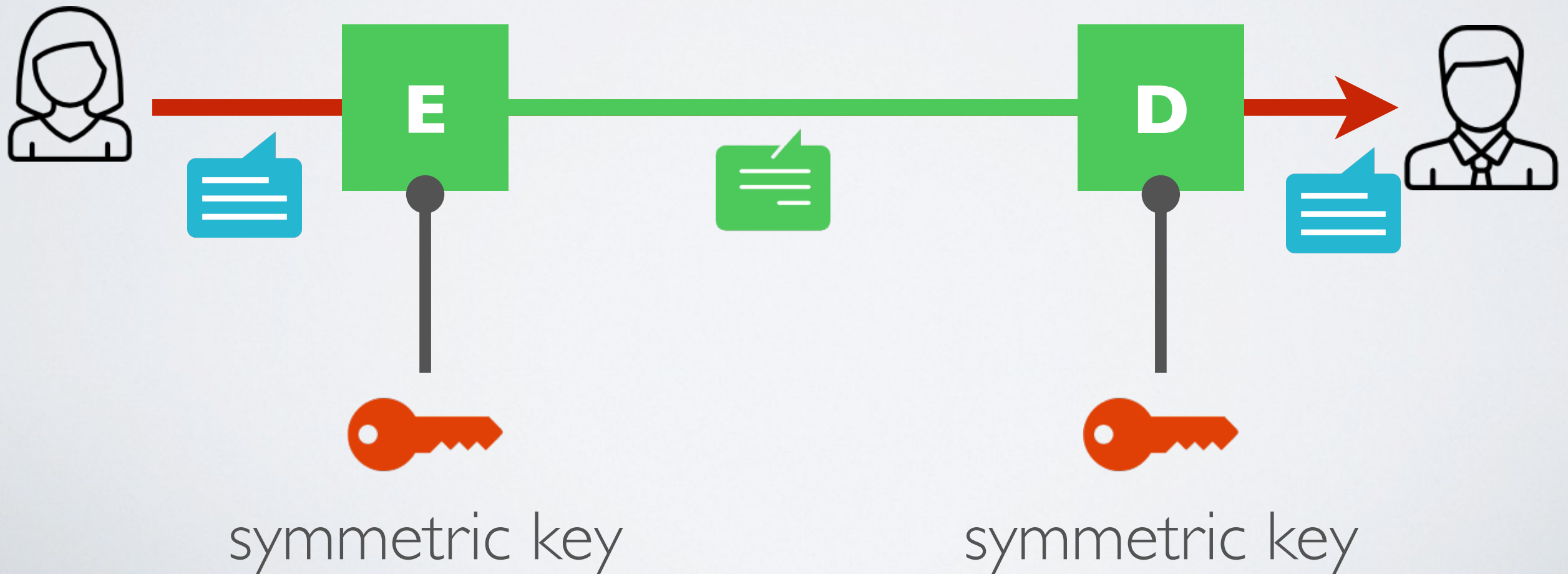
## **Availability**

# The crypto toolbox

- Symmetric cryptography schemes
- Asymmetric cryptography schemes
- Message digests
- Digital signatures
- Certificates

# Symmetric encryption

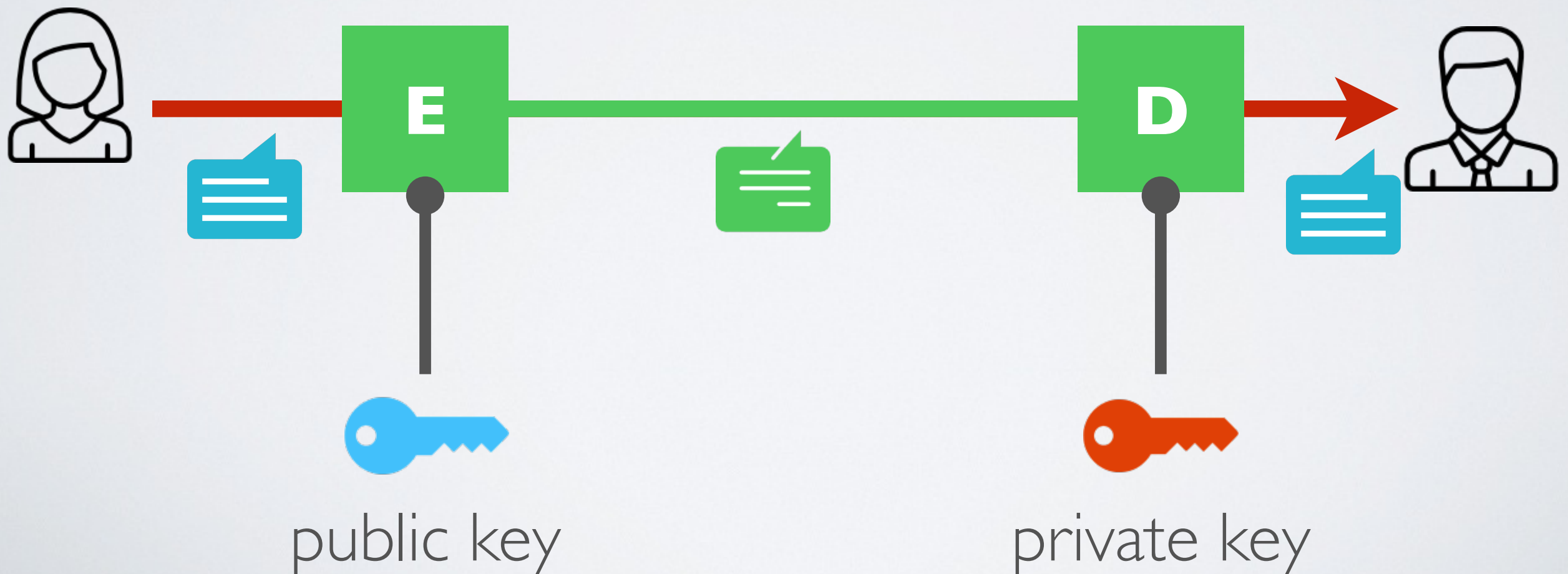
➡ The same key is used for encryption and decryption





# Asymmetric encryption a.k.a Public Key Cryptography

- ➡ The public key for encryption
- ➡ The private key for decryption



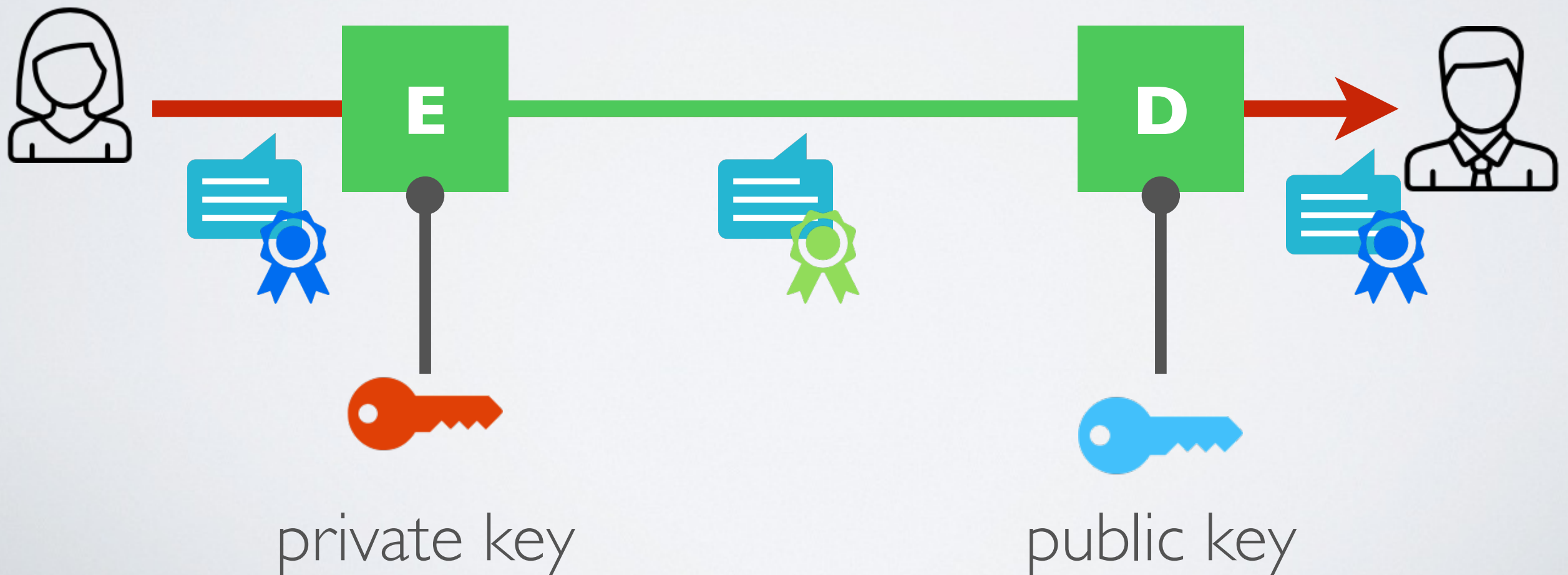
# Message digests

**Message digests** are meant for creating fingerprints of messages

- Un-keyed message digest : hashes, checksum
- Keyed message digests : MACs

# Digital Signature

- ➔ The private key for encryption
- ➔ The public key for decryption



# Certificates - Public Key Infrastructure

**Certificates** are meant for verifying someone's identity

- Binding between a public key and an owner
- Certified by a certification authority