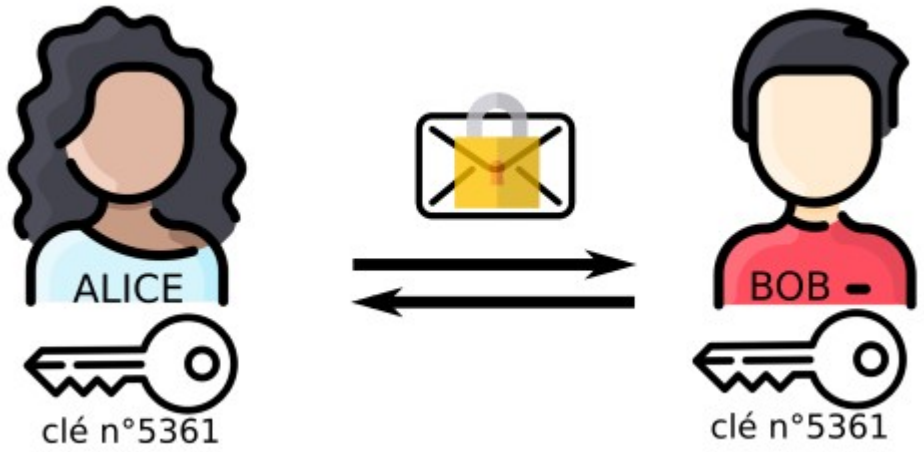
Chiffrements

Nicolas Blanc, Michel Courtieu, Lycée Anna de Noailles (Evian)

Sommaire

1 . Chiffrements symétriques

Le principe du **chiffrement symétrique** est d'utiliser **la même clé** pour chiffrer et déchiffrer un message.



Avantages : Les chiffrements symétriques sont rapides et consomment peu de ressources.

Inconvénients : Transmettre la clé de façon sécurisée.

1.1 Code de César

Principe : Le **code de César** s'applique à n'importe quel message écrit dans un **alphabet** fixé. On choisit un **nombre entier** qui sert de **clé**. Pour chiffrer le message, on remplace chaque caractère par le caractère décalé de la clé dans l'alphabet.

Exemple : Avec l'alphabet des majuscules, et la clé **3** on obtient les décalages suivants.

Clair	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
Codé	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

EXERCICE 1

Chiffrer le mot "PYTHON" avec le code de César et avec la clé **5**.

CORRECTION

Chiffrer le mot "PYTHON" avec le code de César et avec la clé **5**.

Clair	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
Codé	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

TEXTE CLAIR : PYTHON

TEXTE CODE : UDYMTS

Nicolas Blanc, Michel Courtieu, Lycée Anna de Noailles (Evian)

EXERCICE 2

Déchiffrer le mot "FRGH" avec le code de César et avec la clé **3**.

Nicolas Blanc, Michel Courtieu, Lycée Anna de Noailles (Evian)

CORRECTION

Déchiffrer le mot "FRGH" avec le code de César et avec la clé **3**.

Clair	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
Codé	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

TEXTE CODE : FRGH

TEXTE CLAIR : CODE

1.2 Code de Vigenère

Principe : Le **code de Vigenère** reprend le principe du code de César. Mais la clé dans le code de Vigenère est un texte et on décale chaque caractère du message à chiffrer par le caractère décalé suivant les caractères successifs de la clé.

Exemple : Avec l'alphabet des majuscules, et la clé **BC** on chiffre le mot **MATH** en

NCUJ

On peut s'aider pour cela de la table de Vigenère.

	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

EXERCICE 3

Chiffrer le mot "PYTHON" avec le code de Vigenère et avec la clé **NSI**.

Nicolas Blanc, Michel Courtieu, Lycée Anna de Noailles (Evian)

CORRECTION

Chiffrer le mot "PYTHON" avec le code de Vigenère et avec la clé **NSI**.

TEXTE CLAIR : PYTHON

TEXTE CODE : CQBUGV

	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

EXERCICE 4

Déchiffrer le mot "OOOCRG" avec le code de Vigenère et avec la clé **BAC**.

Nicolas Blanc, Michel Courtieu, Lycée Anna de Noailles (Evian)

CORRECTION

Déchiffrer le mot "OOOCRG" avec le code de César et avec la clé **BAC**.

TEXTE CODE : OOOCRG

TEXTE CLAIR : NOMBRE

	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

1.3 Chiffrement affine

Principe : Chaque caractère est associé à un entier (rang dans l'alphabet en partant de 0). On applique une fonction affine f définie par la formule : $f(x) = ax + b$ à chacun de ses rangs. Puis on remplace le caractère du texte en clair par le caractère dont le rang correspond à l'image par la **fonction affine f modulo 26**.

Exemple : On va chiffrer le mot **NSI** avec la fonction affine $f(x) = 3x + 2$.

Clair	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
Rang x	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
$f(x)$	2	5	8	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77
$f(x)\%26$	2	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25
Codé	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z

TEXTE CLAIR : **NSI**

TEXTE CODE : **PEA**

Déchiffrage : Pour pouvoir déchiffrer un chiffrement affine il faut une condition mathématique importante sur le coefficient directeur a de la fonction affine. Il faut que a soit premier avec 26 pour que a soit inversible modulo 26.
On considère une telle fonction affine f définie par $f(x) = a\,x + b$.
On note a_1 l'entier compris entre 0 et 25 tel que : $a\,a_1 = 1$ modulo 26.
Alors la fonction affine f_1 qui permet de déchiffrer est définie par :
$f_1(x) = a_1(x - b) = a_1\,x - a_1\,b = a_1\,x + b_1$.
Avec a_1 : l'inverse de a modulo 26 et $b_1 = -a_1\,b$.

Exemple : On a chiffré le mot **NSI** en **PEA** avec la fonction affine $f(x) = 3\,x + 2$.
Ici $a = 3$ et $b = 2$. On a : $a_1 = 9$ donc $f_1(x) = 9(x - 2) = 9\,x - 18 = 9\,x + 8$ [26]

Codé	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
Rang x	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
$f_1(x)$	8	17	26	35	44	53	62	71	80	89	98	107	116	125	134	143	152	161	170	179	188	197	206	215	224	233
$f_1(x)\%26$	8	17	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25
Clair	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z

TEXTE CODE : **PEA**

TEXTE CLAIR : **NSI**

EXERCICE 5

Chiffrer le mot "LAC" avec le chiffrement affine en utilisant la fonction affine f définie par $f(x) = 3x + 5$.

CORRECTION

Chiffrer le mot "LAC" avec le chiffrement affine en utilisant la fonction affine f définie par $f(x) = 3x + 5$.

Clair	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
Rang x	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
$f(x)$	5	8	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77	80
$f(x)\%26$	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2
Codé	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C

TEXTE CLAIR : LAC

TEXTE CODE : MFL

1.4 Le chiffrement XOR

Table de vérité du XOR (ou exclusif):

Entrées		Sortie
A	B	A ^ B
0	0	
0	1	
1	0	
1	1	

Principe : Le principe est un peu le même que le chiffrement de Vigenère. Pour coder un texte, on utilise une clé qui est elle même un texte. On numérise le texte grâce au code ASCII que l'on écrit en binaire, puis en répétant la clé autant de fois que nécessaire, on effectue un XOR bit à bit.

Exemple : On va chiffrer le mot "PYTHON" avec la clé "NSI".

Caractères	P	Y	T	H	O	N
Code ASCII	80	89	84	72	79	78
ASCII Binaire	01010000	01011001	01010100	01001000	01001111	01001110
Clé répétée						
chiffrement						

N	S	I
78	83	73
01001110	01010011	01001001

Exemple : On va chiffrer le mot "PYTHON" avec la clé "NSI".

Caractères	P	Y	T	H	O	N
Code ASCII	80	89	84	72	79	78
ASCII Binaire	01010000	01011001	01010100	01001000	01001111	01001110
Clé répétée	01001110	01010011	01001001	01001110	01010011	01001001
chiffrement						

N	S	I
78	83	73
01001110	01010011	01001001

Exemple : On va chiffrer le mot "PYTHON" avec la clé "NSI".

Caractères	P	Y	T	H	O	N
Code ASCII	80	89	84	72	79	78
ASCII Binaire	01010000	01011001	01010100	01001000	01001111	01001110
Clé répétée	01001110	01010011	01001001	01001110	01010011	01001001
chiffrement	00011110	00001010	00011101	00000110	00011100	00000111

N	S	I
78	83	73
01001110	01010011	01001001

Déchiffrement : On déchiffre ensuite en utilisant un XOR avec la même clé.

chiffrement	00011110	00001010	00011101	00000110	00011100	00000111
Clé répétée	01001110	01010011	01001001	01001110	01010011	01001001
clair	01010000	01011001	01010100	01001000	01001111	01001110
Code ASCII	80	89	84	72	79	78
Caractères	P	Y	T	H	O	N

EXERCICE 6

Chiffrer le mot "BAC" avec le chiffrement XOR en utilisant la clé 'DE'.

CORRECTION

Chiffrer le mot "BAC" avec le chiffrement XOR en utilisant la clé 'DE'.

Caractères	B	A	C
Code ASCII	66	65	67
ASCII Binaire	01000010	01000001	01000011
Clé répétée	01000100	01000101	01000100
chiffrement	00000110	00000100	00000111

D	E
68	69
01000100	01000101

2 . Chiffrements asymétriques

Le principe du **chiffrement asymétrique** est d'utilisé **deux clés différentes**, une pour chiffrer appelée **clé publique** et l'autre pour déchiffrer appelée **clé privée**.

2.1 Code RSA

Principe : Le **code RSA** est un chiffrement asymétrique. La **clé publique** est constituée de deux nombres entiers (e , n) et la **clé privée** est constituée aussi de deux nombres entiers (d , n) . Ces clés sont construites à partir de nombres premiers. Le code RSA permet de crypter des informations numériques de type entier (par exemple le code ASCII).

Chiffrement : On code n'importe quel entier m de la façon suivante :

$$c = m^{e} \text{ modulo } n$$

Déchiffrement : On décode n'importe quel entier codé c de la façon suivante :

$$m = c^{d} \text{ modulo } n$$

Exemple : On veut chiffrer le nombre 7 avec du code RSA en utilisant la clé publique (3 , 33) , puis on va déchiffrer le nombre codé avec la clé privée (7 , 33) .

$m = 7$ on chiffre : $c = 7^3$ modulo 33 = 13

$c = 13$ on déchiffre : $m = 13^7$ modulo 33 = 7

Remarque : Le calcul de m^e peut rapidement dépasser la taille du type int (4 octets). Donc pour calculer m^e modulo n on utilisera plutôt une boucle :

```
c = 1
compteur = 0
tant que compteur < e :
   c = (c * m) % 26
   compteur = compteur + 1
retourner c
```

2.2 Le protocole sécurisé HTTPS

Principe :

- Le **client** (**navigateur**) effectue une **requête HTTPS** vers le **serveur**, en retour le **serveur** envoie sa **clé publique** (**KpuS**) au client.
- Le **client** "fabrique" une **clé symétrique** **K** (qui sera utilisée pour chiffrer les futurs échanges), chiffre cette clé **K** avec **KpuS** et envoie la version chiffrée de la clé **K** au **serveur**.
- Le **serveur** reçoit la version chiffrée de la clé **K** et la déchiffre en utilisant sa **clé privée** (**KprS**). À partir de ce moment-là, le client et le serveur sont en possession de la **clé symétrique** **K** .
- Le **client** et le **serveur** commencent à échanger des données en les chiffrant et en les déchiffrant à l'aide de la **clé symétrique** **K** .