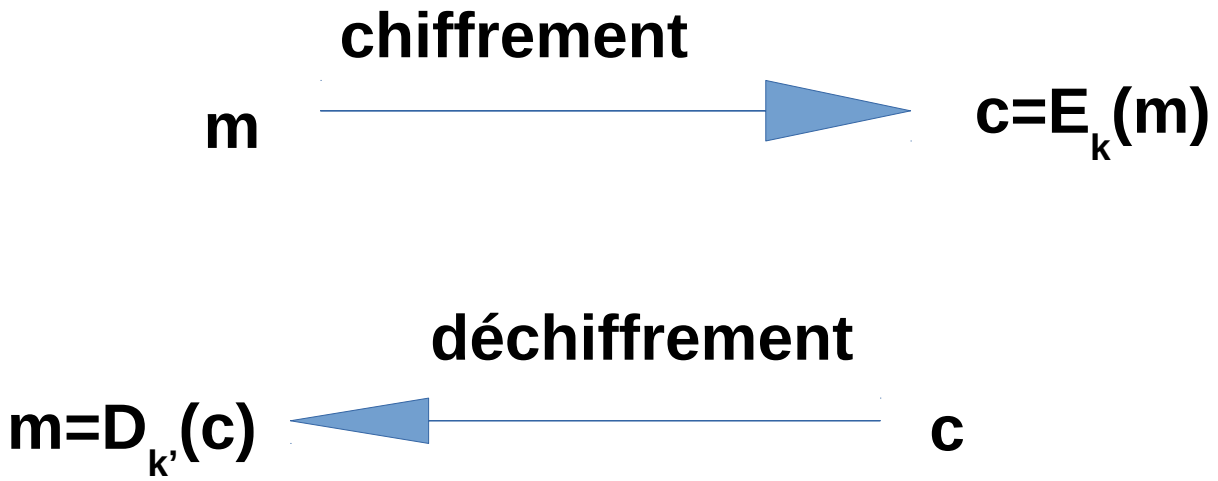
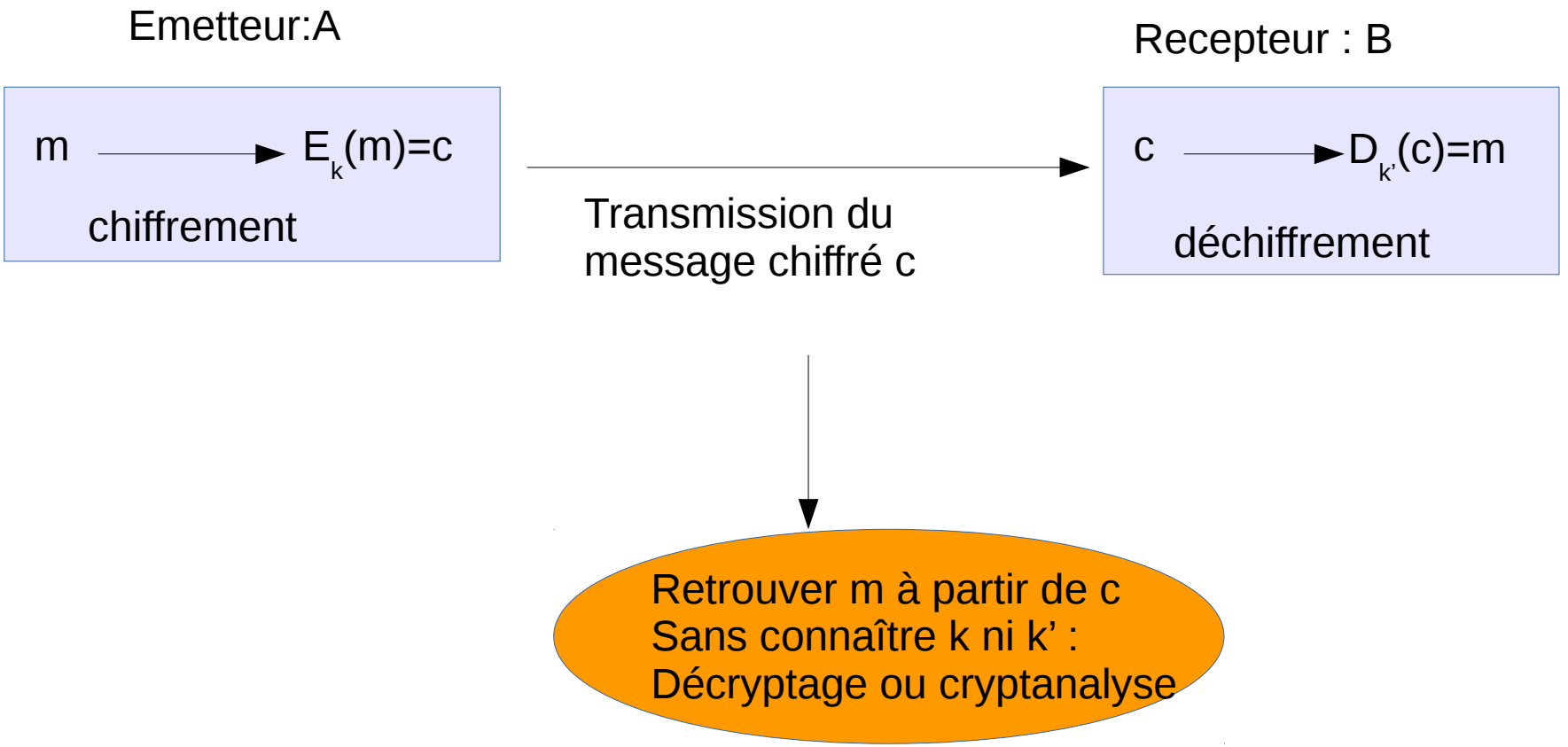
Cryptographie

m= message en clair (un mot français, un texte, une suite de lettres, un mot binaire, un entier…)



c=message chiffré

Cryptographie



Cryptographie

- On fait la distinction entre l'algorithme de chiffrement et sa clé (principe de Kerckhoffs).
- La sécurité du chiffrement en cryptographie repose sur la clé (la clé secrète en cryptographie symétrique, la clé privée en cryptographie asymétrique)

Cryptographie symétrique et cryptographie asymétrique

- Exemple : **le chiffrement de César**

  m est un mot de la langue française ; **c** est le mot obtenu en remplaçant chaque lettre par la lettre située 3 rangs plus loin dans l'ordre alphabétique. Par exemple **m= CRYPTO** devient **c=FUBSWR**

  k=3 est la clé de chiffrement. C'est aussi la clé de déchiffrement (**k'=3**)

- **Si k=k' : cryptographie symétrique.** La clé k ne doit être connue que de l'emetteur et du recepteur.
- **Si k≠k':cryptographie asymétrique** :
  - k est la **clé publique** (connue de tous les emetteurs potentiels vers un même recepteur A)
  - k' est la **clé privée** connue uniquement du recepteur A considéré

Cryptographie symétrique : Vigénère

A	B	C	D	E	F	G	H	I	J	K	L	M	N	0	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

k=CRYPTO

m	M	A	T	H	E	M	A	T	I	Q	U	E	S
u	12	0	19	7	4	12	0	19	8	16	20	4	18
k	C	R	Y	P	T	0	C	R	Y	P	T	O	C
v	2	17	24	15	19	14	2	17	24	15	19	14	2
u+v	14	17	17	22	23	0	2	10	6	5	13	18	20
c	O	R	R	W	X	A	C	K	G	F	N	S	U

$\mathbb{Z}/26\mathbb{Z}$

Limites de la cryptographie symétrique

- 1) problème de l'échange des clés secrètes
- 2) nombre important de clés (n(n-1)/2 dans un réseau de n personnes)
- 3) déterminisme : un message m est toujours chiffré de la même façon.

(RSA permet de résoudre 1 et 2.

El Gamal permet de résoudre aussi le point 3)

Cryptographie asymétrique

- La clé de chiffrement k est publique
- La clé de déchiffrement k’ est secrète
- $D_{k'}$ « impossible » à trouver à partir de E_k
- Pour l’algorithme de chiffrement RSA :

$$\mathbf{(p,q)} \xrightarrow{\mathbf{f}} \mathbf{n=pq}$$

Pour **p** et **q** deux nombres premiers « très grands », $\mathbf{f^{-1}}$ est trop long à calculer