IDENTITIES

Enlightening
Interdisciplinarity
in STEM
for Teaching

Introductory lecture on cryptography elements

Cryptography module

Co-funded by the
Erasmus+ Programme
of the European Union

Grant Agreement n°2019-1-IT02-KA203-063184

Cryptography used to *ensure secure communication* (**confidentiality**, **integrity**, **authenticity**)

- Internet security
- Credit cards (smart cards)
- Electronic passports
- Electronic currency (bitcoins)
- Electronic voting
- Medical data

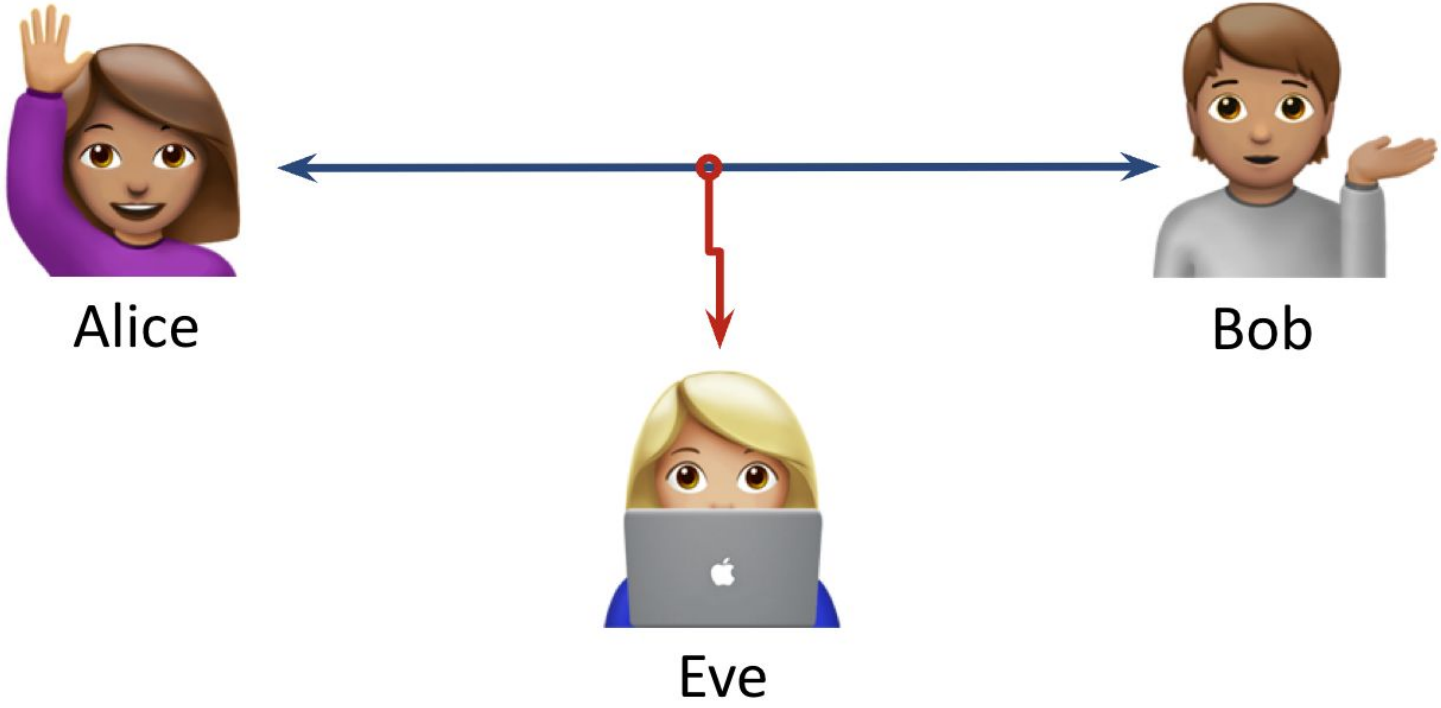

Alice
Bob
Eve

Figure out the answer to the riddle below.
Use the cipher table to show how the letters were encrypted.
Find a pattern to complete the table.

What is a clumsy bee?

B CVNCMJOH CFF

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

Figure out the answer to the riddle below.
Use the cipher table to show how the letters were encrypted.
Find a pattern to complete the table.

What is a clumsy bee?

B		C	V	N	C	M	J	O	H		C	F	F

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

Figure out the answer to the riddle below.
Use the cipher table to show how the letters were encrypted.
Find a pattern to complete the table.

What is a clumsy bee?

a		b	u	m	b	l	i	n	g		b	e	e
B		C	V	N	C	M	J	O	H		C	F	F

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

*How do we **encrypt**?*

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	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

*How do we **encrypt**?*

- Shift the alphabet by 1
- C = m +1 (mod 26)

Example: the 11th letter is encrypted by the 12th letter (k -> L)

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	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

We can shift by another number k

Additive Ciphers

- Plaintext **m**
- Ciphertext **C**
- Key **k**
- **Encryption** C = m+k (mod 26)
- **Decryption** m = C-k (mod 26)

L MFXMWTYR MPP

Example: Shifting by 11

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
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

PROBLEM with this system

To determine what the shift is, we need to guess *only one letter*

(...there are 25 guesses at most!)

L		M	F	X	M	W	T	Y	R		M	P	P

We need to add some more confusion ...

Multiplicative Ciphers

- Plaintext **m**
- CIPHERTEXT **C**
- Key **k**
- **Encryption** C = m*k (mod 26)
- **Decryption** m = C*k^-1 (mod 26)

Multiplicative Ciphers (examples of enc dec)

- Plaintext **m**
- CIPHERTEXT **C**
- Key **k** (here **k**=5)

Encryption **C** = m*k(mod 26)

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
0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
A	F	K	P	U	Z	E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B	G	L	Q	V

m = C*k^-1(mod 26) **Decryption**

5 * 21 = 105 (mod 26) = 1 (mod 26) => k^-1 = 21 i.e. 21 is the multiplicative inverse of k=5
For example to decipher D => 3 * 21(mod 26) = 63 (mod 26)= 11 (mod 26) => l

Multiplicative Ciphers

- The KEY has to be coprime with 26 (alphabet length)
  - The possible keys are only the numbers coprime with 26
- If not, **encryption is NOT injective**
  - Example (table below): the **KEY is 2** (*not coprime with 26*).
    Because of the modulo operation the encryption produces only half of the letters.

Encryption **C** = m*k(mod 26)

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
0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
A	C	E	G	I	K	M	O	Q	S	U	W	Z	A	C	E	G	I	K	M	O	Q	S	U	W	Z

k = 2 example a => A, but also n => A because 13*2=26=0mod26

Problem:
Each plaintext letter is always encrypted with the same ciphertext letter.

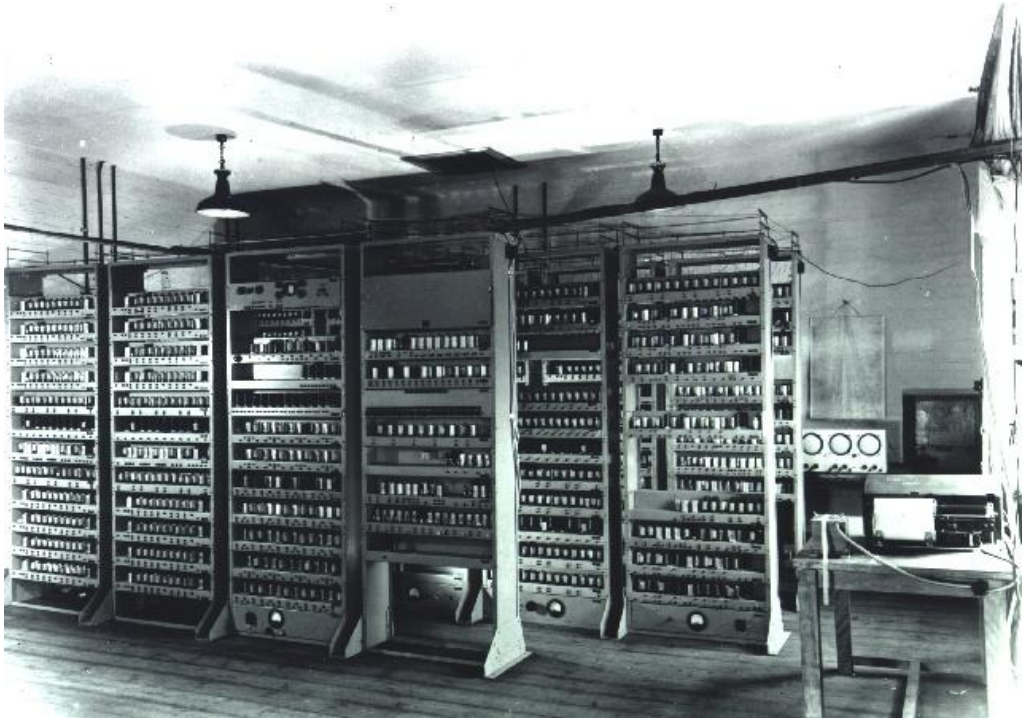
Solution:
Polyalphabetic Ciphers like the Vigenere Code

Each plaintext letter is encrypted by different ciphertext 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
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

But even that was broken and ....

COMPUTER SCIENCE came in the 50s



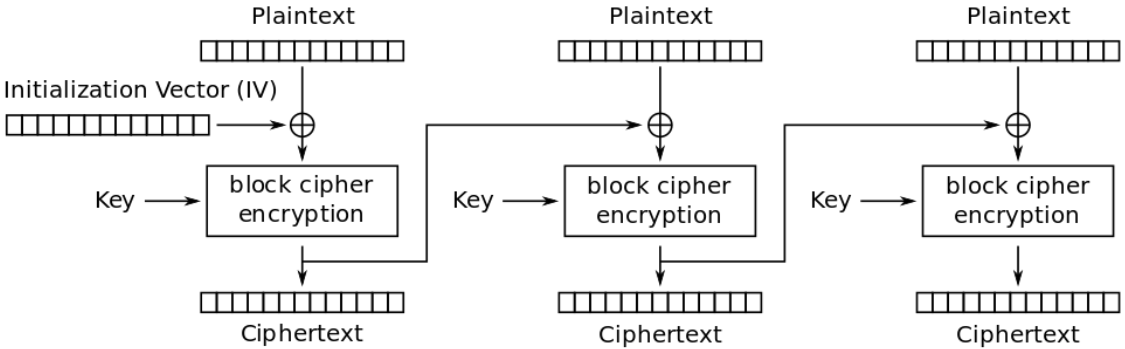
Binary ciphers

- **Every letter is translated to a binary vector**
- The message is splitted into blocks
- Every block is encrypted using a binary cipher

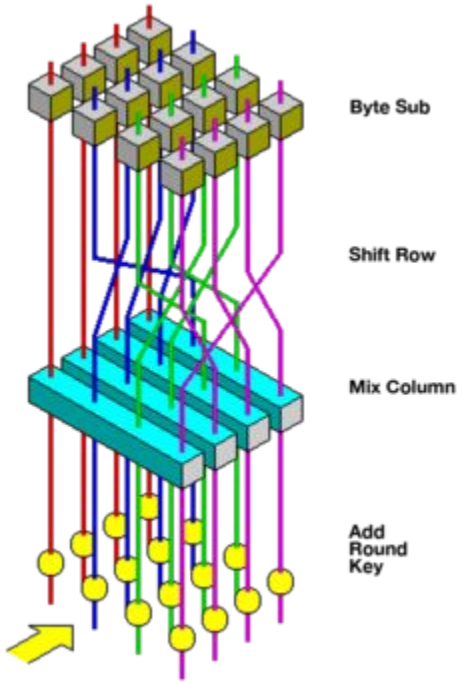
ASCII Alphabet			
A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

Binary ciphers

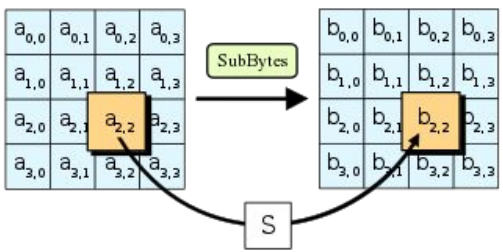
- Every letter is translated to a binary vector
- **The message is splitted into blocks**
- **Every block is encrypted using a binary cipher**

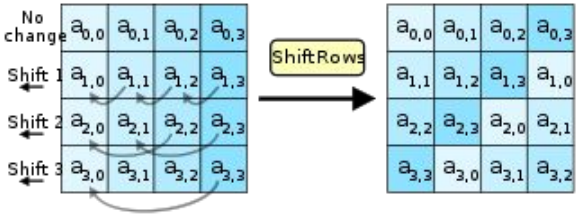


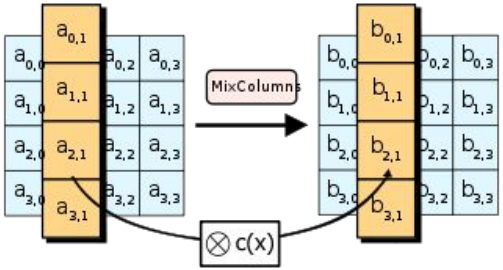
Cipher Block Chaining (CBC) mode encryption

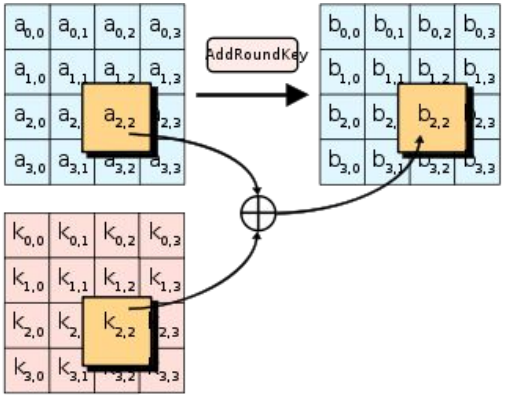


Nowadays we are using **AES**
(***A**dvanced **E**ncryption **S**tandard*)

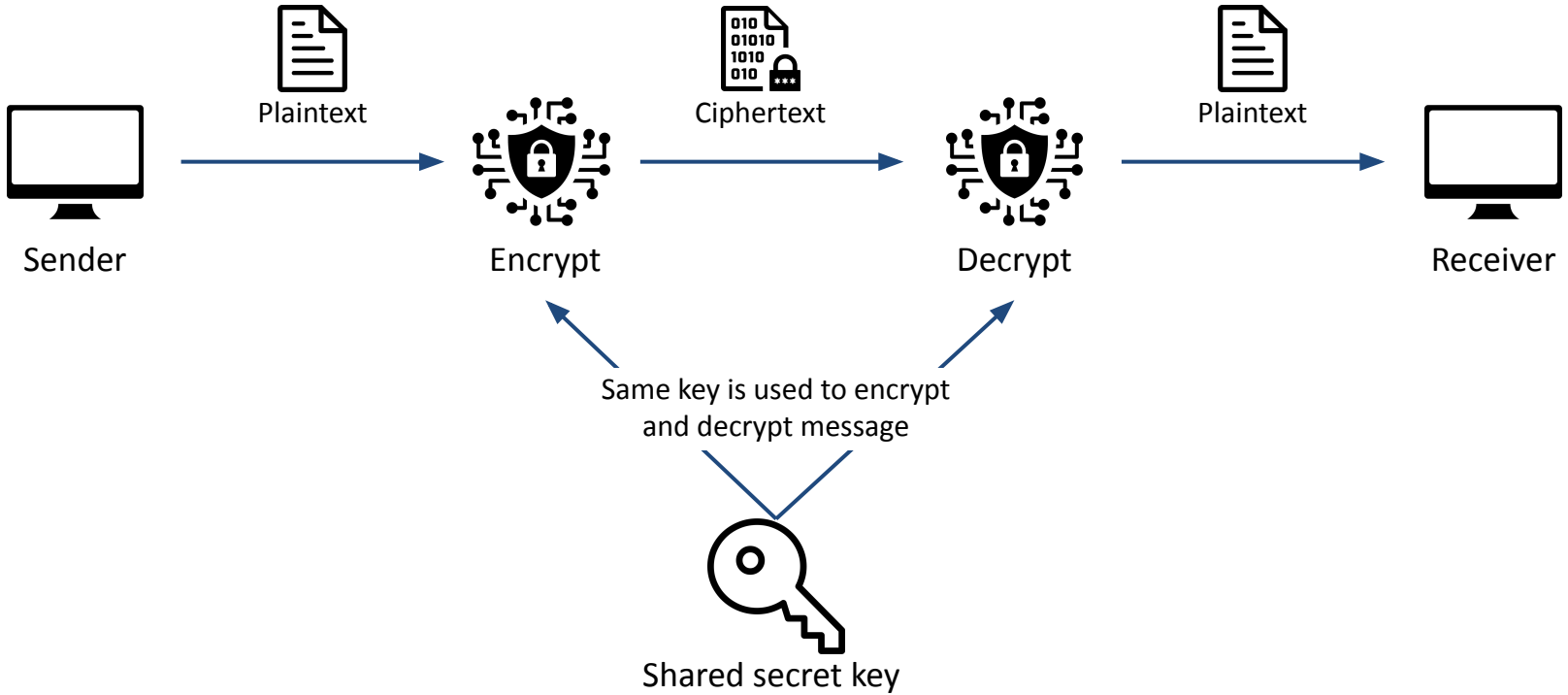




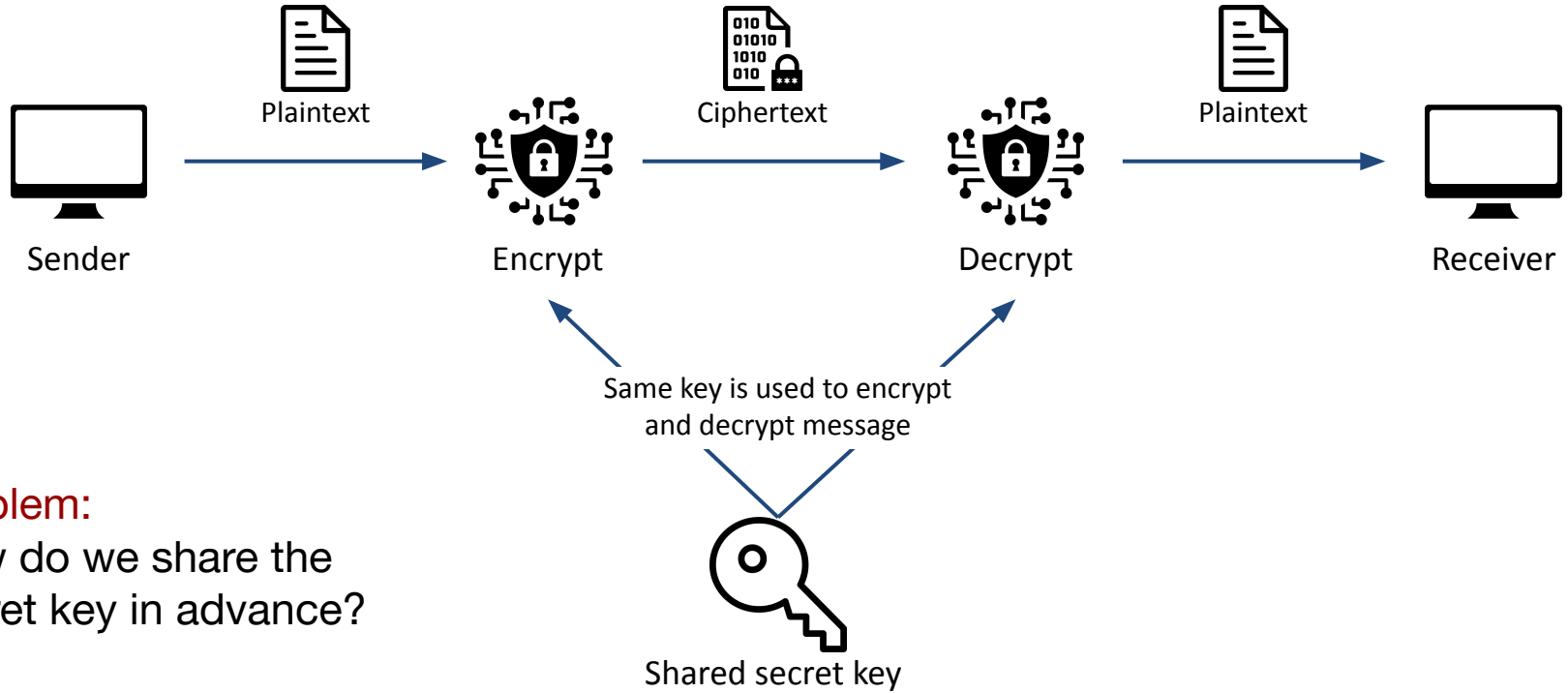




SYMMETRIC CRYPTOSYSTEM

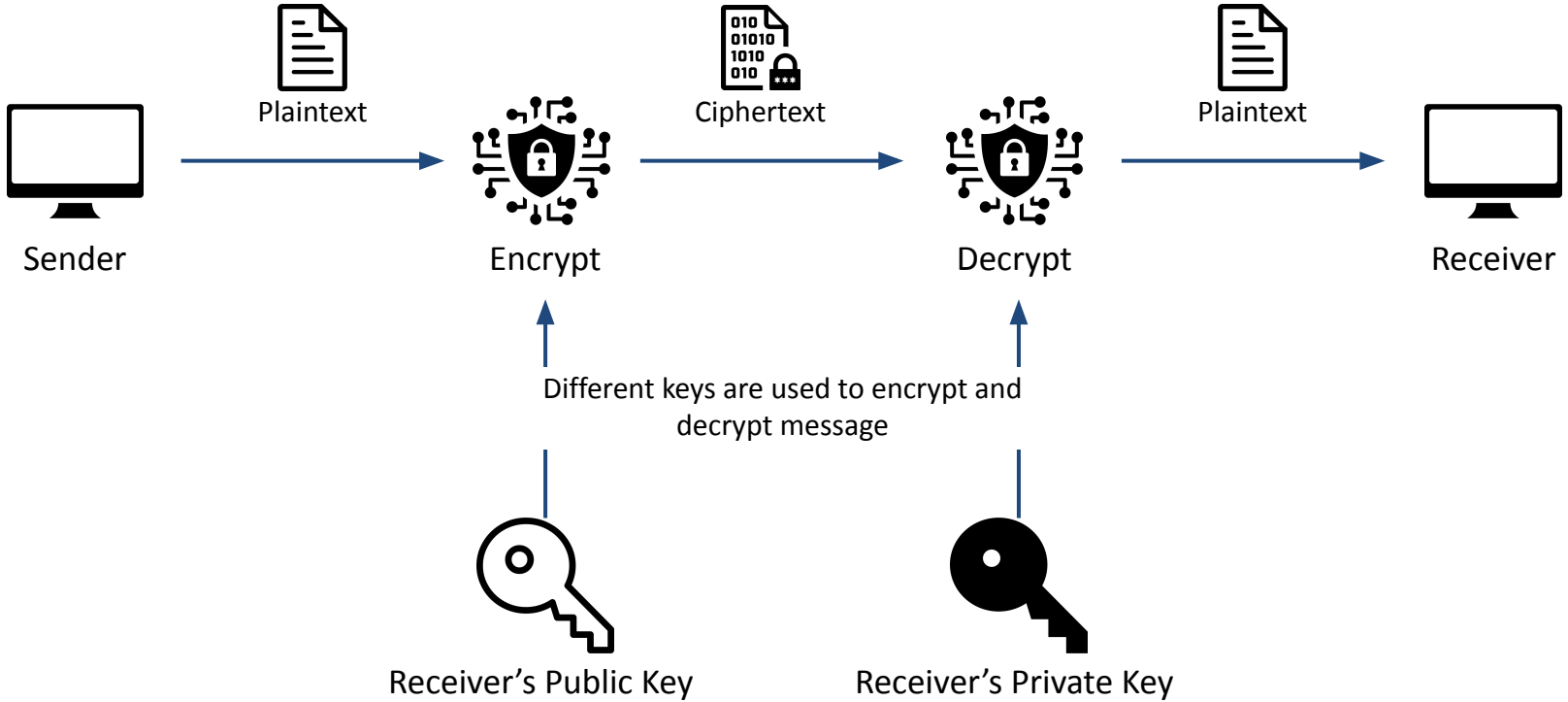


SYMMETRIC CRYPTOSYSTEM



Problem:
How do we share the secret key in advance?

ASYMMETRIC CRYPTOSYSTEM



Kerckhoff's Principle

A cryptosystem should be secure even if everything about the system EXCEPT THE KEY is public knowledge

Engineers should design their system assuming that their opponent knows the system in detail

Credits for the images

- Bee: Openclipart: Cartoon Bee is licensed under CC0 1.0 Universal (CC0 1.0). Public Domain Dedication
- Encryption using the Cipher Block Chaining (CBC) mode: By WhiteTimberwolf (SVG version) - PNG version, Public Domain, https://commons.wikimedia.org/w/index.php?curid=26434096
- AES (Rijndael) Round Function: By John Savard - https://www.eng.tau.ac.il/~yash/crypto-netsec/rijndael.htm, CC0, https://commons.wikimedia.org/w/index.php?curid=103718081
- SubBytes operation for AES. By User:Matt Crypto - Own work, Public Domain https://commons.wikimedia.org/w/index.php?curid=1118913
- ShiftRows operation for AES. By User:Matt Crypto - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=1118782
- MixColumns operation for AES. By User:Matt Crypto - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=1118874
- AddRoundKey operation for AES. By User:Matt Crypto - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=1118831
- EDSAC: Copyright Computer Laboratory, University of Cambridge. Reproduced by permission. CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=432935

IDENTITIES

Enlightening
Interdisciplinarity
in STEM
for Teaching

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

UNIVERSITAT DE
BARCELONA

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

UNIVERSITÀ
DI PARMA

Co-funded by the
Erasmus+ Programme
of the European Union

Grant Agreement n°2019-1-IT02-KA203-063184