Introduction à la cryptographie

Alice Pellet--Mary

ENS de Lyon
LIP

30 Mai, 2018

Qu'est-ce que la cryptographie ?

Définition (Wikipédia)

La **cryptographie** est une discipline s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou *clés*.

Applications

Qu'est-ce que la cryptographie ?

Définition (Wikipédia)

La **cryptographie** est une discipline s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou *clés*.

Applications

- Espionnage, armée...

Qu'est-ce que la cryptographie ?

Définition (Wikipédia)

La **cryptographie** est une discipline s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou *clés*.

Applications

- Espionnage, armée...
- Payements sécurisés sur Internet, communications par mail...

Qu'est-ce que la cryptographie ?

Définition (Wikipédia)

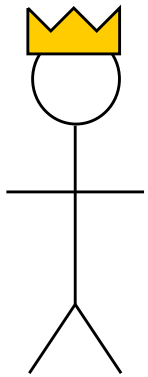
La **cryptographie** est une discipline s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou *clés*.

Applications

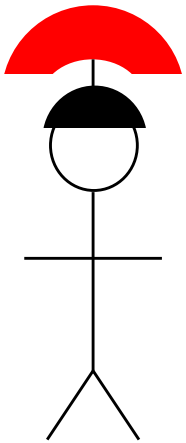
- Espionnage, armée...
- Payements sécurisés sur Internet, communications par mail...
- Vote électronique.
- ...

Plan

Contexte (fictif)

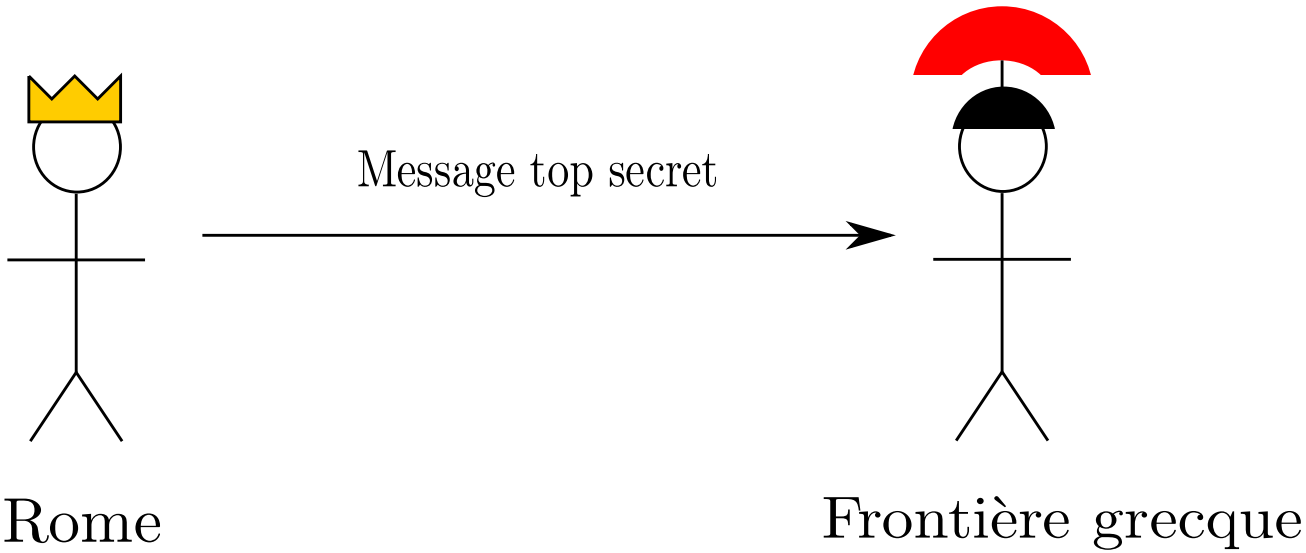


Rome

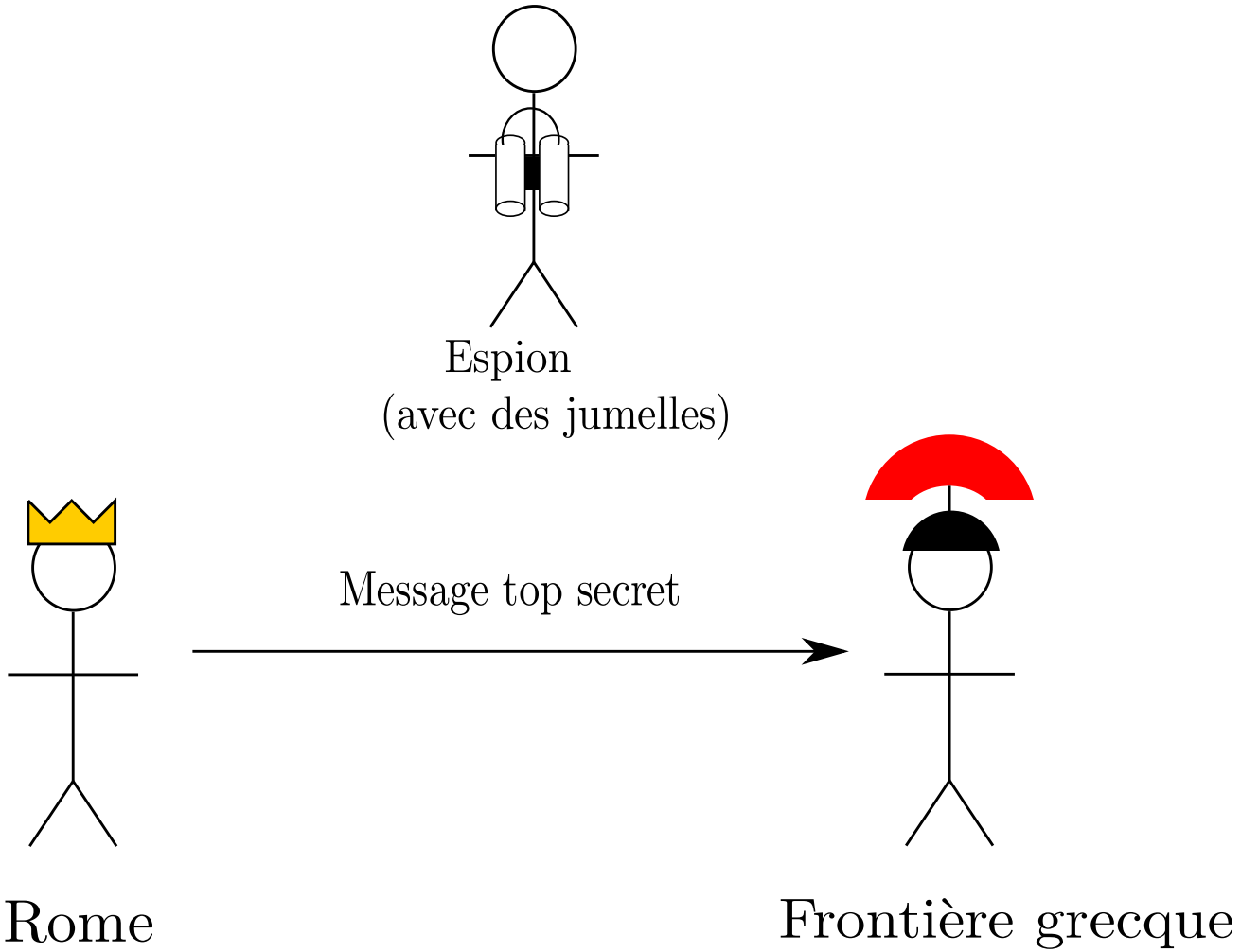


Frontière grecque

Contexte (fictif)



Contexte (fictif)



Chiffrement de César

Idée

Décaler toutes les lettres de l'alphabet de 3.

Lettre d'origine	a	b	c	d	e	f	g	h	i	j	k	l	m
Lettre après décalage	d	e	f	g	h	i	j	k	l	m	n	o	p

Lettre d'origine	n	o	p	q	r	s	t	u	v	w	x	y	z
Lettre après décalage	q	r	s	t	u	v	w	x	y	z	a	b	c

Chiffrement de César

Idée

Décaler toutes les lettres de l'alphabet de 3.

Lettre d'origine	a	b	c	d	e	f	g	h	i	j	k	l	m
Lettre après décalage	d	e	f	g	h	i	j	k	l	m	n	o	p

Lettre d'origine	n	o	p	q	r	s	t	u	v	w	x	y	z
Lettre après décalage	q	r	s	t	u	v	w	x	y	z	a	b	c

Exemple :

A v e C e s a r

Chiffrement de César

Idée

Décaler toutes les lettres de l'alphabet de 3.

Lettre d'origine	a	b	c	d	e	f	g	h	i	j	k	l	m
Lettre après décalage	d	e	f	g	h	i	j	k	l	m	n	o	p

Lettre d'origine	n	o	p	q	r	s	t	u	v	w	x	y	z
Lettre après décalage	q	r	s	t	u	v	w	x	y	z	a	b	c

Exemple :

A v e C e s a r
D

Chiffrement de César

Idée

Décaler toutes les lettres de l'alphabet de 3.

Lettre d'origine	a	b	c	d	e	f	g	h	i	j	k	l	m
Lettre après décalage	d	e	f	g	h	i	j	k	l	m	n	o	p

Lettre d'origine	n	o	p	q	r	s	t	u	v	w	x	y	z
Lettre après décalage	q	r	s	t	u	v	w	x	y	z	a	b	c

Exemple :

A v e C e s a r
D y

Chiffrement de César

Idée

Décaler toutes les lettres de l'alphabet de 3.

Lettre d'origine	a	b	c	d	e	f	g	h	i	j	k	l	m
Lettre après décalage	d	e	f	g	h	i	j	k	l	m	n	o	p

Lettre d'origine	n	o	p	q	r	s	t	u	v	w	x	y	z
Lettre après décalage	q	r	s	t	u	v	w	x	y	z	a	b	c

Exemple :

A v e C e s a r
D y h

Chiffrement de César

Idée

Décaler toutes les lettres de l'alphabet de 3.

Lettre d'origine	a	b	c	d	e	f	g	h	i	j	k	l	m
Lettre après décalage	d	e	f	g	h	i	j	k	l	m	n	o	p

Lettre d'origine	n	o	p	q	r	s	t	u	v	w	x	y	z
Lettre après décalage	q	r	s	t	u	v	w	x	y	z	a	b	c

Exemple :

A	v	e		C	e	s	a	r
D	y	h		F	h	v	d	u

Chiffrement de César

Idée

Décaler toutes les lettres de l'alphabet de 3.

Lettre d'origine	a	b	c	d	e	f	g	h	i	j	k	l	m
Lettre après décalage	d	e	f	g	h	i	j	k	l	m	n	o	p

Lettre d'origine	n	o	p	q	r	s	t	u	v	w	x	y	z
Lettre après décalage	q	r	s	t	u	v	w	x	y	z	a	b	c

Challenge :

D w w d t x h g h p d l q

Chiffrement de César

Idée

Décaler toutes les lettres de l'alphabet de 3.

Lettre d'origine	a	b	c	d	e	f	g	h	i	j	k	l	m
Lettre après décalage	d	e	f	g	h	i	j	k	l	m	n	o	p

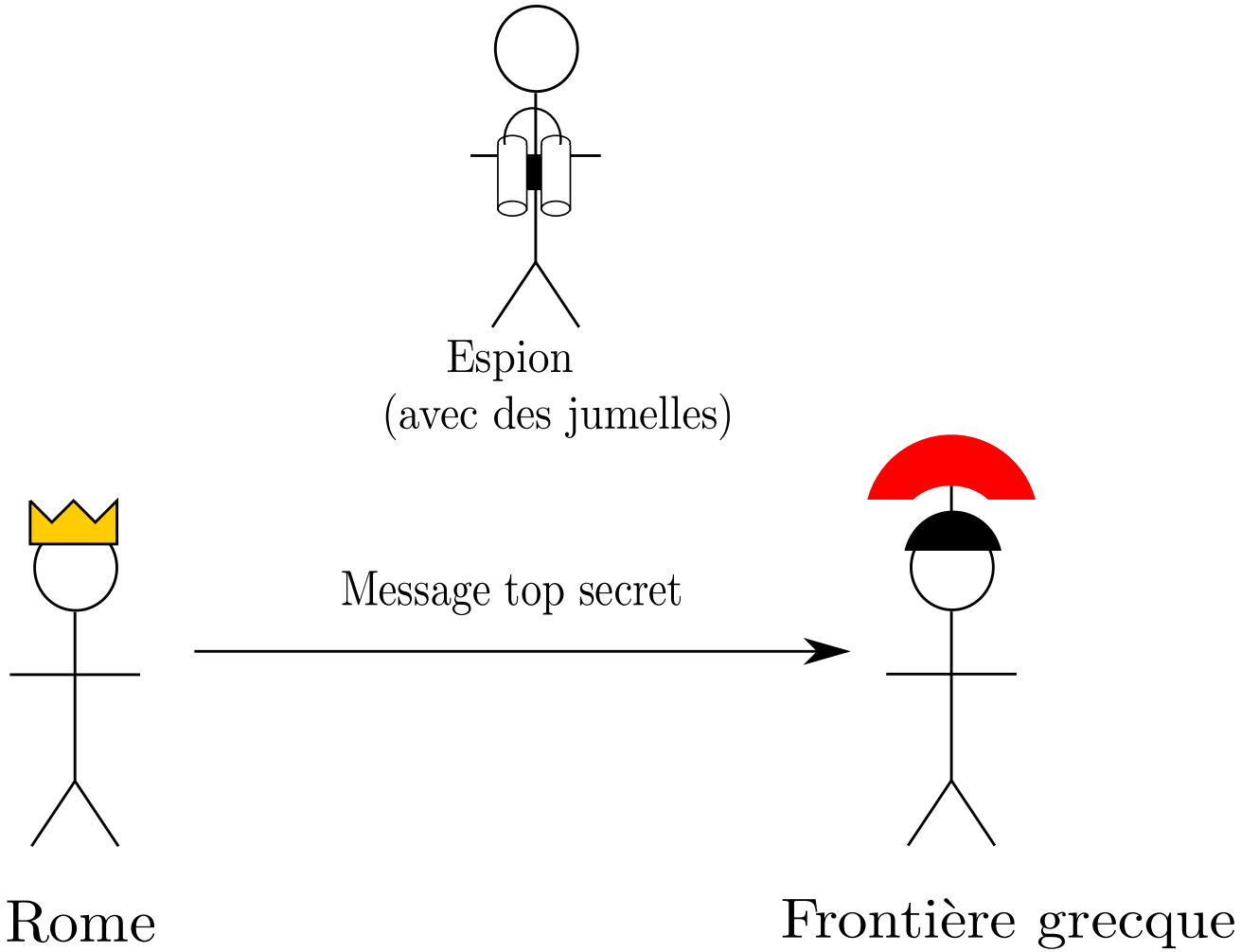
Lettre d'origine	n	o	p	q	r	s	t	u	v	w	x	y	z
Lettre après décalage	q	r	s	t	u	v	w	x	y	z	a	b	c

Challenge :

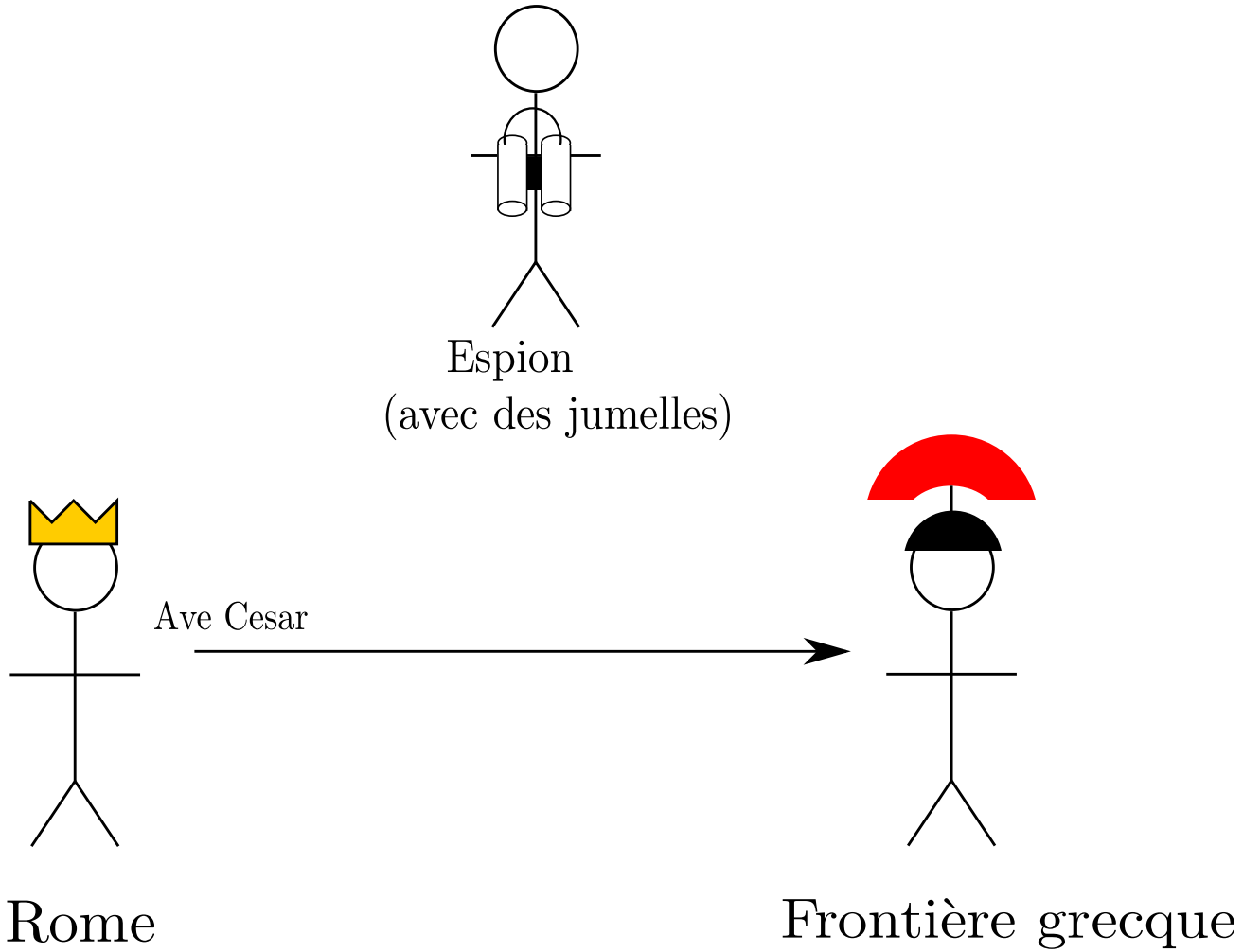
D w w d t x h g h p d l q

A t t a q u e d e m a i n

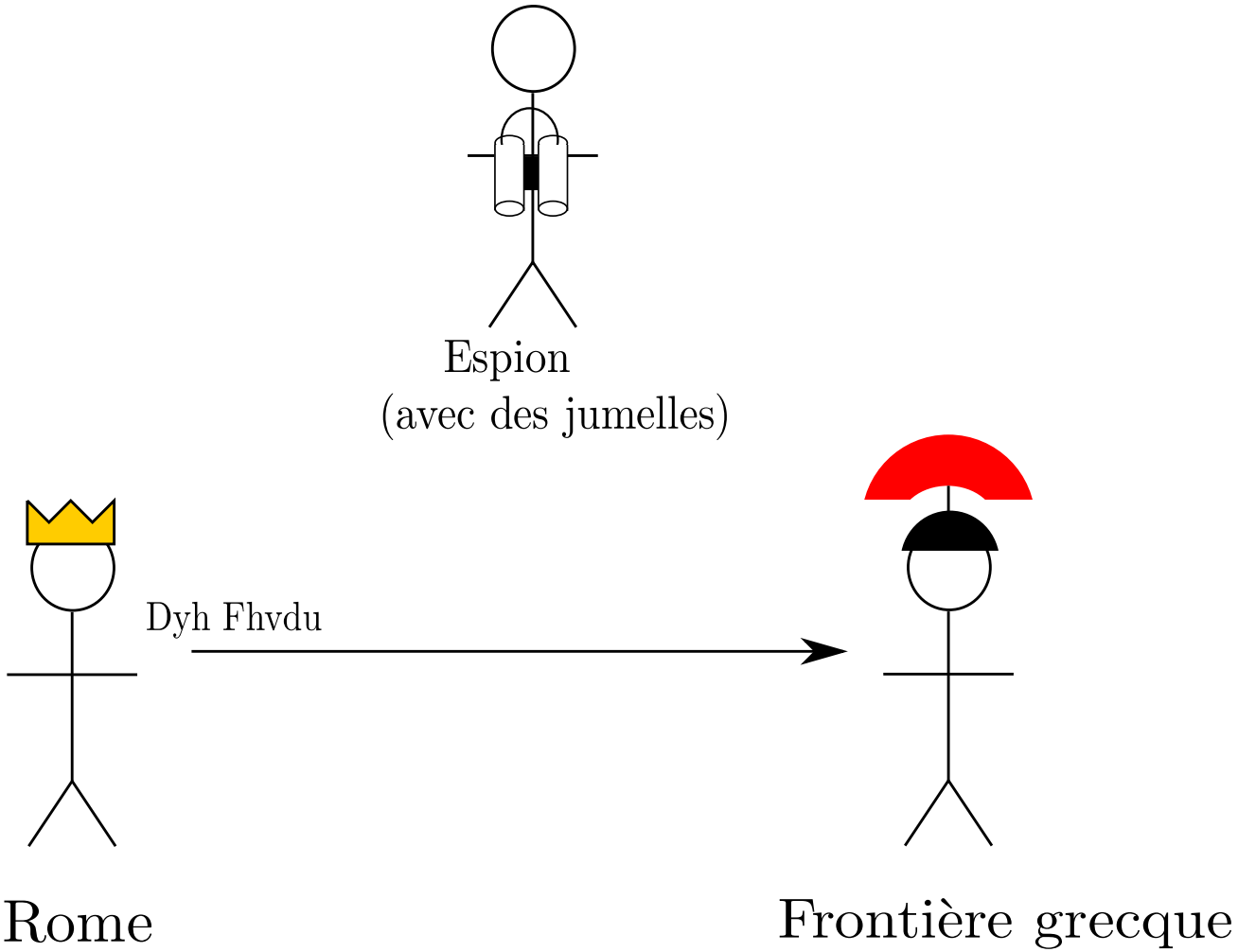
Retour à l'histoire



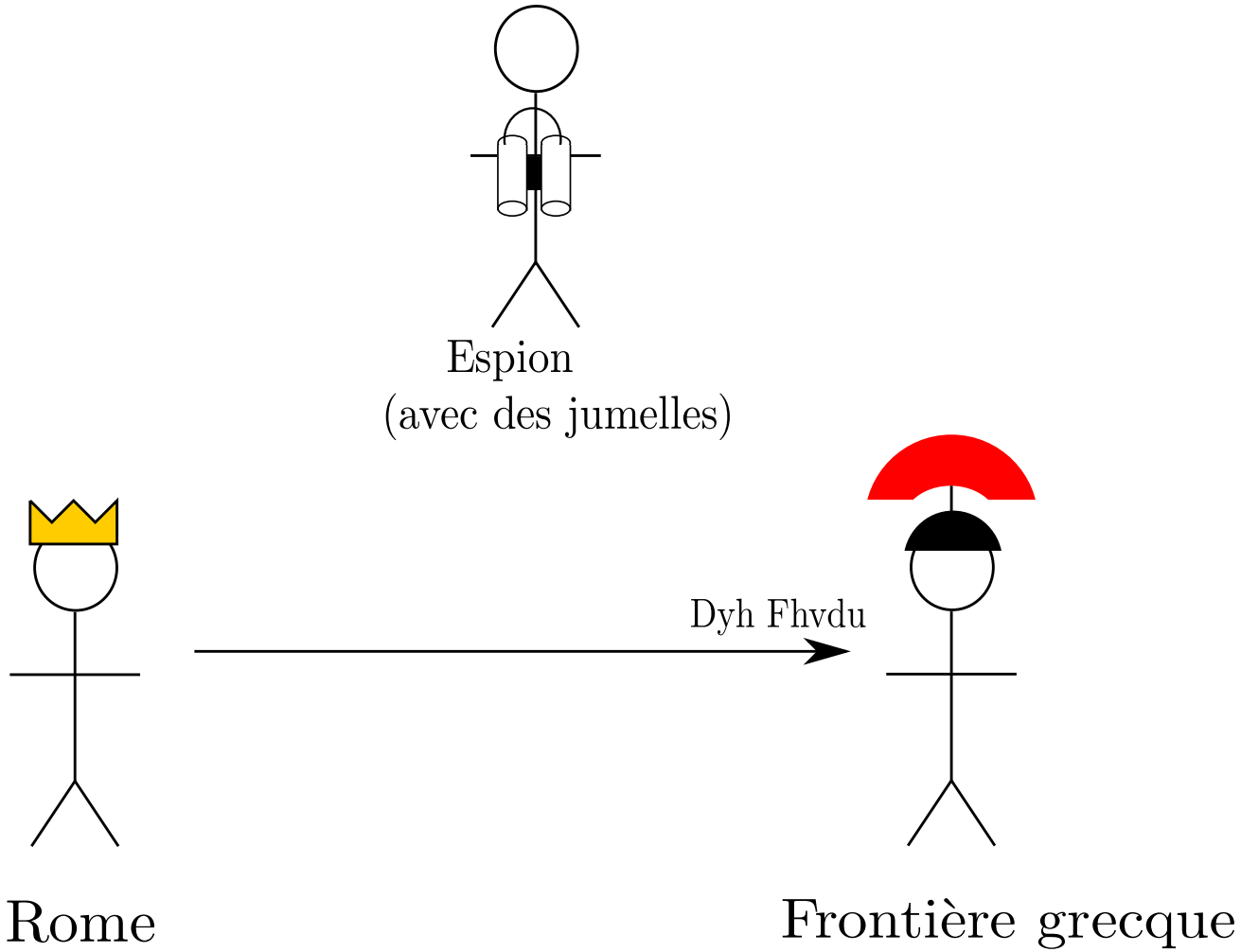
Retour à l'histoire



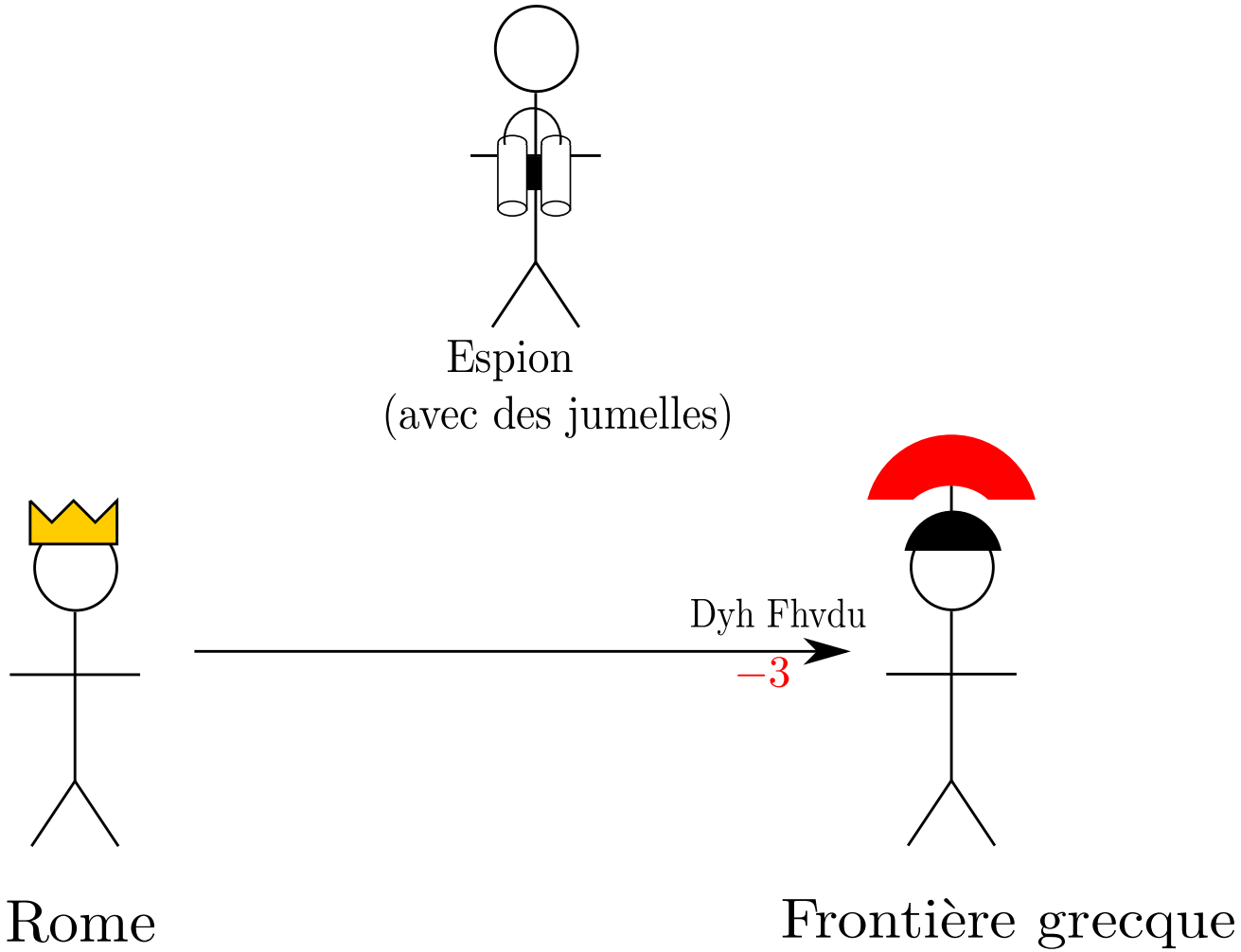
Retour à l'histoire



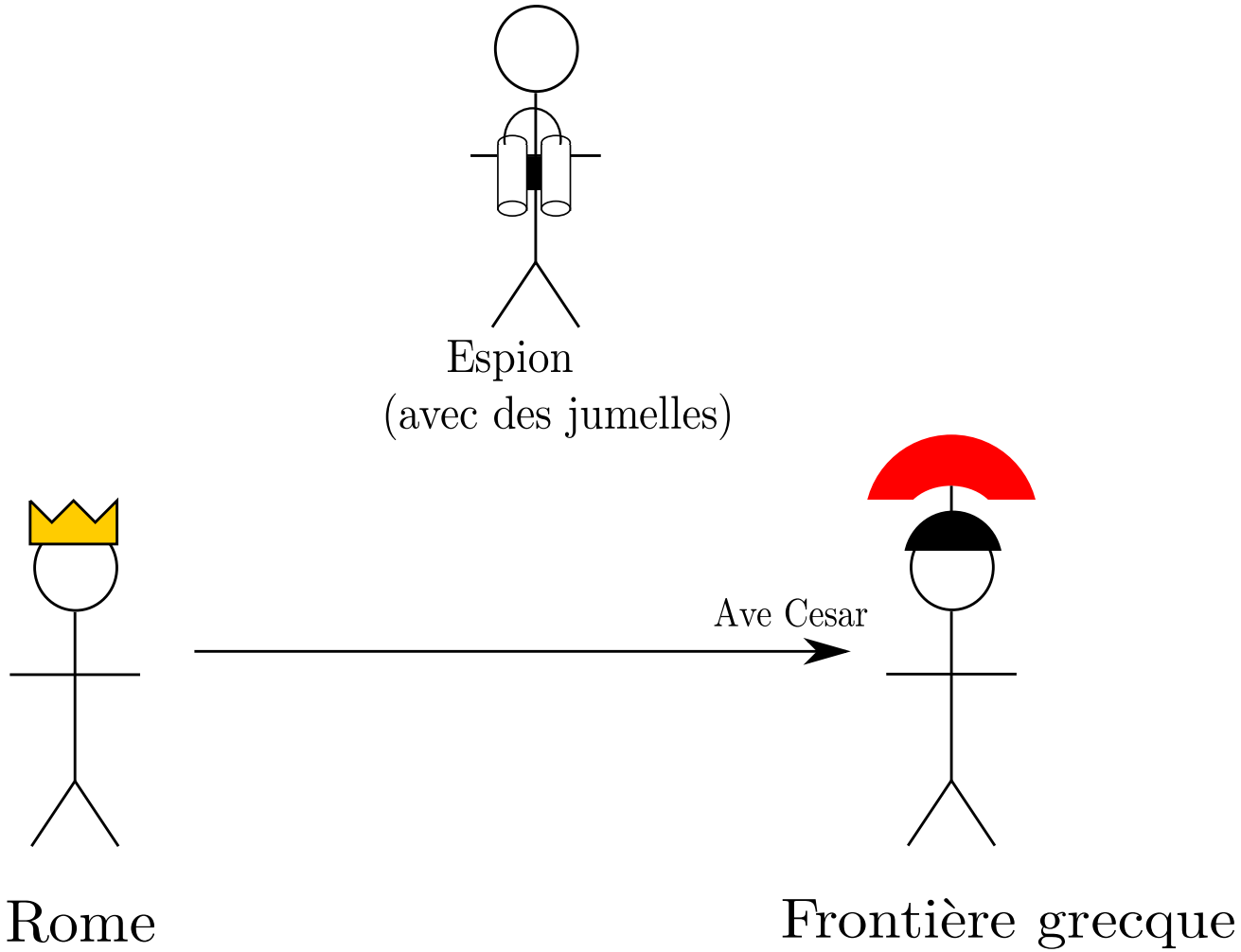
Retour à l'histoire



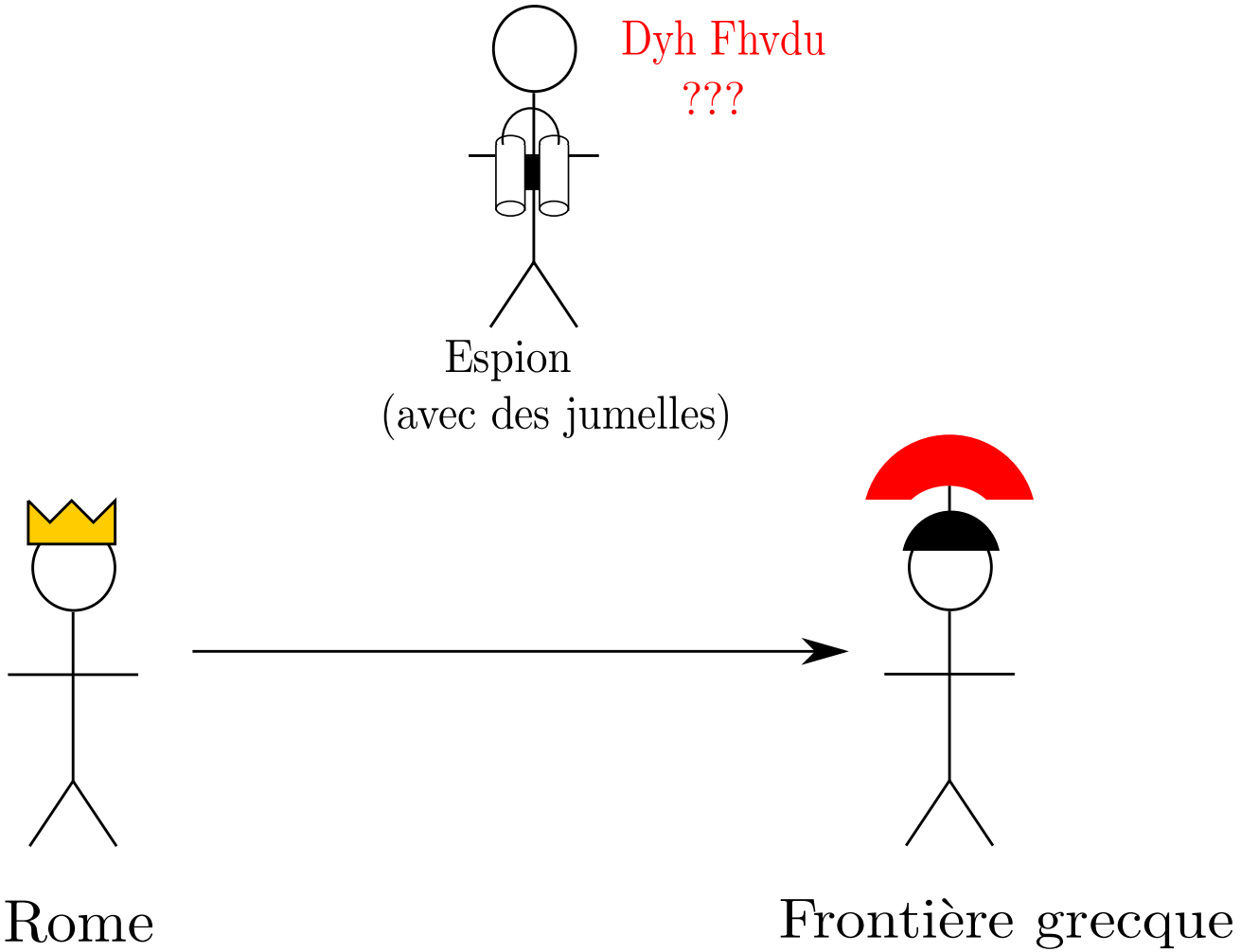
Retour à l'histoire



Retour à l'histoire



Retour à l'histoire



Oui mais...

Problème

Et si un jour un espion grec découvre le principe ? Faut-il reconstruire un nouveau code secret ?

Oui mais...

Problème

Et si un jour un espion grec découvre le principe ? Faut-il reconstruire un nouveau code secret ?

Non. On peut simplement changer le décalage. Par exemple, décaler de 7 lettres au lieu de 3.

Oui mais...

Problème

Et si un jour un espion grec découvre le principe ? Faut-il reconstruire un nouveau code secret ?

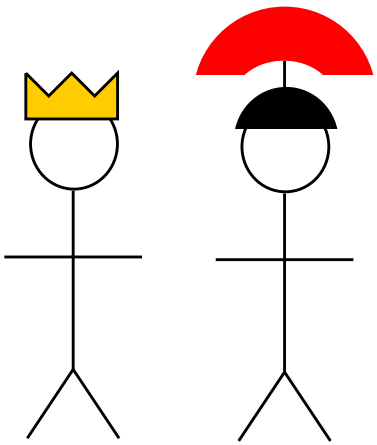
Non. On peut simplement changer le décalage. Par exemple, décaler de 7 lettres au lieu de 3.

Nouveau protocole

César et son général choisissent un entier k entre 1 et 25. Cet entier k est appelé *clé secrète*. Ils décalent ensuite les lettres de k positions pour chiffrer leurs messages.

Même si les Grecs connaissent le protocole, tant qu'ils ne connaissent pas la clé secrète k, ils ne peuvent pas déchiffrer les messages chiffrés.

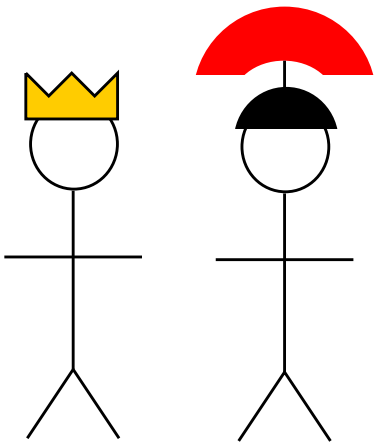
Retour à l'histoire



Rome

Frontière grecque

Retour à l'histoire

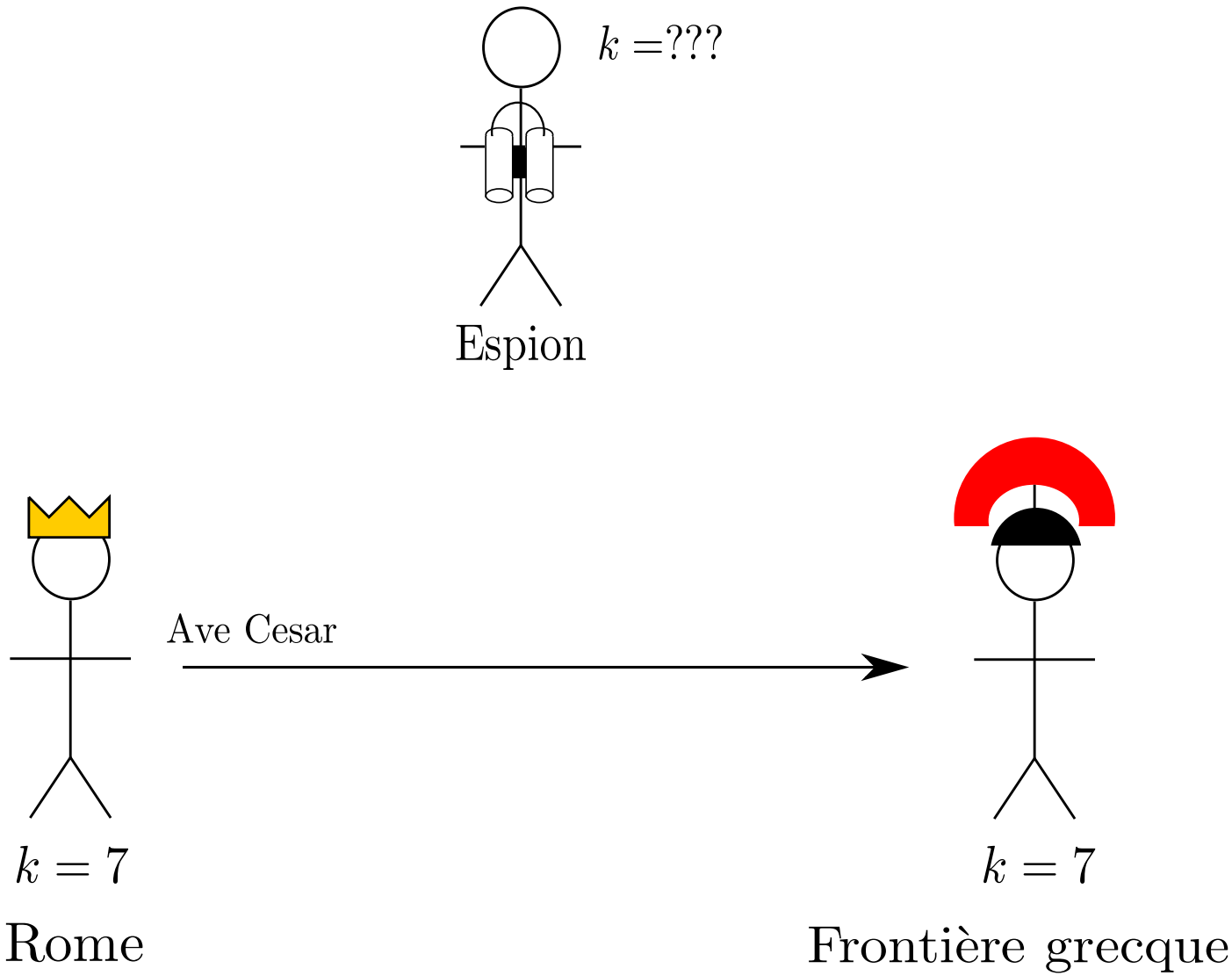


$k = 7$

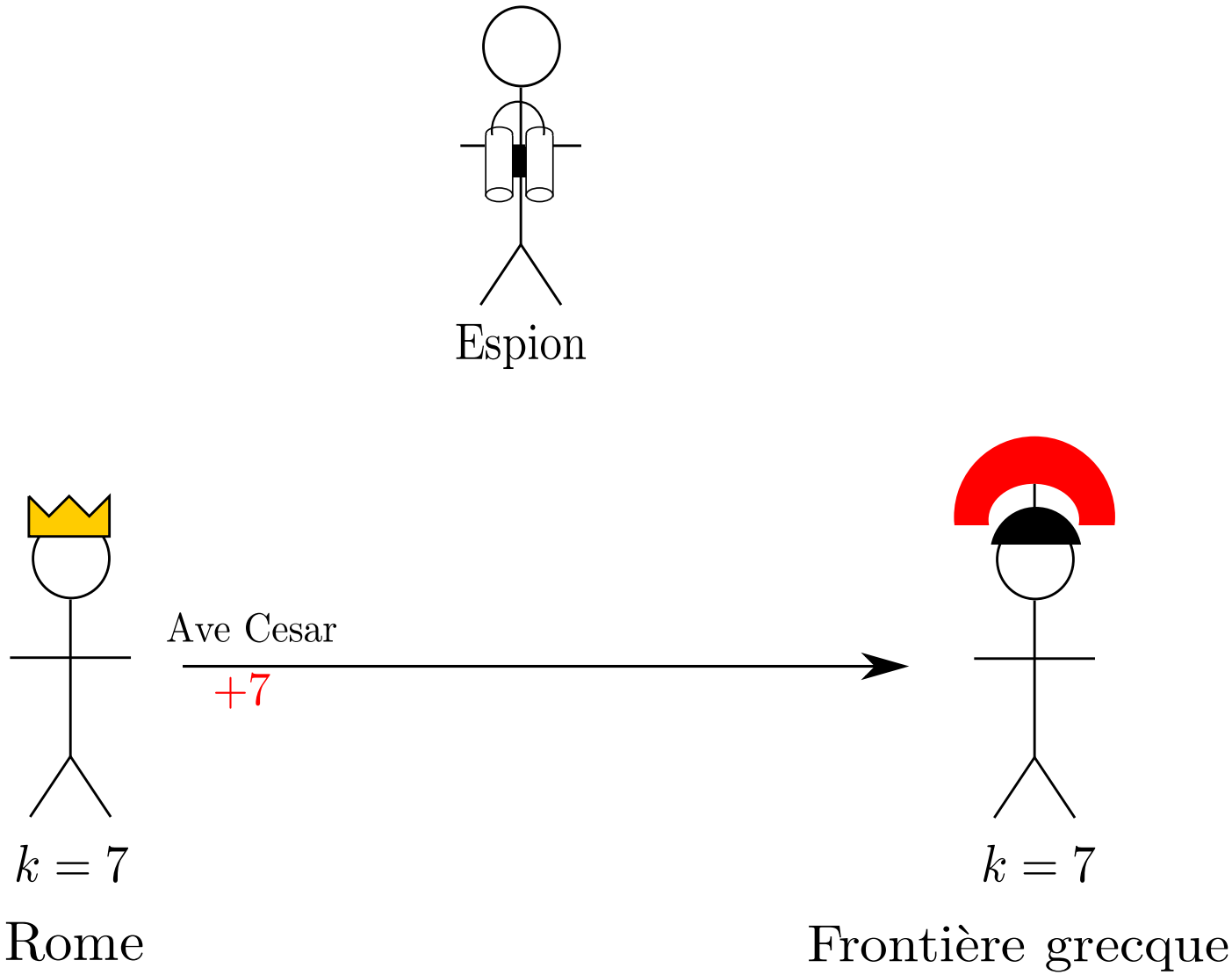
Rome

Frontière grecque

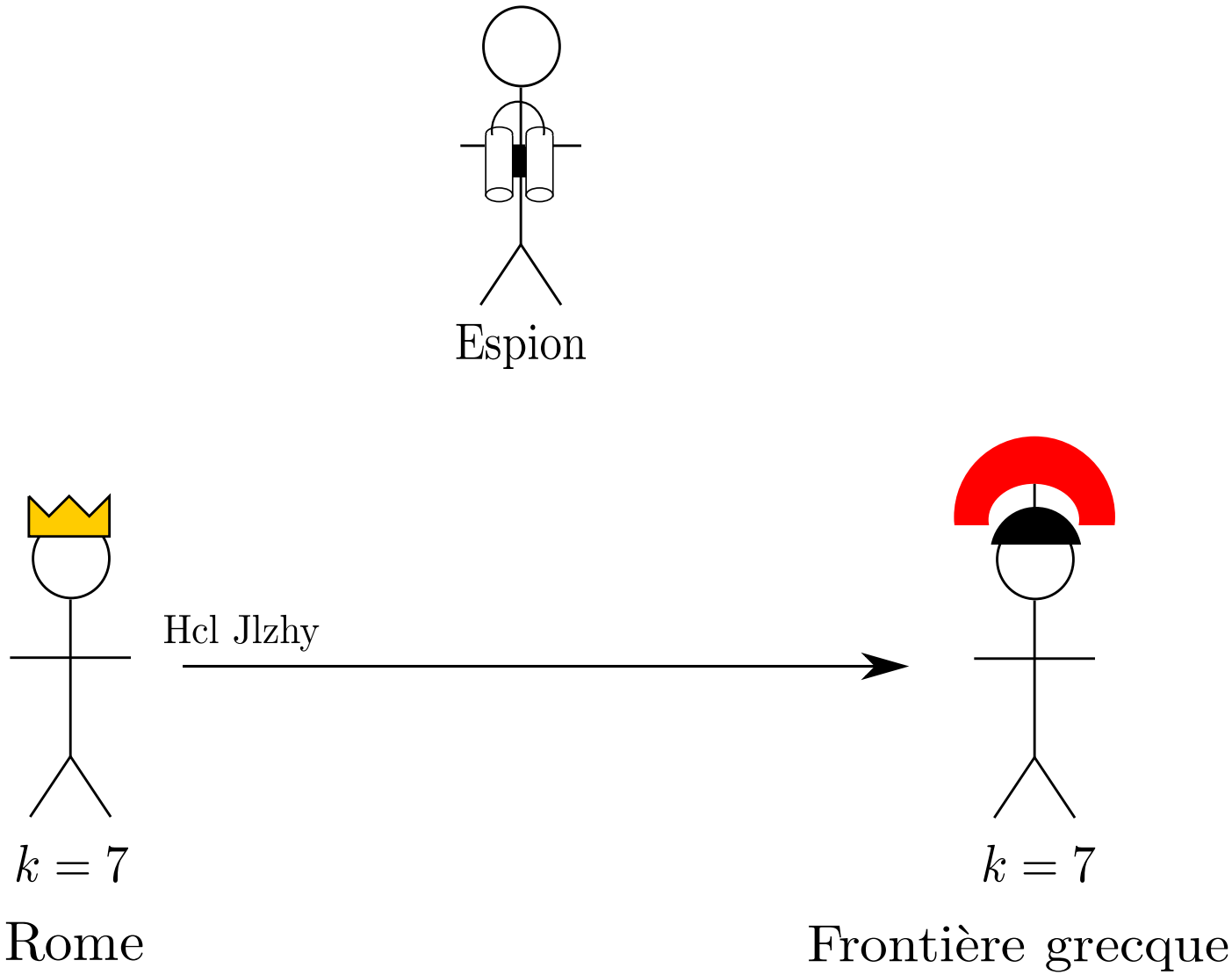
Retour à l'histoire



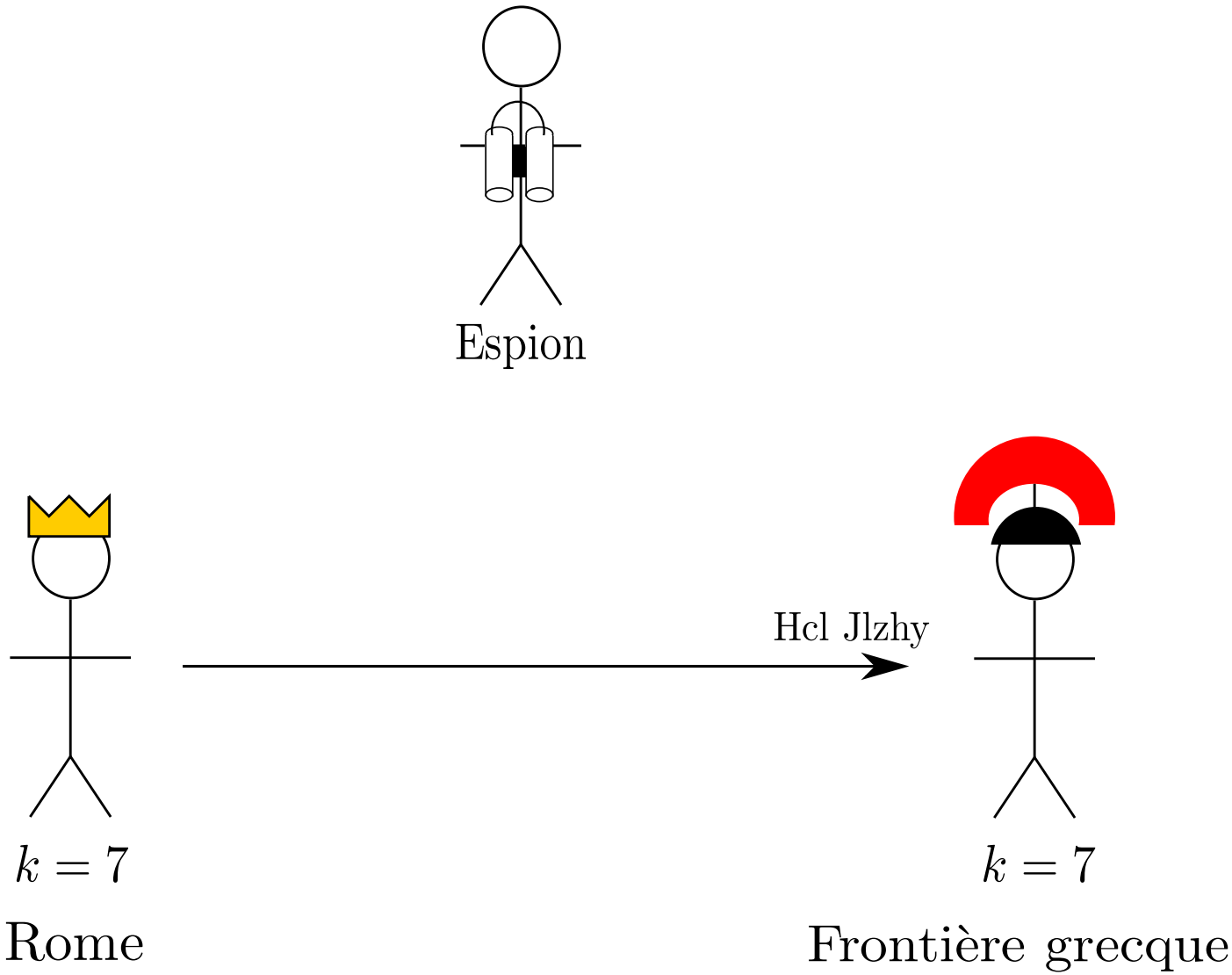
Retour à l'histoire



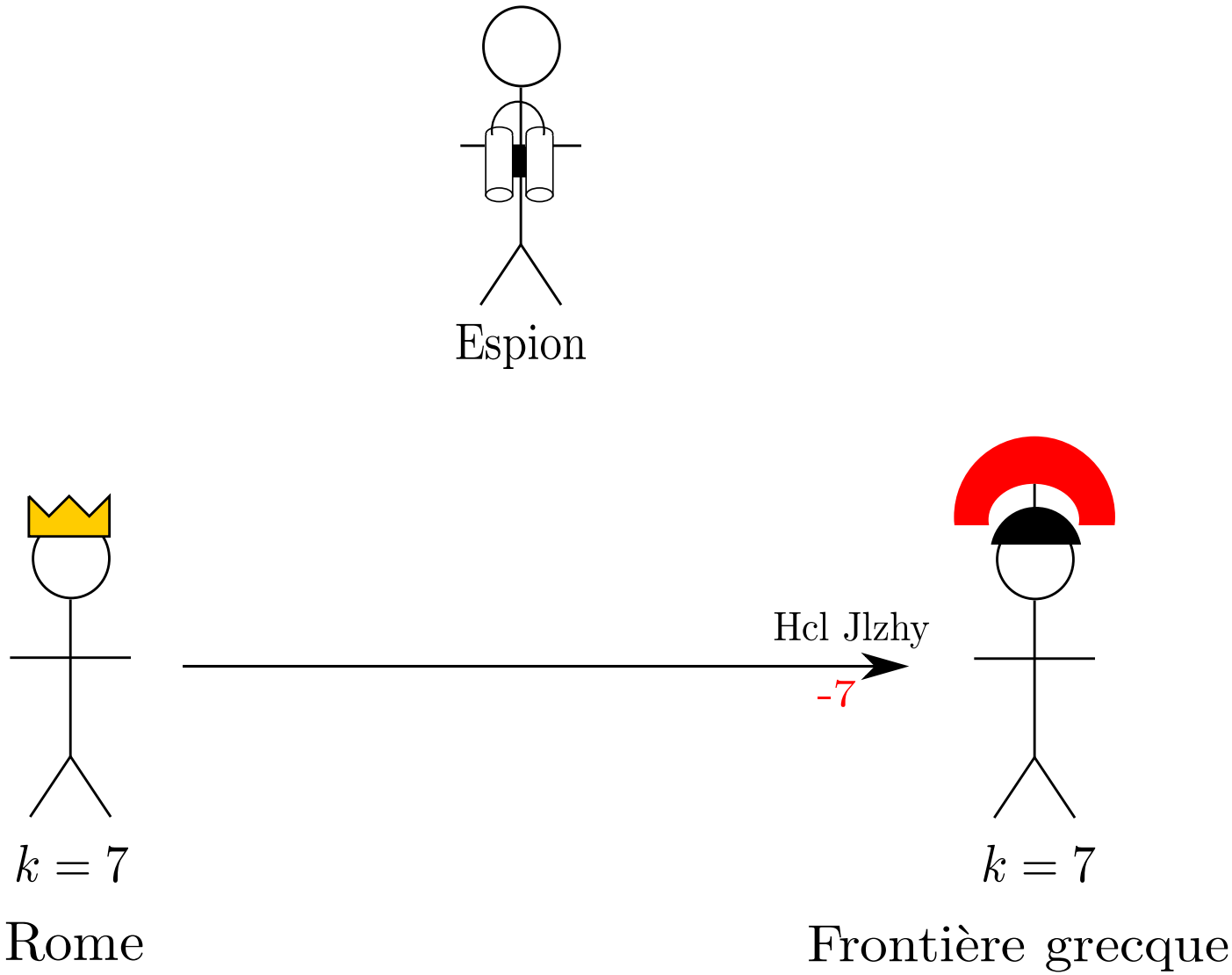
Retour à l'histoire



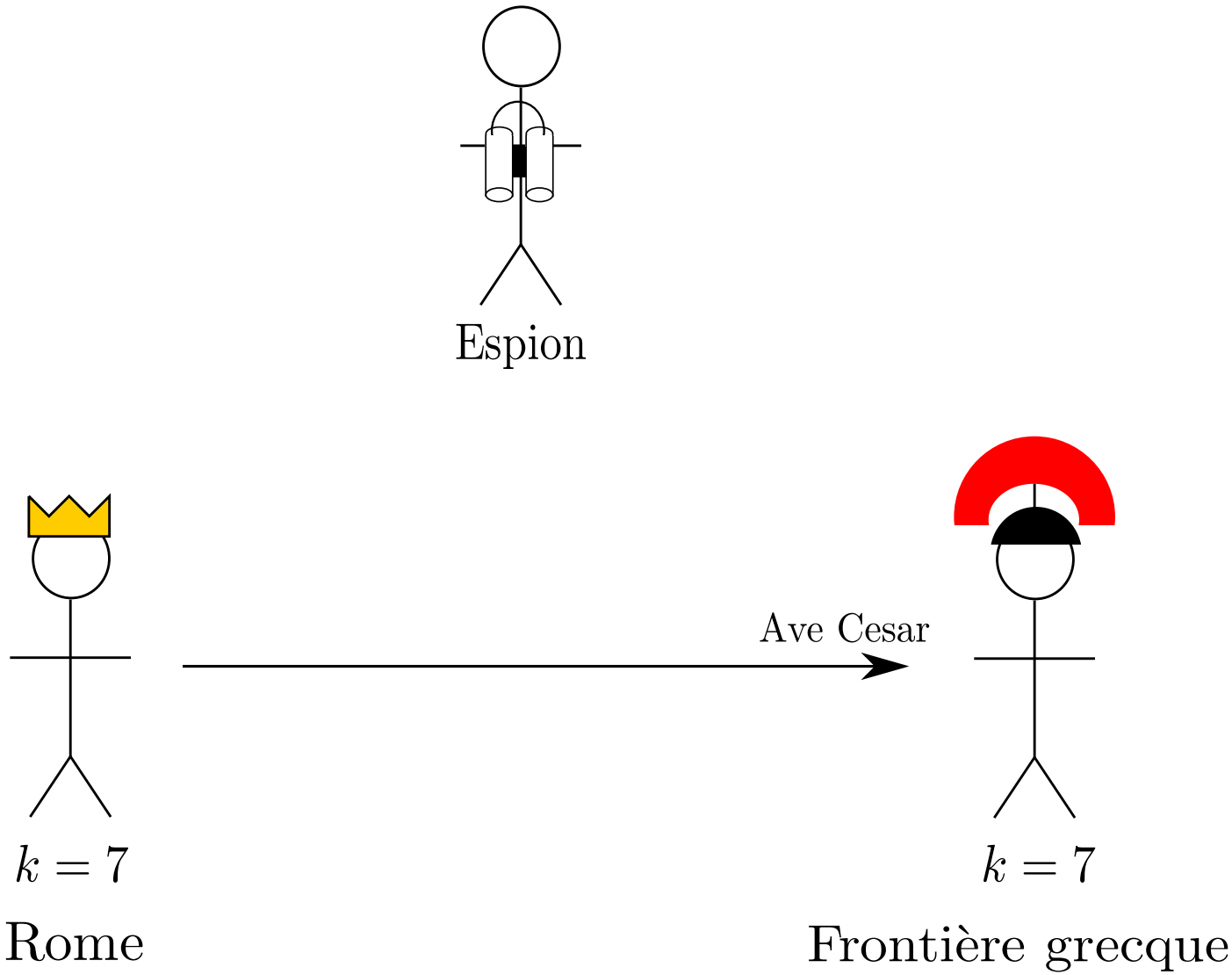
Retour à l'histoire



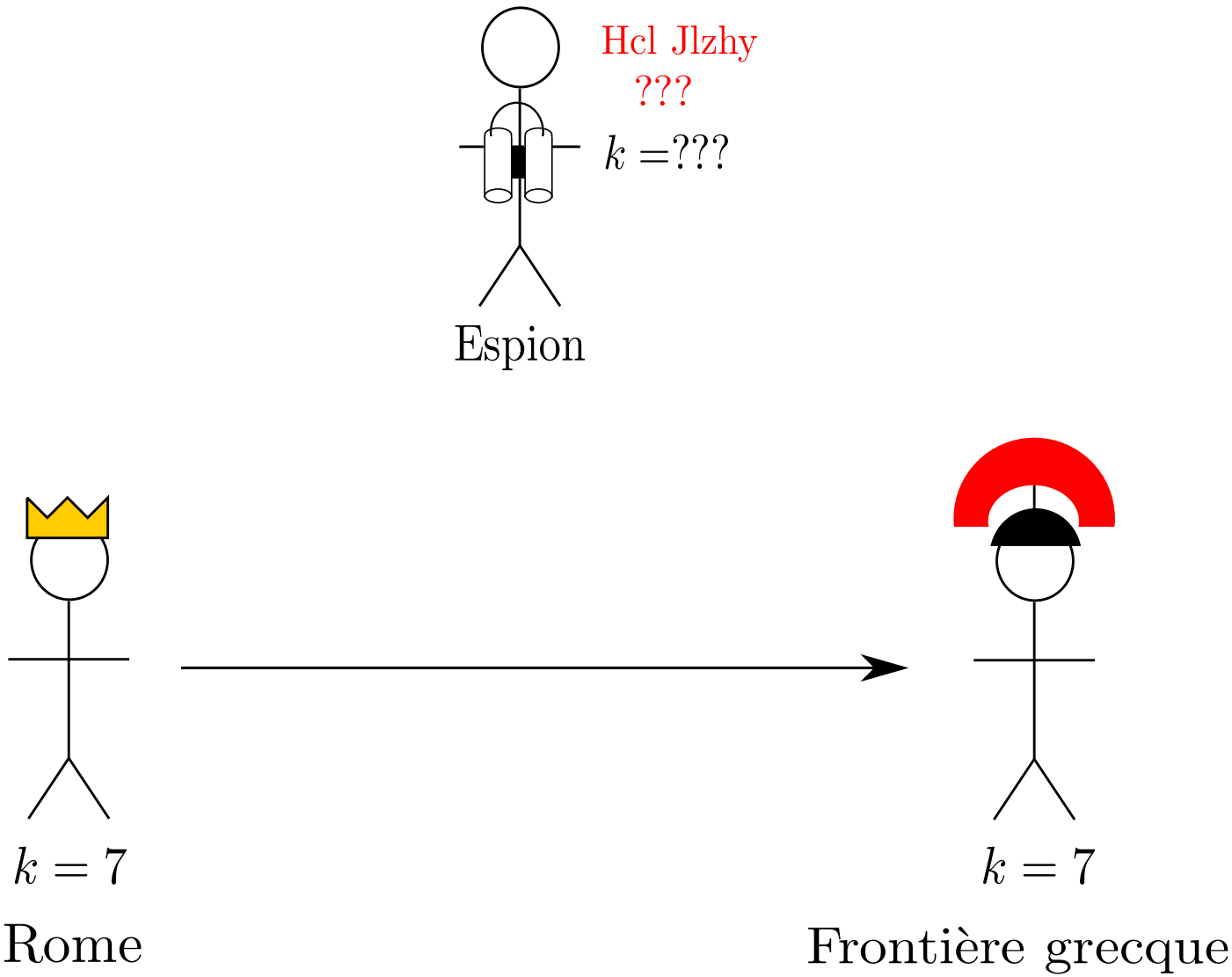
Retour à l'histoire



Retour à l'histoire



Retour à l'histoire



Les problèmes restants

- On peut tester les 25 possibilités de décalage.
- Analyse des fréquences des lettres.

Les problèmes restants

- On peut tester les 25 possibilités de décalage.
- Analyse des fréquences des lettres.

Aujourd'hui, on sait faire mieux que César, par exemple la machine Enigma, utilisée pendant la seconde guerre mondiale.

Les problèmes restants

- On peut tester les 25 possibilités de décalage.
- Analyse des fréquences des lettres.

Aujourd'hui, on sait faire mieux que César, par exemple la machine Enigma, utilisée pendant la seconde guerre mondiale.

- Il faut que César et son général se rencontrent.
  $\Rightarrow$ Achats sur Internet ?

Plan

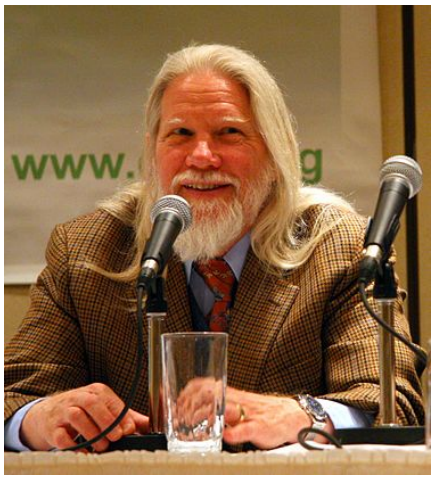
Question

César et son général peuvent-ils échanger des messages chiffrés sans s'être rencontrés avant ?

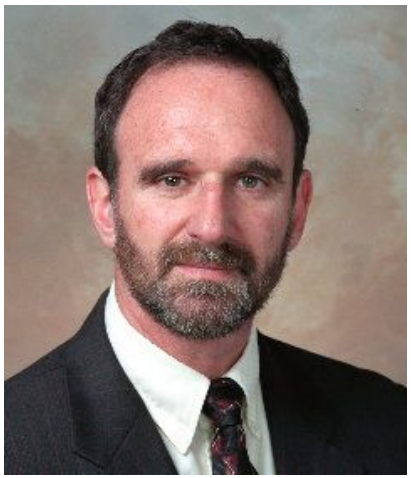
Question

César et son général peuvent-ils échanger des messages chiffrés sans s'être rencontrés avant ?

Oui. C'est la cryptographie *asymétrique*. Première construction proposée par Whitfield Diffie et Martin Hellman en 1976.

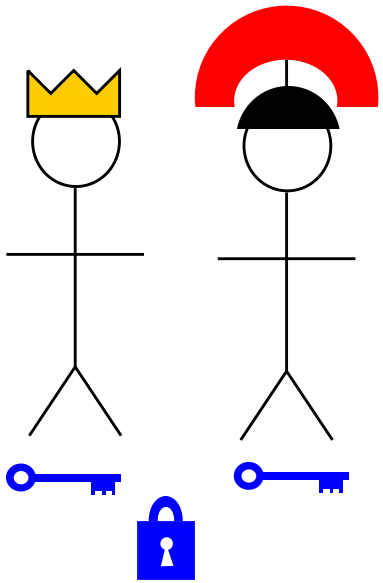


Whitfield Diffie



Martin Hellman

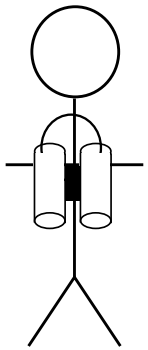
Chiffrement symétrique (par exemple chiffrement de César)



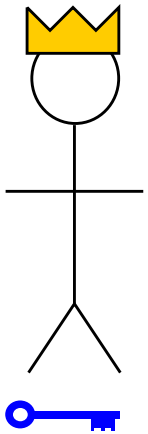
Rome

Frontière grecque

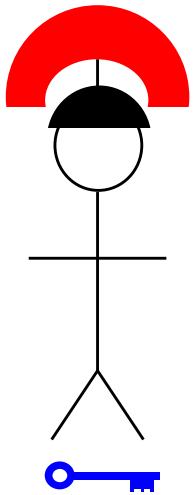
Chiffrement symétrique (par exemple chiffrement de César)



Espion

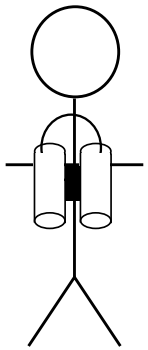


Rome

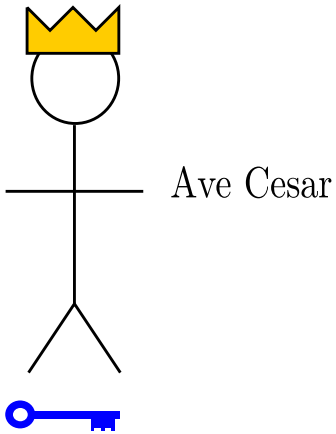


Frontière grecque

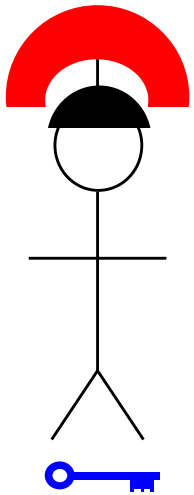
Chiffrement symétrique (par exemple chiffrement de César)



Espion

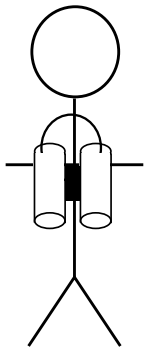


Rome

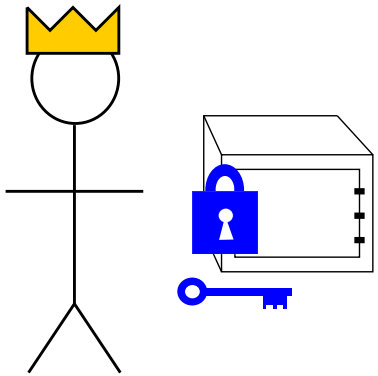


Frontière grecque

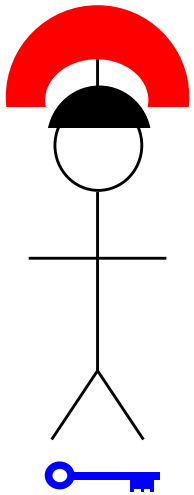
Chiffrement symétrique (par exemple chiffrement de César)



Espion

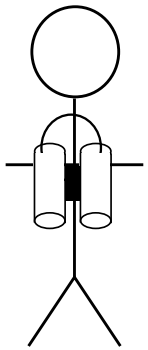


Rome

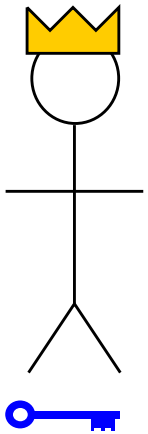


Frontière grecque

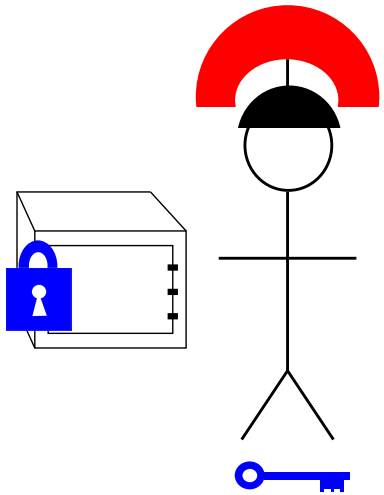
Chiffrement symétrique (par exemple chiffrement de César)



Espion

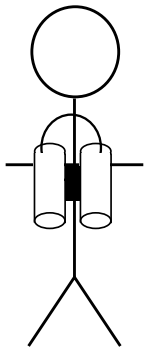


Rome

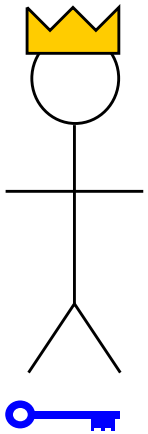


Frontière grecque

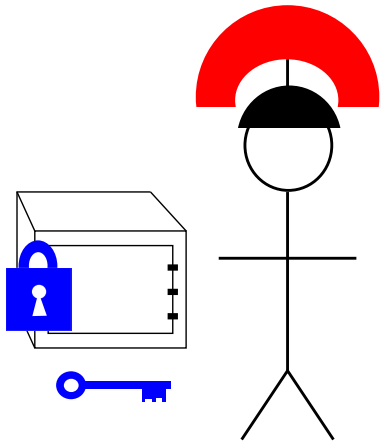
Chiffrement symétrique (par exemple chiffrement de César)



Espion

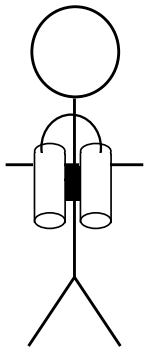


Rome

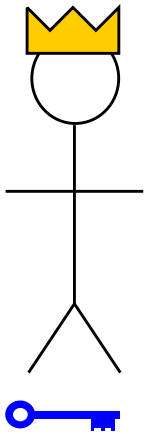


Frontière grecque

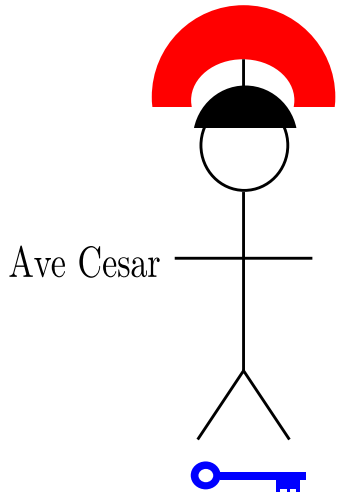
Chiffrement symétrique (par exemple chiffrement de César)



Espion

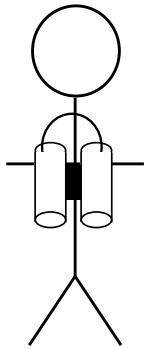


Rome

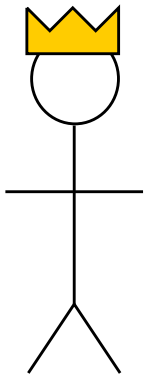


Frontière grecque

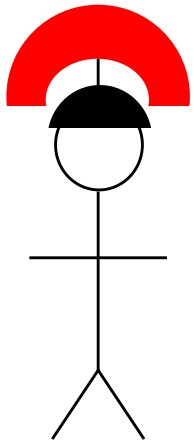
Chiffrement asymétrique



Espion

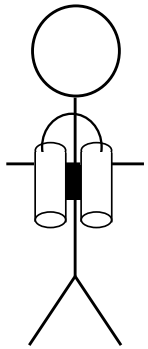


Rome

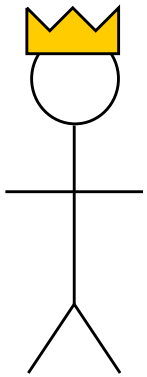


Frontière grecque

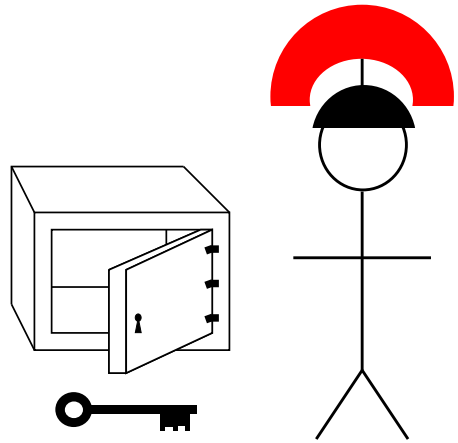
Chiffrement asymétrique



Espion

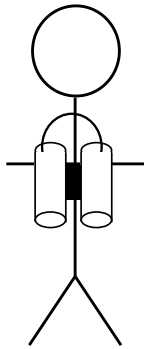


Rome

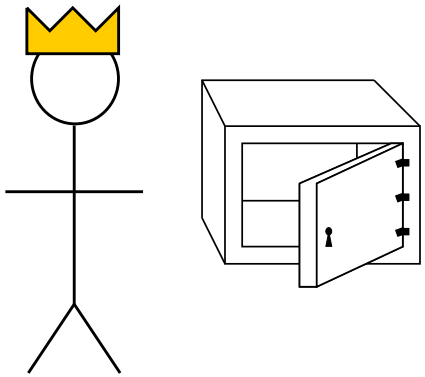


Frontière grecque

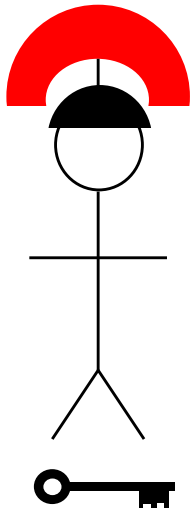
Chiffrement asymétrique



Espion

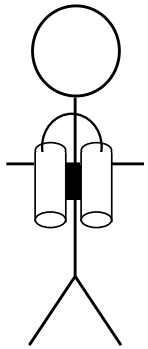


Rome

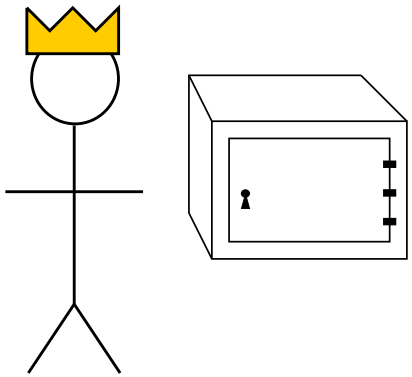


Frontière grecque

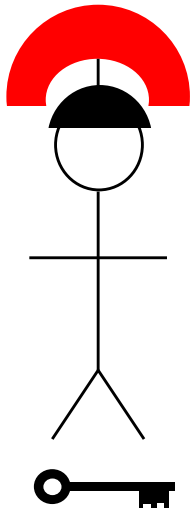
Chiffrement asymétrique



Espion

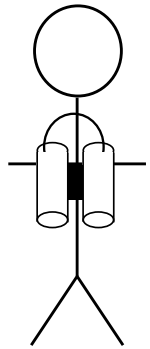


Rome

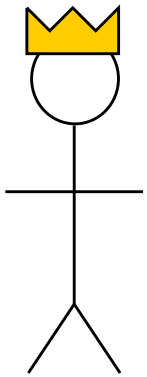


Frontière grecque

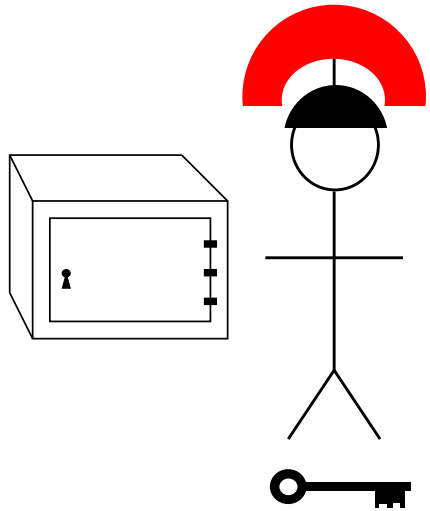
Chiffrement asymétrique



Espion

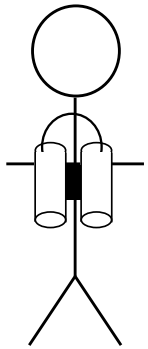


Rome

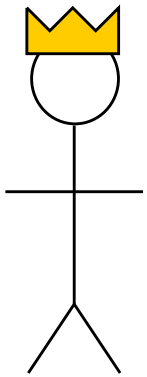


Frontière grecque

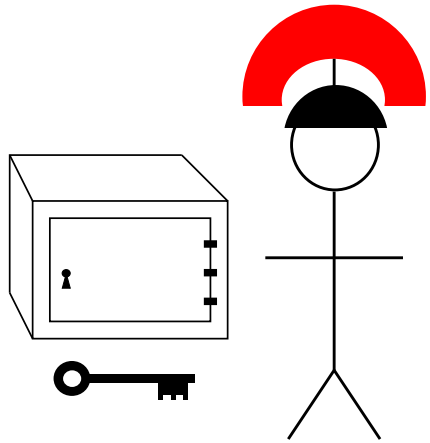
Chiffrement asymétrique



Espion

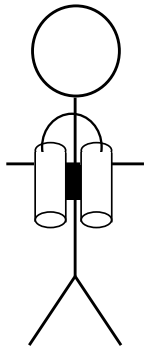


Rome

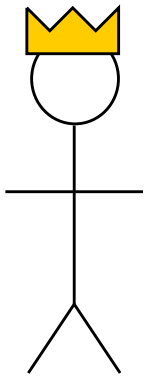


Frontière grecque

Chiffrement asymétrique



Espion

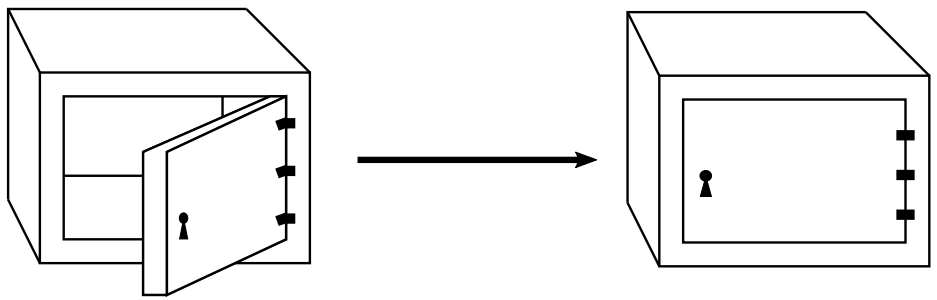


Rome

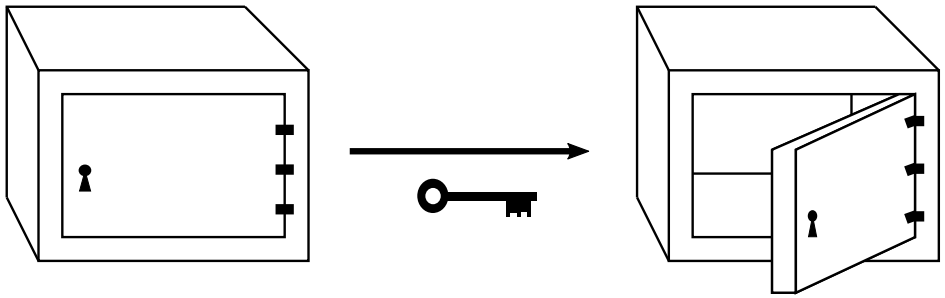
Frontière grecque

En pratique, comment ça marche ?

Les boîtes sont remplacées par des maths.



Facile



Difficile
(besoin de la clé)

Objectif : trouver un problème de maths facile dans un sens et difficile dans l'autre.

Factorisation

Factoriser

Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$6 =$

Factorisation

Factoriser

Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$6 = 2 \times 3$,

Factorisation

Factoriser

Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$6 = 2 \times 3, \qquad 16 =$

Factorisation

Factoriser

Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$6 = 2 \times 3, \qquad 16 = 4 \times 4 = 2 \times 8,$

Factorisation

Factoriser

Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$6 = 2 \times 3, \qquad 16 = 4 \times 4 = 2 \times 8, \qquad 291149 = ???$

Factorisation

Factoriser

Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$6 = 2 \times 3, \qquad 16 = 4 \times 4 = 2 \times 8, \qquad 291149 = 811 \times 359$

Factorisation

Factoriser

Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$$6 = 2 \times 3, \qquad 16 = 4 \times 4 = 2 \times 8, \qquad 291149 = 811 \times 359$$

On a trouvé notre problème de maths

Factoriser est un problème *difficile*, mais multiplier c'est *facile*.

Factorisation

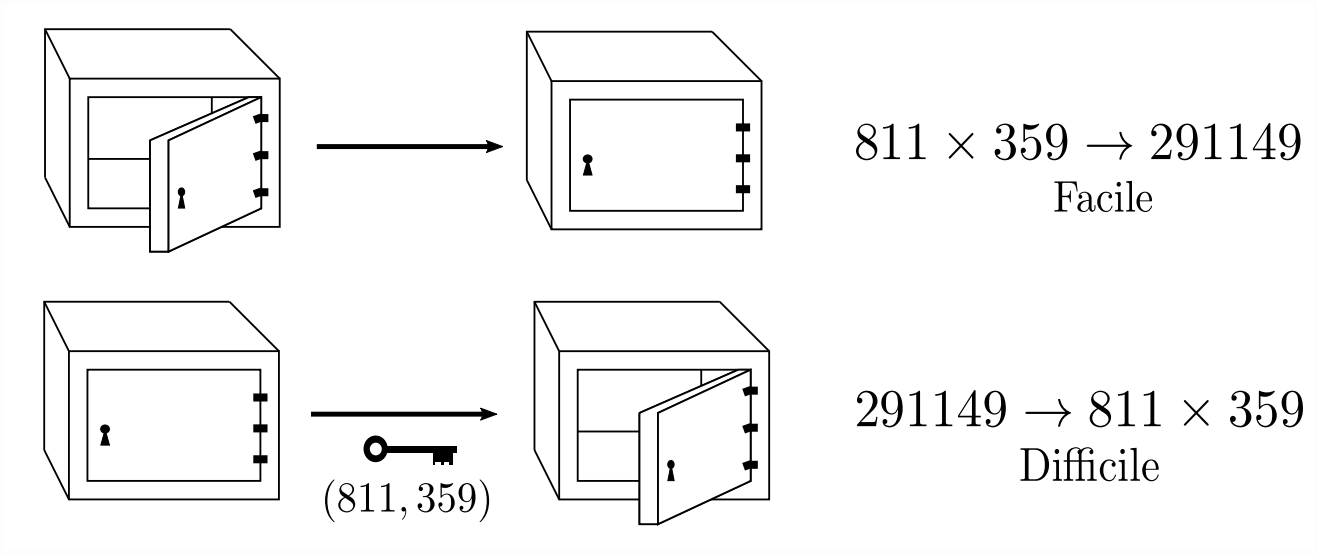
Factoriser

Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$$6 = 2 \times 3, \qquad 16 = 4 \times 4 = 2 \times 8, \qquad 291149 = 811 \times 359$$

On a trouvé notre problème de maths

Factoriser est un problème *difficile*, mais multiplier c'est *facile*.



Factorisation

Factoriser

Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$6 = 2 \times 3, \qquad 16 = 4 \times 4 = 2 \times 8, \qquad 291149 = 811 \times 359$

On a trouvé notre problème de maths

Factoriser est un problème *difficile*, mais multiplier c'est *facile*.

Challenge :

Multiplier : $557 \times 881 \rightarrow$

Factoriser : $391 \rightarrow$

$391109 \rightarrow$

Factorisation

Factoriser

Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$6 = 2 \times 3, \qquad 16 = 4 \times 4 = 2 \times 8, \qquad 291149 = 811 \times 359$

On a trouvé notre problème de maths

Factoriser est un problème *difficile*, mais multiplier c'est *facile*.

Challenge :

Multiplier : $557 \times 881 \to 490717$

Factoriser : $391 \to$

$391109 \to$

Factorisation

Factoriser

Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$$6 = 2 \times 3, \qquad 16 = 4 \times 4 = 2 \times 8, \qquad 291149 = 811 \times 359$$

On a trouvé notre problème de maths

Factoriser est un problème *difficile*, mais multiplier c'est *facile*.

Challenge :

Multiplier : $557 \times 881 \to 490717$

Factoriser : $391 \to 17 \times 23$

$391109 \to$

Factorisation

Factoriser

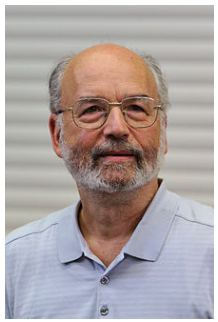
Factoriser un nombre, c'est l'écrire comme produit de deux nombres plus petits.

$6 = 2 \times 3, \qquad 16 = 4 \times 4 = 2 \times 8, \qquad 291149 = 811 \times 359$

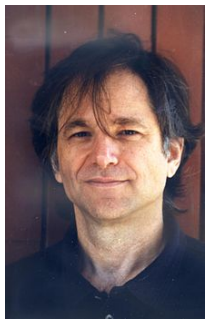
On a trouvé notre problème de maths

Factoriser est un problème *difficile*, mais multiplier c'est *facile*.

Ronald Rivest



Adi Shamir



Leonard Adleman

Chiffrement RSA (1977)

Questions ?