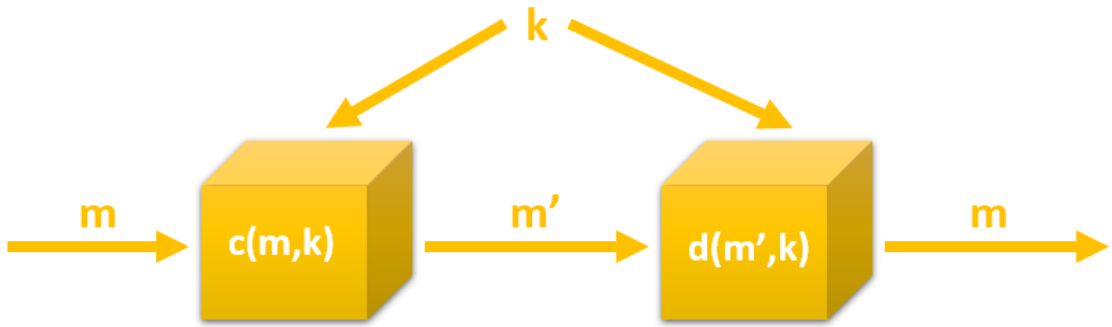
Sécurisation des communications

Terminale NSI - 2022

Cryptographie symétrique

- c(m,k) est la fonction de chiffrement
- m est un message
- k est une clé de chiffrement
- m’ est le message codé
- d(m’, k) est la fonction de déchiffrement

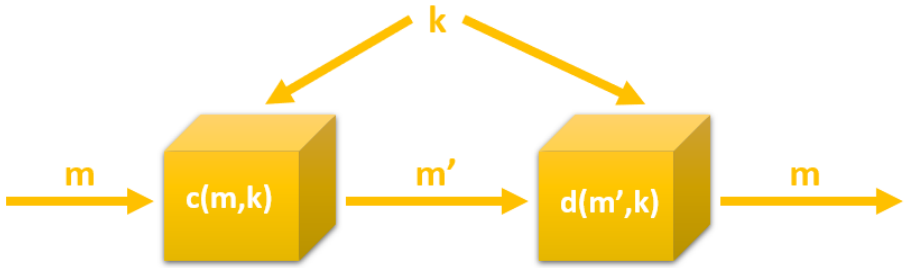


Cryptographie symétrique

OU exclusif (XOR)

Table de vérité de XOR		
A	**B**	**R = A ⊕ B**
0	0	0
0	1	1
1	0	1
1	1	0

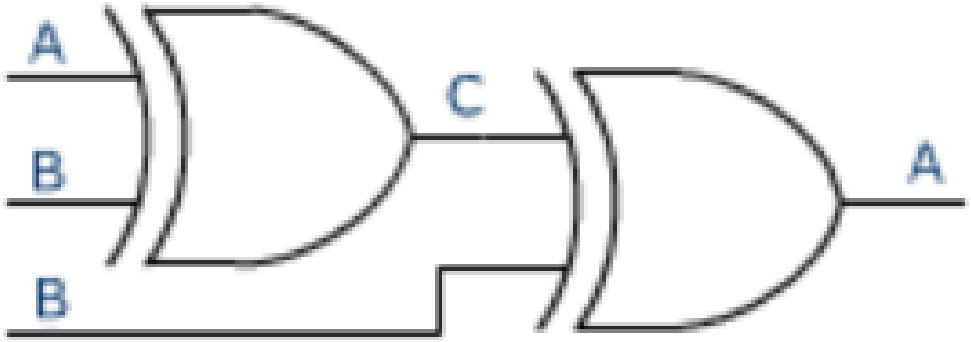
Cryptographie symétrique
OU exclusif (XOR)



A ⊕ B = C,

A ⊕ C = B,

B ⊕ C = A



Cryptographie symétrique
OU exclusif (XOR)

m = L'INFORMATIQUE
C'EST SUPER

k = NSI

c(m,k) =	L	`	I	N	F	O	R	M	A	T	I	Q	U	E		C	`	E	S	T		S	U	P	E	R			
	N	S	I	N	S	I	N	S	I	N	S	I	N	S	I	N	S	I	N	S	I	N	S	I	N	S	I	N	S
m' =	2	116	0	0	21	6	28	30	8	26	26	24	27	22	105	13	116	12	29	7	105	29	6	25	11	1			

Cryptographie symétrique
OU exclusif (XOR)

	01001100	76
⊕	01001110	78
---	---	---
	00000010	2

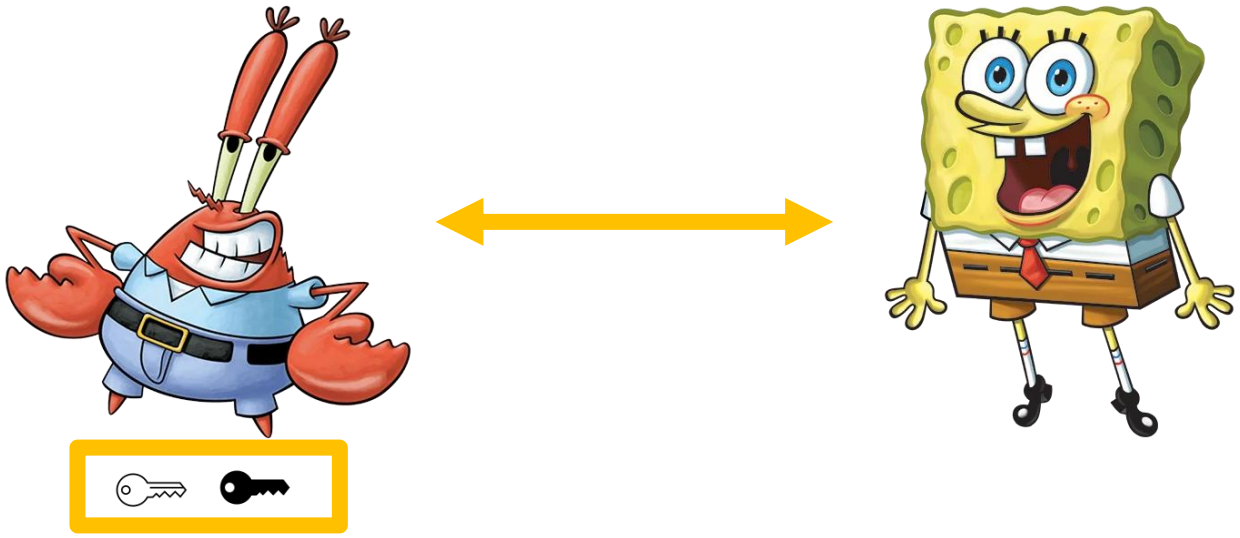
8	0	80	P	112	p
9	1	81	Q	113	q
0	2	82	R	114	r
1	3	83	S	115	s
2	4	84	T	116	t
3	5	85	U	117	u
4	6	86	V	118	v
5	7	87	W	119	w
6	8	88	X	120	x
7	9	89	Y	121	y
8	:	90	Z	122	z
9	;	91	[	123	{
0	<	92	\	124	|
1	=	93	]	125	}
2	>	94	^	126	~
3	?	95	_		

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o

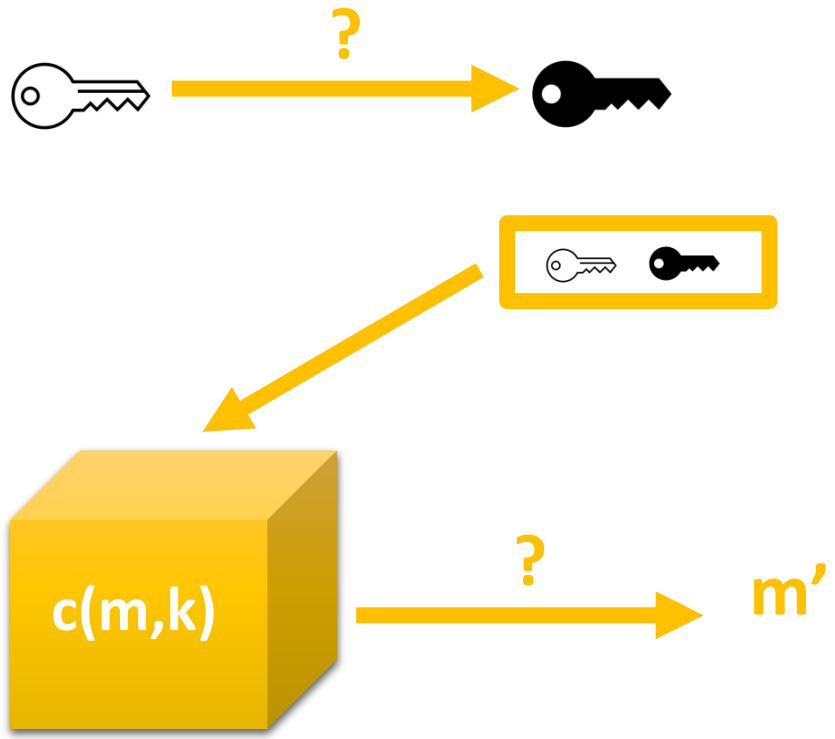
Cryptographie asymétrique
RSA

- Krabs et Bob veulent communiquer.
- Krabs possède une paire de clé publique et clé privée.



Cryptographie asymétrique
RSA

- En connaissant la clé publique de Krabs il est impossible de deviner sa clé privée.
- En connaissant soit le cryptage du message par la clé publique soit par la clé privée il est impossible de deviner le message.

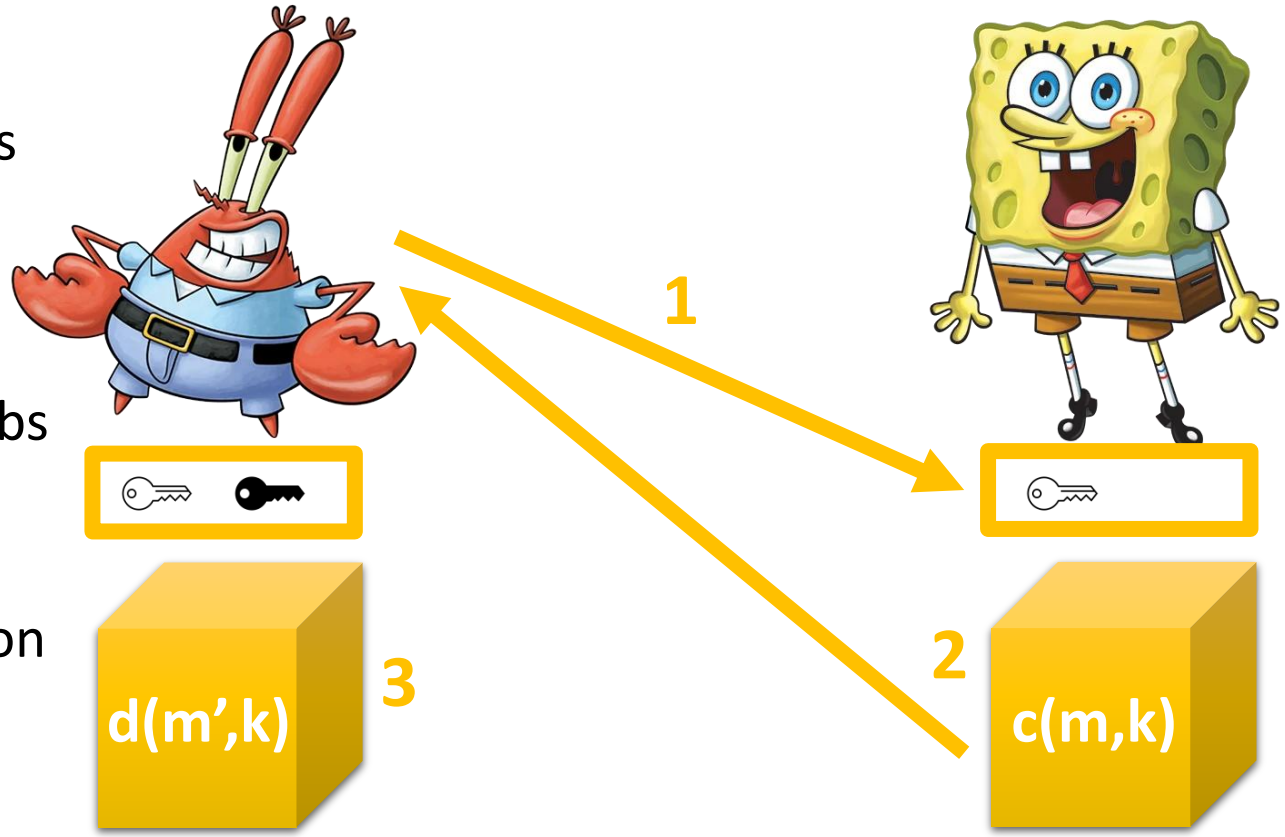


Cryptographie asymétrique
RSA

1. Krabs diffuse sa clé publique, mais garde sa clé privée.

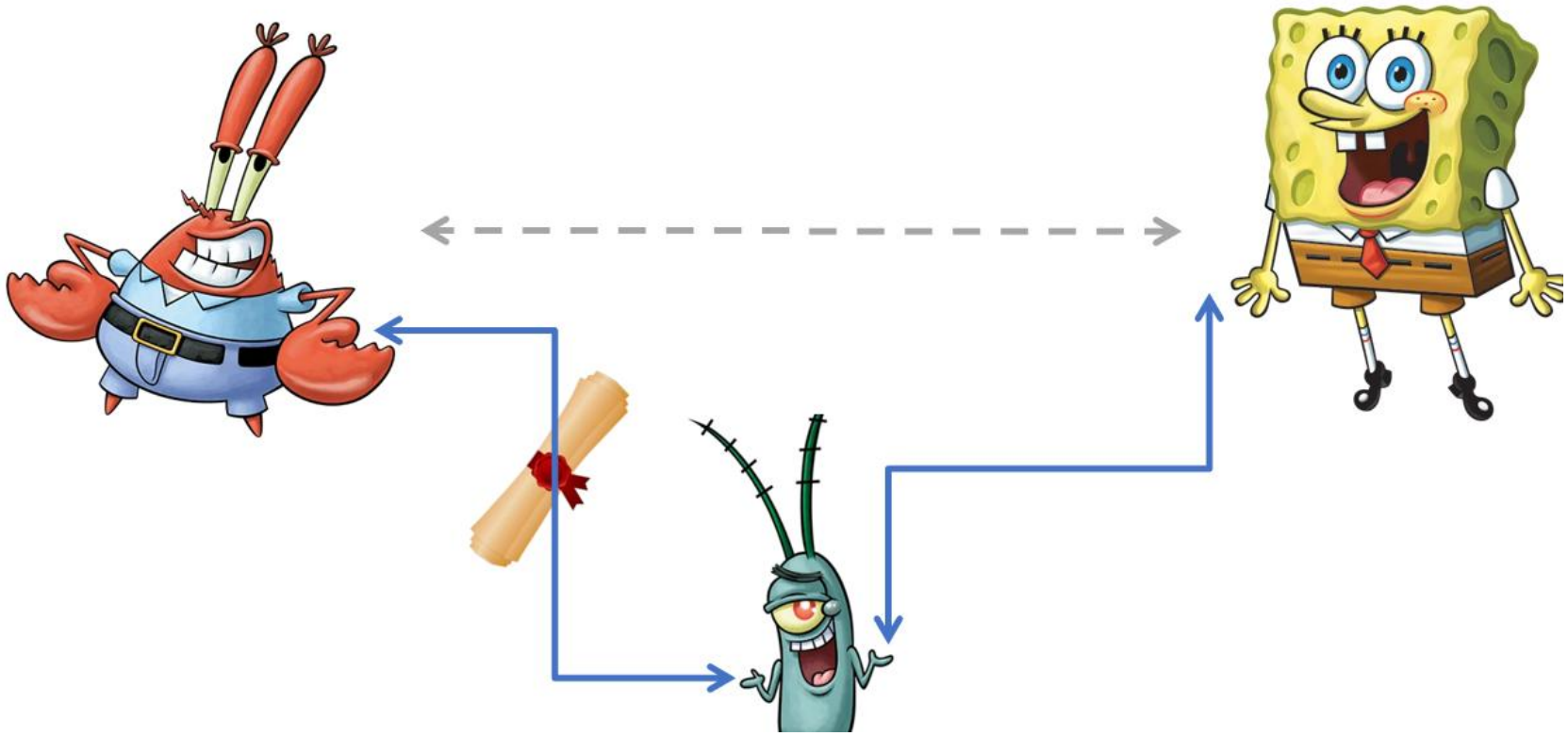
2. Bob chiffre son message en effectuant le chiffrement de son message avec la clé publique de Krabs et lui envoie.

3. Krabs applique sa clé privée au message chiffré pour retrouver le bon message.



Cryptographie asymétrique

Man In The Middle



Cryptographie asymétrique

Tiers de confiance

- S’assurer de l’identité de son correspondant.
- Tiers de confiance : Carlo.

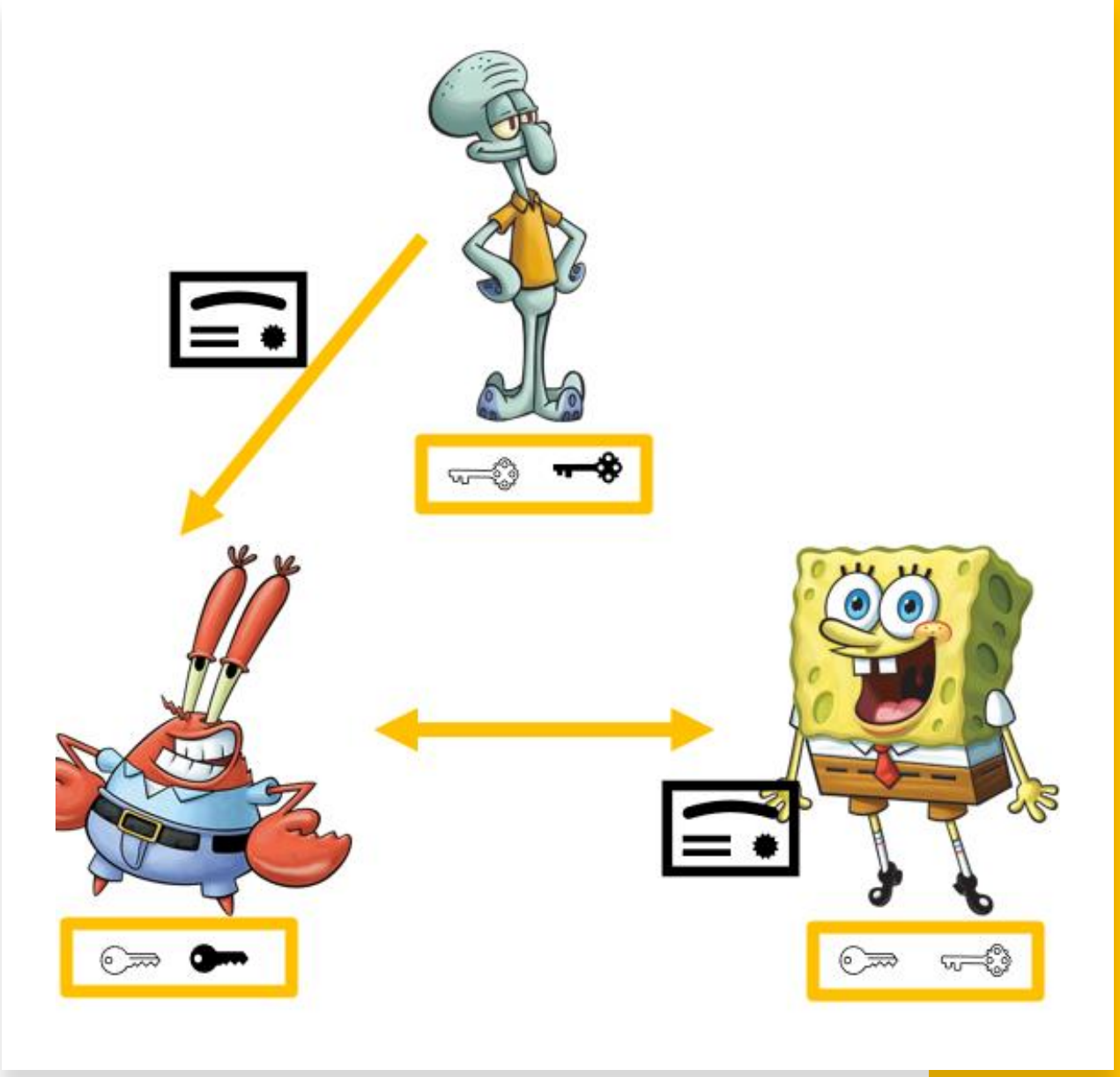
Cryptographie asymétrique
Certificat

1. Krabs va voir Carlo. Carlo vérifie que Krabs est bien le propriétaire du site leCrabeCroustillant.com. Carlo utilise sa clé privée pour chiffrer la clé publique de Krabs, qui obtient alors un certificat.

2. Bob veut se connecter au site. Lors de la connexion, le site lui fournit la clé publique de Krabs, ainsi que le certificat.

3. Bob récupère alors la clé publique de Carlo, en qui il a confiance.

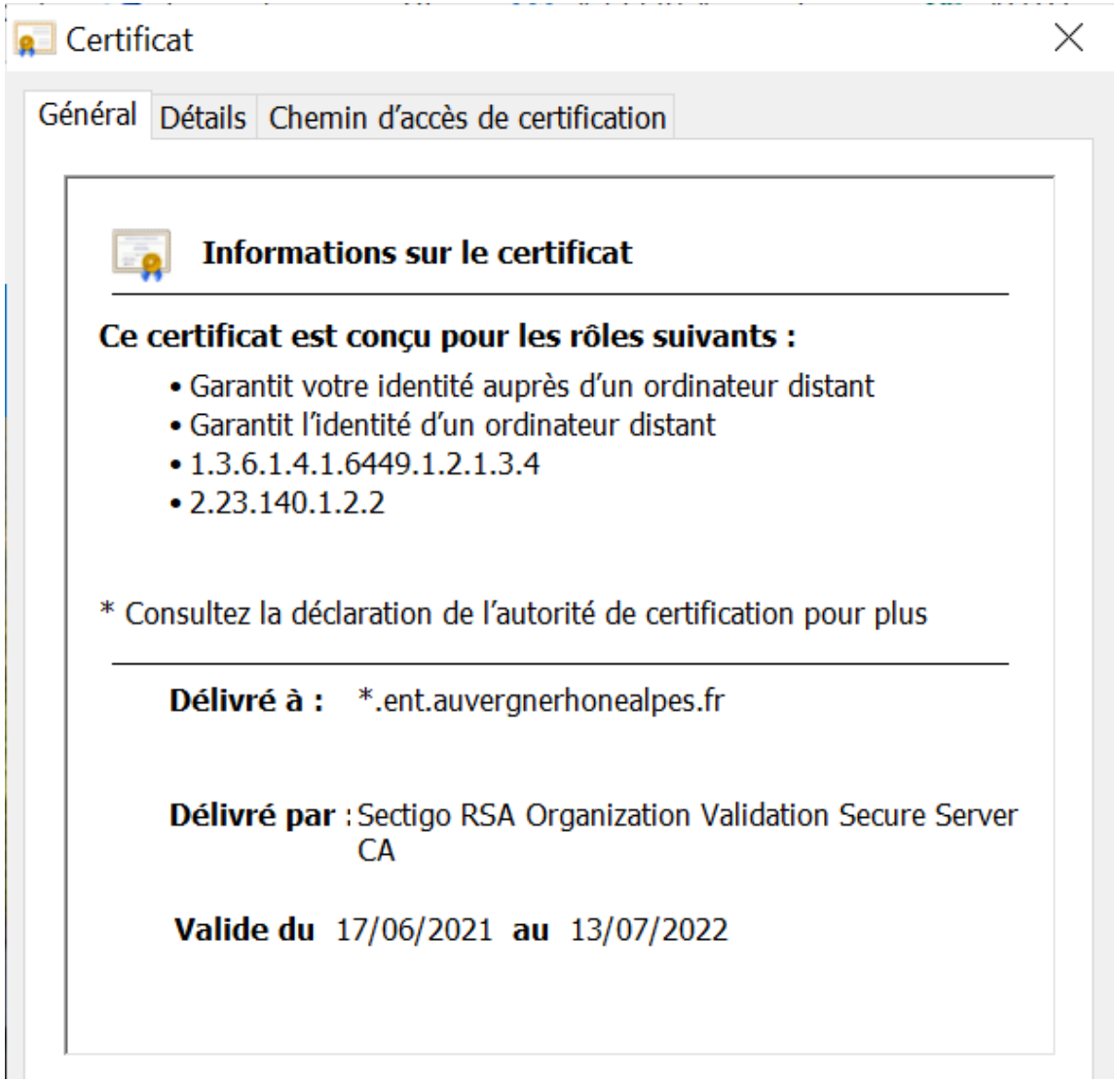
4. Bob ayant authentifié leCrabeCroustillant.com comme étant bien le site détenu par Krabs, il peut initier avec lui une communication sécurisée.



HTTPS

Autorités de certifications (AC)

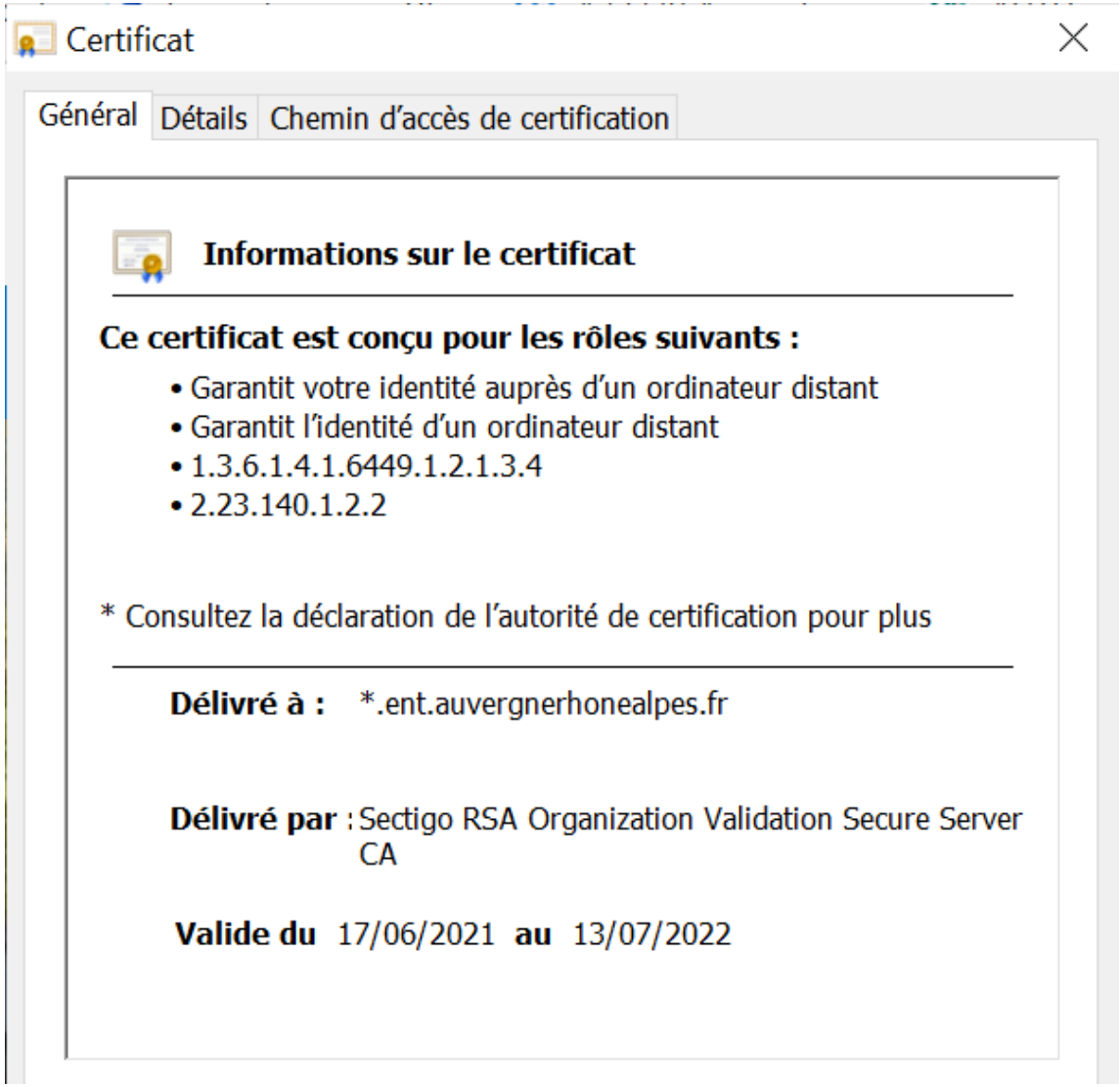
- Des entreprises spécialisées
- Des associations à but non lucratif
- Des états.



HTTPS
Format X.509

Format de fichier binaire:

- L'identifiant de l'AC qui signe le certificat
- L'identifiant de l'entité certifiée
- La date de validité du certificat
- La clé publique de l'entité certifiée
- L'algorithme utilisé pour la signature du certificat
- La signature du certificat par l'AC.



HTTPS
Principe

- HTTP + TLS

Etape 1: Le client envoi un message initial ainsi que des options (algorithmes cryptographiques).

Etape 2: Le serveur envoie sa réponse, contenant le certificat contenant sa clé publique, signée par une autorité de certification.

Etape 3: Le client vérifie le certificat au moyen de la clé publique de l'AC.

Etape 4: Le client et le serveur conviennent d'une clé de session pour un algorithme symétrique.

Etape 5: Le serveur est authentifié par le client, et les deux ont convenu d'une clé de session.