Mathématiques et secrets

Nicolas Billerey

Laboratoire de Mathématiques
Université Blaise Pascal – Clermont-Ferrand 2

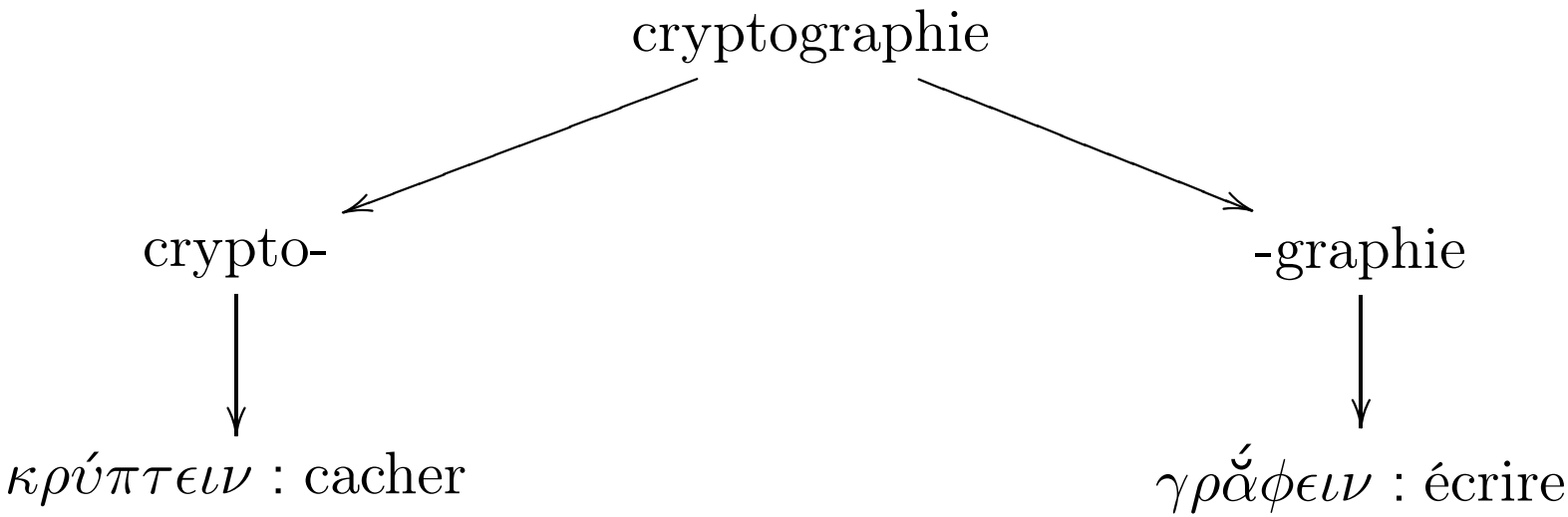
Fête de la science 2013

Introduction à la cryptographie

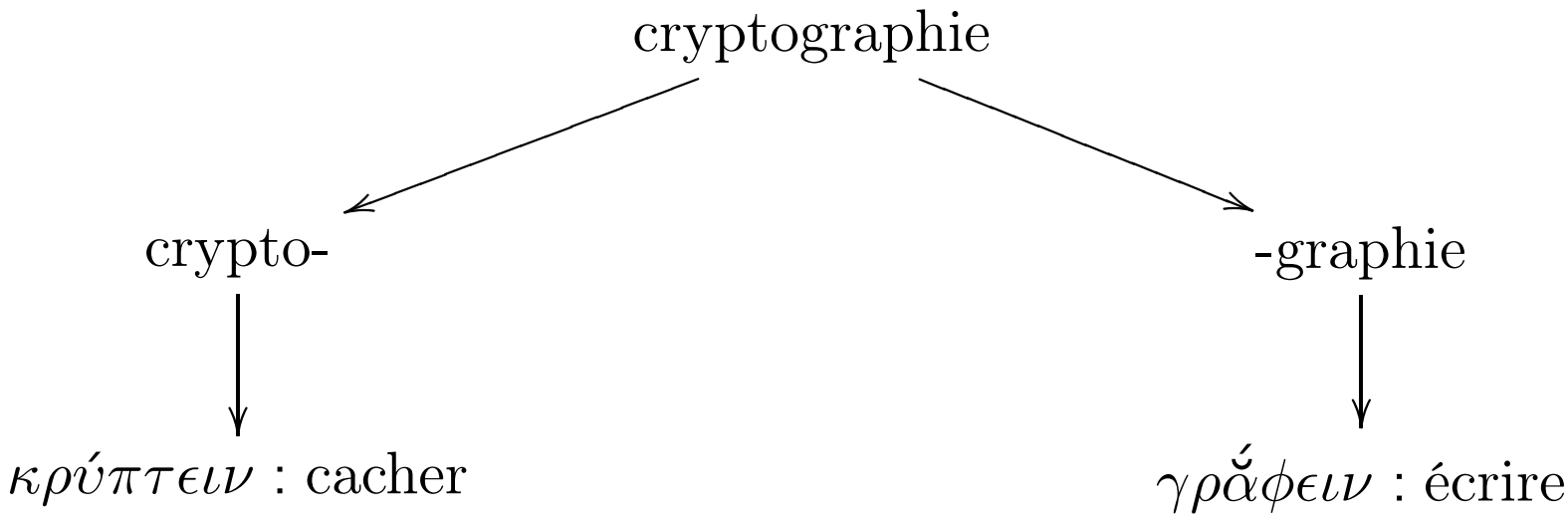
Introduction à la cryptographie asymétrique / à clé publique

Un peu d'étymologie

Un peu d'étymologie

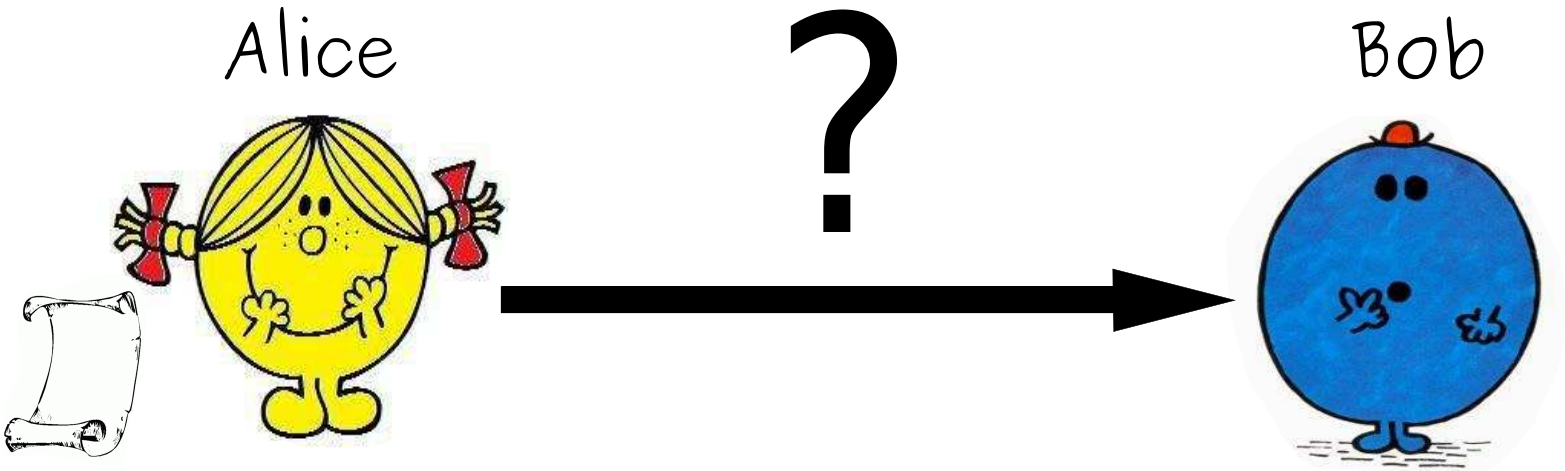


Un peu d'étymologie



La cryptographie désigne l'art ou la science d'écrire en caractères secrets.

Les deux protagonistes : Alice et Bob



Sommaire

Permutation sur l'alphabet

- Chaque lettre de l'alphabet est remplacée par une autre.

Permutation sur l'alphabet

- Chaque lettre de l'alphabet est remplacée par une autre.
- Deux lettres différentes ne peuvent être remplacées par la même.

Permutation sur l'alphabet

- Chaque lettre de l'alphabet est remplacée par une autre.
- Deux lettres différentes ne peuvent être remplacées par la même.

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Chiffrement

« CE QUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT, ET LES MOTS POUR LE DIRE ARRIVENT AISEMENT. »

Chiffrement

« CE QUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT, ET LES MOTS POUR LE DIRE ARRIVENT AISEMENT. »

Le texte clair est *chiffré* en remplaçant chaque lettre par son *image* sous la permutation.

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Chiffrement

« CE QUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT, ET LES MOTS POUR LE DIRE ARRIVENT AISEMENT. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Chiffrement

« YE QUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT, ET LES MOTS POUR LE DIRE ARRIVENT AISEMENT. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Chiffrement

« YE QUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT, ET LES MOTS POUR LE DIRE ARRIVENT AISEMENT. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Chiffrement

« YT QUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT, ET LES MOTS POUR LE DIRE ARRIVENT AISEMENT. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Chiffrement

« YT QUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT, ET LES MOTS POUR LE DIRE ARRIVENT AISEMENT. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Chiffrement

« YT LUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT, ET LES MOTS POUR LE DIRE ARRIVENT AISEMENT. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Chiffrement

« YT LUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT, ET LES MOTS POUR LE DIRE ARRIVENT AISEMENT. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Chiffrement

« YT LSE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT, ET LES MOTS POUR LE DIRE ARRIVENT AISEMENT. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Chiffrement

« YT LST G'JI YJIYJDQ RDTI N'TIJIYT YGCDMTHTIQ, TQ GTN HJQN KJSM GT PDMT CMMDUTIQ CDNTHTIQ. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Déchiffrement

« YT LST G'JI YJIYJDQ RDTI N'TIJIYT YGCDMTHTIQ, TQ GTN HJQN KJSM GT PDMT CMMDUTIQ CDNTHTIQ. »

Déchiffrement

« YT LST G'JI YJIYJDQ RDTI N'TIJIYT YGCDMTHTIQ, TQ GTN HJQN KJSM GT PDMT CMMDUTIQ CDNTHTIQ. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Déchiffrement

« YT LST G'JI YJIYJDQ RDTI N'TIJIYT YGCDMTHTIQ, TQ GTN HJQN KJSM GT PDMT CMMDUTIQ CDNTHTIQ. »

Le texte chiffré est déchiffré en remplaçant chaque lettre par son *antécédent* sous la permutation.

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Déchiffrement

« CT LST G'JI YJIYJDQ RDTI N'TIJIYT YGCDMTHTIQ, TQ GTN HJQN KJSM GT PDMT CMMDUTIQ CDNTHTIQ. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Déchiffrement

« CT LST G'JI YJIYJDQ RDTI N'TIJIYT YGCDMTHTIQ, TQ GTN HJQN KJSM GT PDMT CMMDUTIQ CDNTHTIQ. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Déchiffrement

« CE LST G'JI YJIYJDQ RDTI N'TIJIYT YGCDMTHTIQ, TQ GTN HJQN KJSM GT PDMT CMMDUTIQ CDNTHTIQ. »

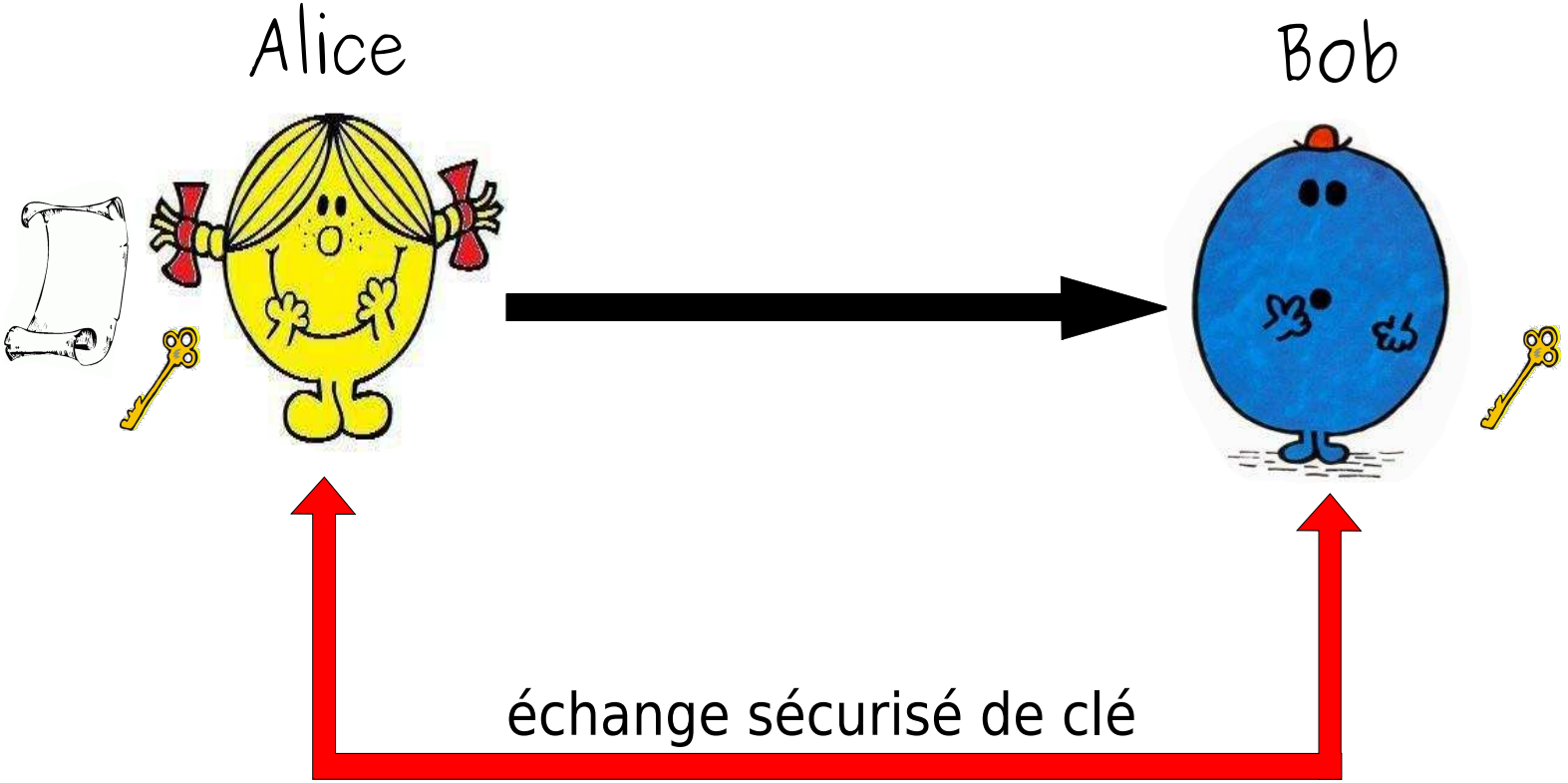
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Déchiffrement

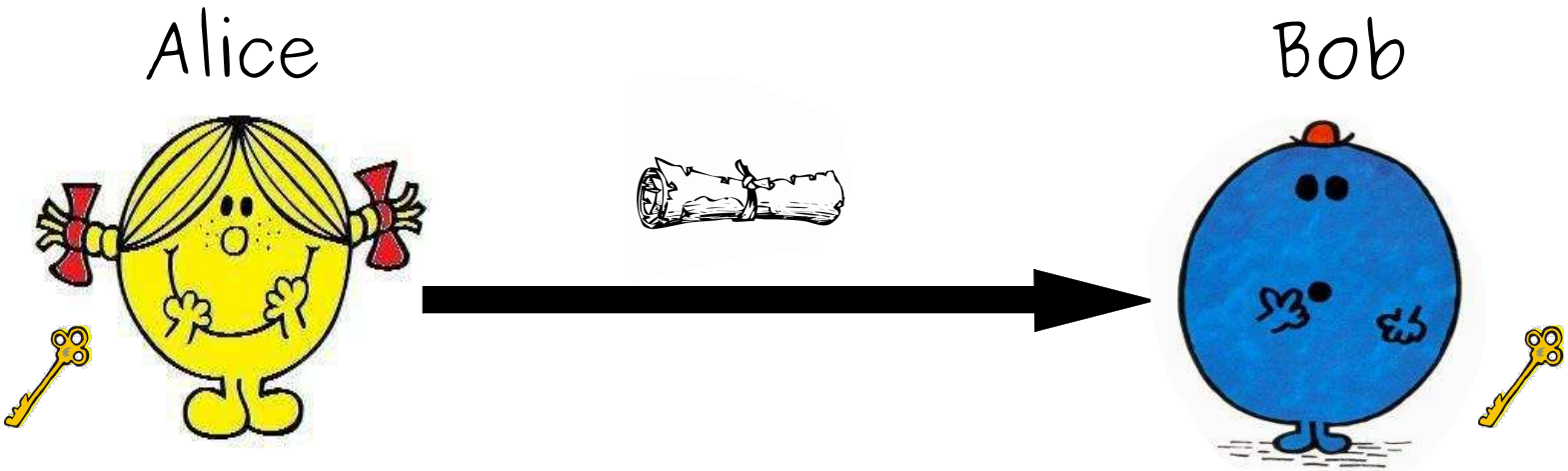
« CE QUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT, ET LES MOTS POUR LE DIRE ARRIVENT AISEMENT. »

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
C	**R**	**Y**	**P**	**T**	**O**	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

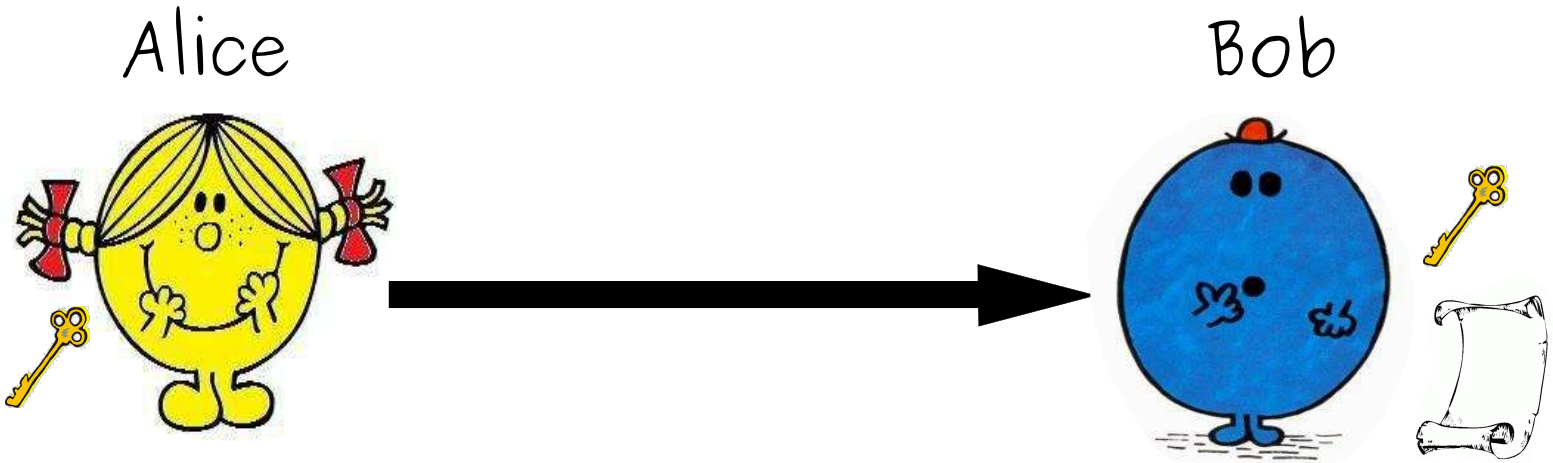
1. Alice et Bob conviennent *secrètement* d'une « clé ».



2. Alice chiffre son message avec la clé et l'envoie à Bob.



3. Avec la clé secrète Bob déchiffre le message reçu.



Cryptosystème à clé secrète

On appelle *cryptosystème* l'ensemble formé par les algorithmes fournissant la clé ainsi que la méthode de chiffrement et de déchiffrement.

Cryptosystème à clé secrète

On appelle *cryptosystème* l'ensemble formé par les algorithmes fournissant la clé ainsi que la méthode de chiffrement et de déchiffrement.

Un *cryptosystème à clé secrète* est un cryptosystème où la clé est. . .secrète !

Et si...

- ...Alice et Bob ne se rencontraient jamais ?

Et si...

- ...Alice et Bob ne se rencontraient jamais ?
- ...une personne mal intentionnée espionnait en permanence leur communication ?

Et si...

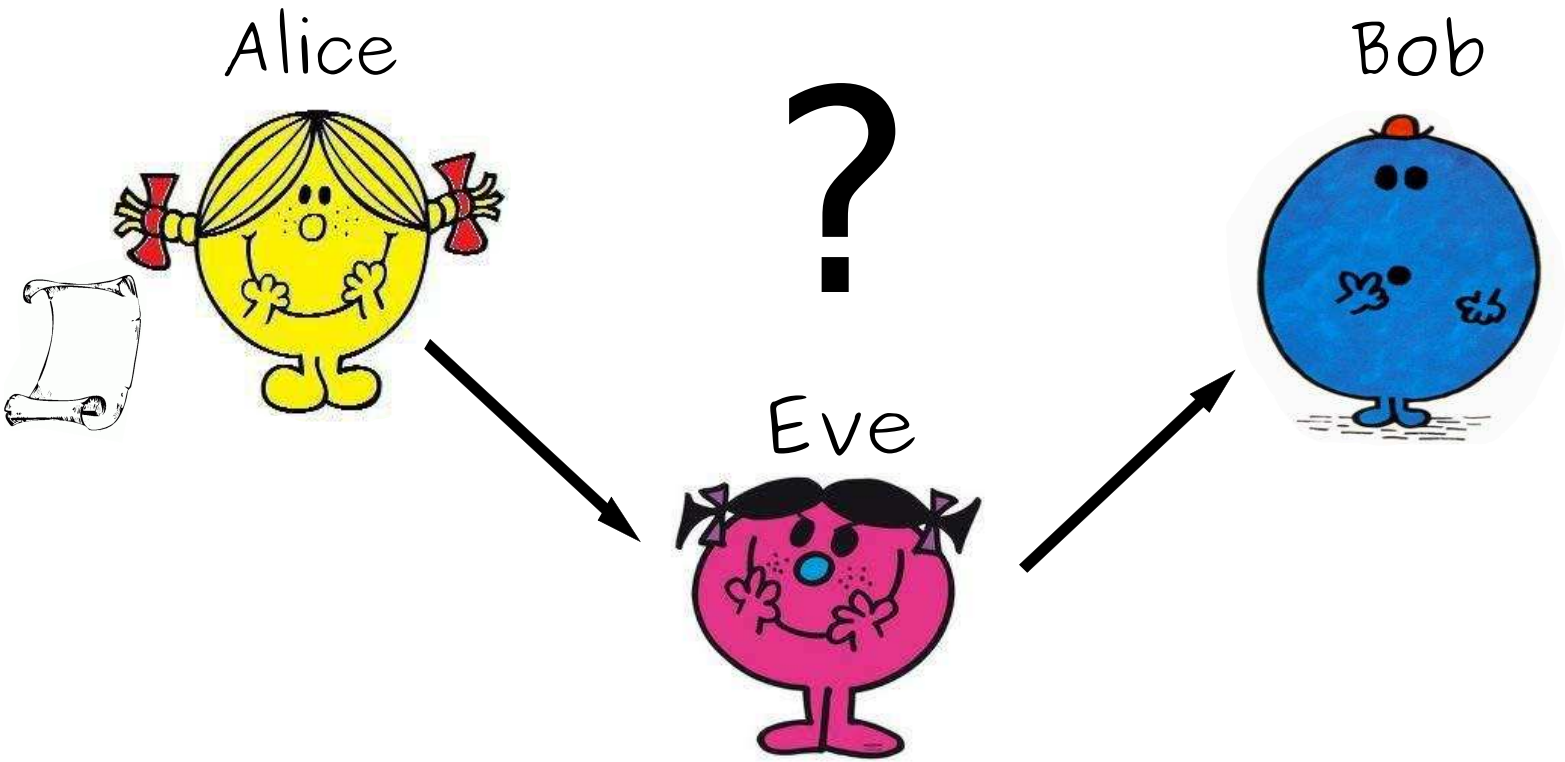
- ...Alice et Bob ne se rencontraient jamais ?
- ...une personne mal intentionnée espionnait en permanence leur communication ?
- ...Alice et Bob n'étaient en fait que deux ordinateurs ?

Et si...

- ...Alice et Bob ne se rencontraient jamais ?
- ...une personne mal intentionnée espionnait en permanence leur communication ?
- ...Alice et Bob n'étaient en fait que deux ordinateurs ?

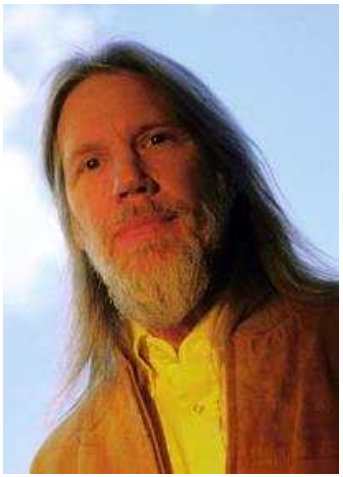
Comment feraient-ils ?

Et maintenant l'espionne !

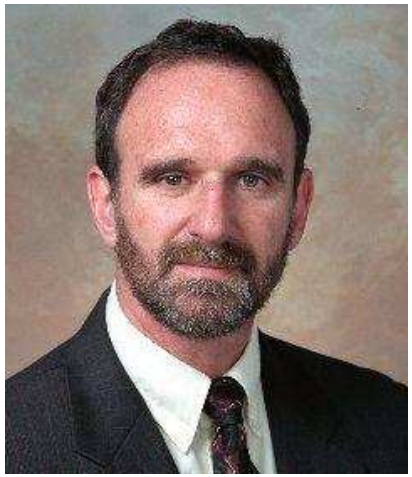


L'intuition de Diffie et Hellman

L'intuition de Diffie et Hellman

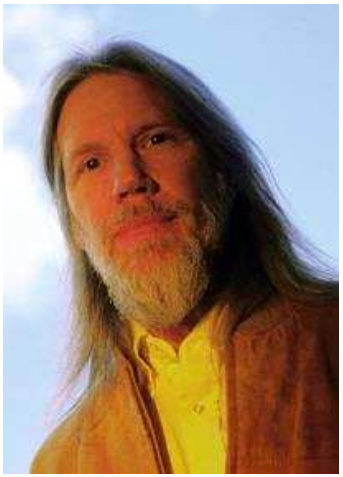


W. Diffie

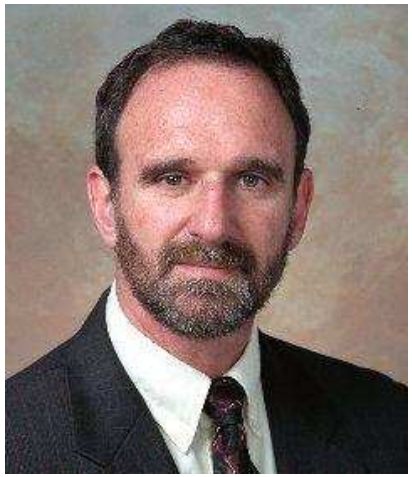


M. Hellman

L'intuition de Diffie et Hellman



W. Diffie



M. Hellman

"Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature."

W. Diffie and M. Hellman, *New directions in Cryptography*, 1976.

Ce qu'ils expliquent dans leur article et les conséquences

Les cryptosystèmes à clé secrète ne sont pas les seuls !

Ce qu'ils expliquent dans leur article et les conséquences

Les cryptosystèmes à clé secrète ne sont pas les seuls !

- Alice et Bob peuvent communiquer secrètement même en présence d'un espion.

Ce qu'ils expliquent dans leur article et les conséquences

Les cryptosystèmes à clé secrète ne sont pas les seuls !

- Alice et Bob peuvent communiquer secrètement même en présence d'un espion.
- Ces cryptosystèmes offrent les mêmes garanties que le courrier papier : confidentialité et authenticité.

Sommaire

Le fonctionnement

1. Bob dispose de deux algorithmes : l'un de chiffrement C et l'autre de déchiffrement D.

Le fonctionnement

1. Bob dispose de deux algorithmes : l'un de chiffrement C et l'autre de déchiffrement D.
2. Étant donné un texte clair m, le chiffrer puis le déchiffrer revient à ne rien faire : $(D \circ C)(m) = m$.

Le fonctionnement

1. Bob dispose de deux algorithmes : l'un de chiffrement C et l'autre de déchiffrement D.
2. Étant donné un texte clair m, le chiffrer puis le déchiffrer revient à ne rien faire : $(D \circ C)(m) = m$.
3. Étant donné un texte chiffré M, le déchiffrer puis le (re)chiffrer revient à ne rien faire : $(C \circ D)(M) = M$.

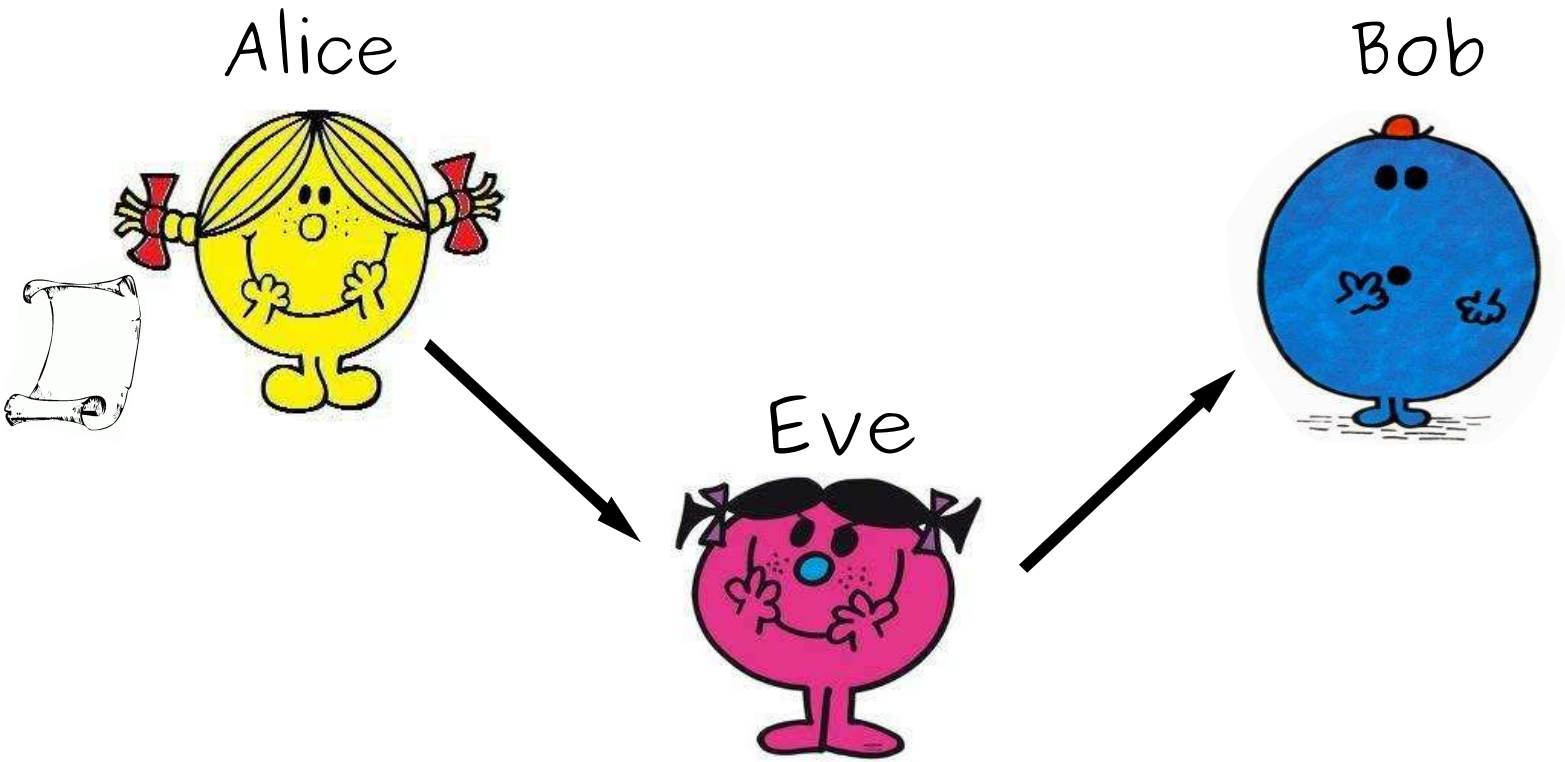
Le fonctionnement

1. Bob dispose de deux algorithmes : l'un de chiffrement C et l'autre de déchiffrement D.
2. Étant donné un texte clair m, le chiffrer puis le déchiffrer revient à ne rien faire : $(D \circ C)(m) = m$.
3. Étant donné un texte chiffré M, le déchiffrer puis le (re)chiffrer revient à ne rien faire : $(C \circ D)(M) = M$.
4. Bob rend C public, mais garde pour lui D.

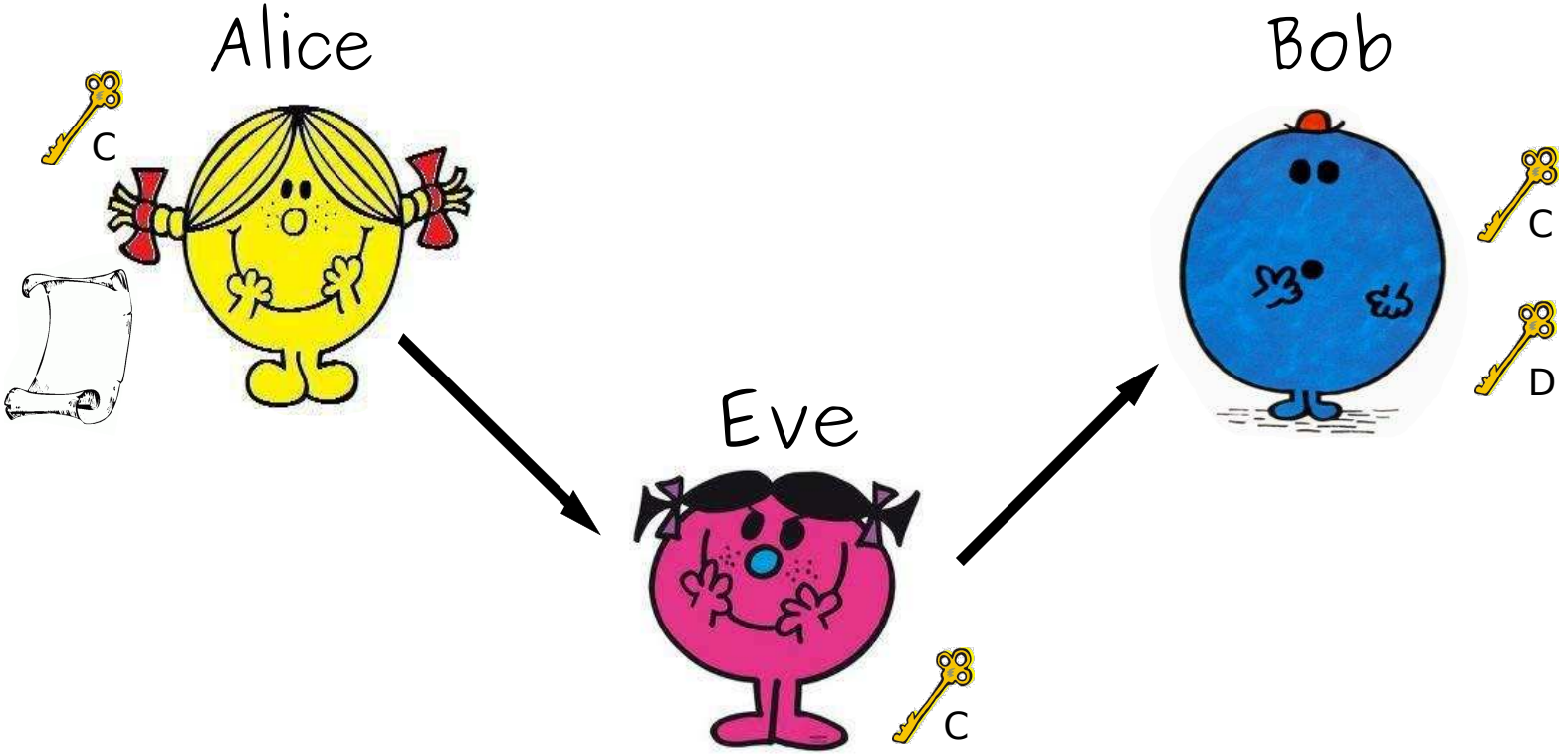
Le fonctionnement

1. Bob dispose de deux algorithmes : l'un de chiffrement C et l'autre de déchiffrement D.
2. Étant donné un texte clair m, le chiffrer puis le déchiffrer revient à ne rien faire : $(D \circ C)(m) = m$.
3. Étant donné un texte chiffré M, le déchiffrer puis le (re)chiffrer revient à ne rien faire : $(C \circ D)(M) = M$.
4. Bob rend C public, mais garde pour lui D.
5. Les algorithmes C et D sont faciles à exécuter, mais à partir de la connaissance de C, il est extrêmement difficile de déterminer D.

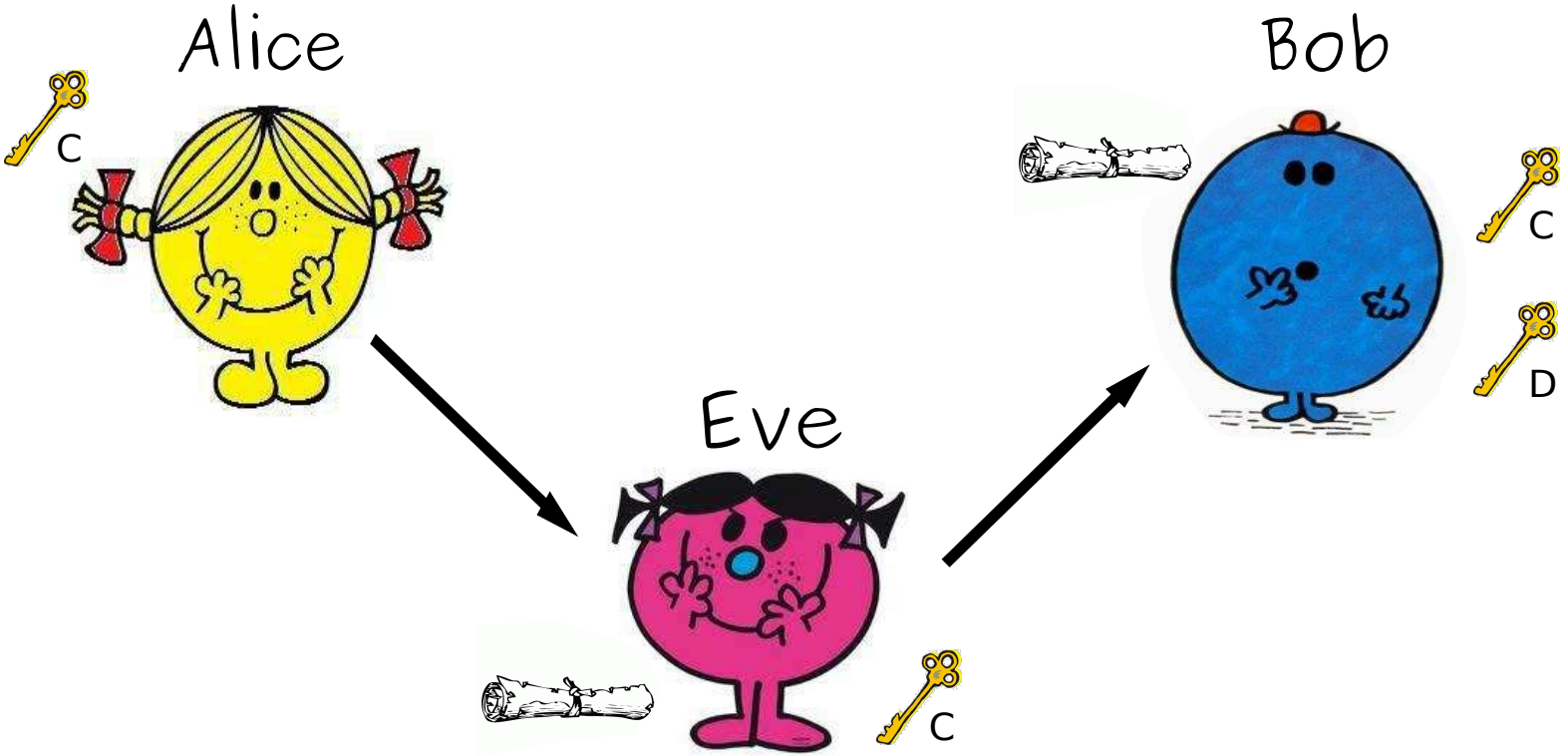
La pratique



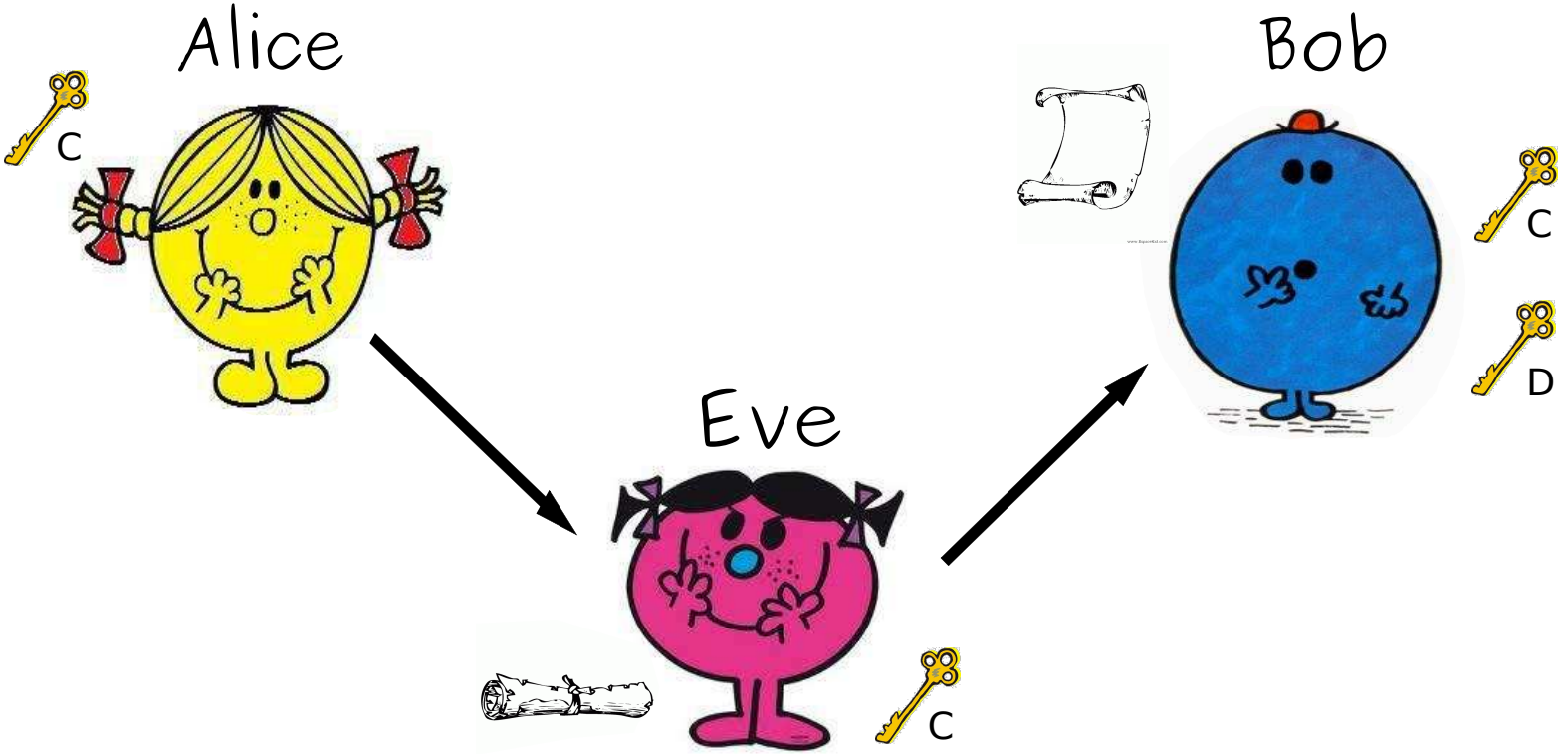
1. Bob rend publique sa clé de chiffrement.



2. Alice chiffre son message à l'aide de la clé de chiffrement de Bob et l'envoie à Bob.



3. À l'aide de sa clé de déchiffrement D, Bob déchiffre le message envoyé par Alice. Et c'est le seul à pouvoir le faire !



Comment peut-on réaliser un cryptosystème à clé publique ?

Sommaire

Définition

Un codage désigne un procédé, *connu de tous*, par lequel on transforme chaque élément d'un jeu de caractères d'un système d'écriture donné en une représentation numérique.

Définition

Un codage désigne un procédé, *connu de tous*, par lequel on transforme chaque élément d'un jeu de caractères d'un système d'écriture donné en une représentation numérique.

- Le code Morse : A (.−), B (−...), C (−. − .), etc.

Définition

Un codage désigne un procédé, *connu de tous*, par lequel on transforme chaque élément d'un jeu de caractères d'un système d'écriture donné en une représentation numérique.

- Le code Morse : A (.−), B (−...), C (−. − .), etc.
- Le code ASCII (American Standard Code for Information Interchange) :

caractère	code ASCII	caractère	code ASCII
A	1000001	'	0100111
B	1000010	!	0100001
C	1000011	␣	0100000
D	1000100	a	1100001

Moralité

Chiffrer un message revient à chiffrer un nombre !

Sommaire

Les créateurs de l'arithmétique modulaire

Fermat (début $17^{\text{ème}}$–1665)

Euler (1707–1783)

Gauss (1777–1855)

Le principe

Soit $N \geq 1$ un entier fixé.

Le principe

Soit $N \geq 1$ un entier fixé.

Définition

On dit que deux entiers a et b sont congrus modulo N et on écrit $a \equiv b\ [N]$ si la différence $a - b$ est un multiple de N.

Le principe

Soit $N \geq 1$ un entier fixé.

Définition

On dit que deux entiers a et b sont congrus modulo N et on écrit $a \equiv b\ [N]$ si la différence $a - b$ est un multiple de N.

Par exemple, $45 \equiv 11\ [17]$ car $45 - 11 = 34 = 2 \times 17$.

Le principe

Soit $N \geq 1$ un entier fixé.

Définition

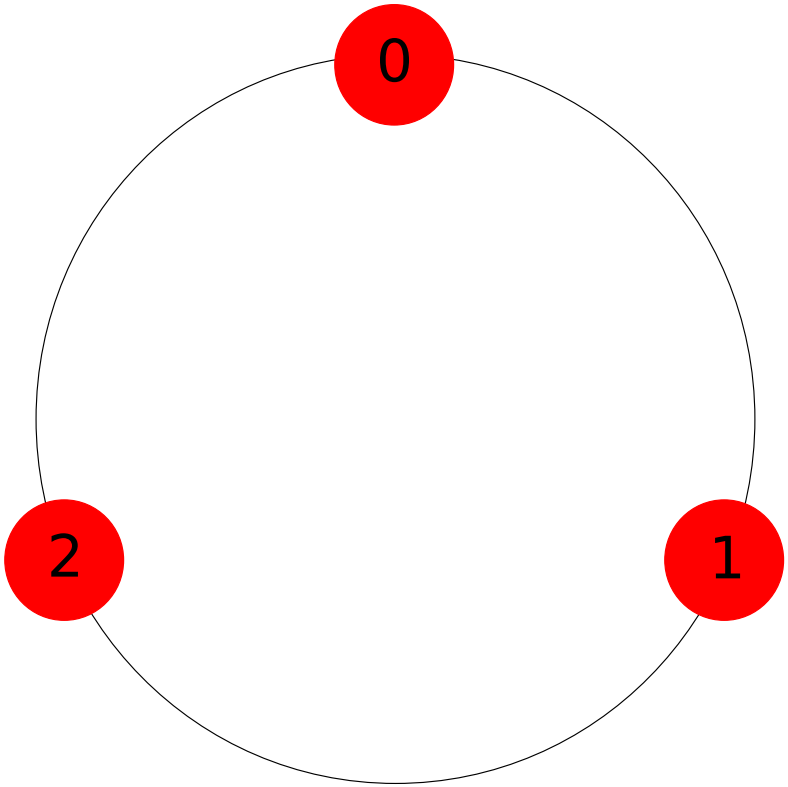
On dit que deux entiers a et b sont congrus modulo N et on écrit $a \equiv b\ [N]$ si la différence $a - b$ est un multiple de N.

Par exemple, $45 \equiv 11\ [17]$ car $45 - 11 = 34 = 2 \times 17$.

Propriété

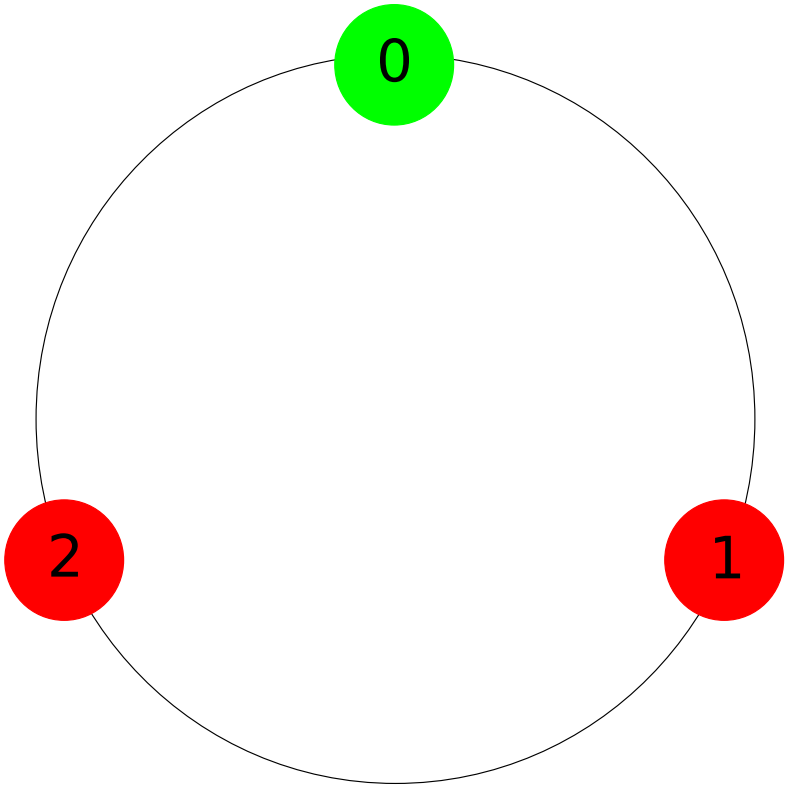
Pour tout entier a, il existe un unique entier $b \in \{0, \ldots, N-1\}$ tel que $a \equiv b\ [N]$.

$N = 3$



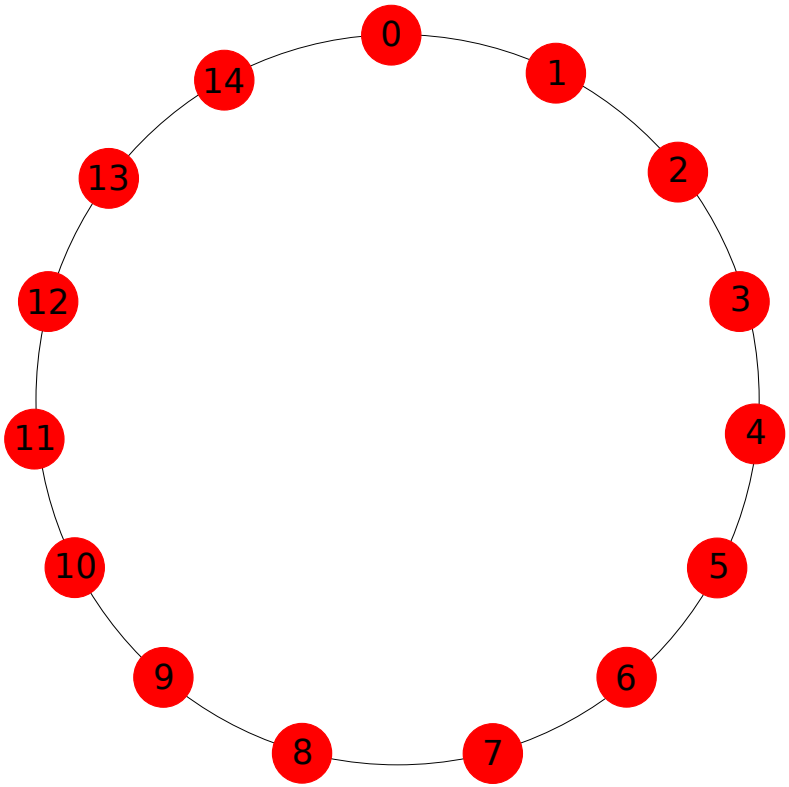
$87654567 \equiv ? \ [3].$

$N = 3$

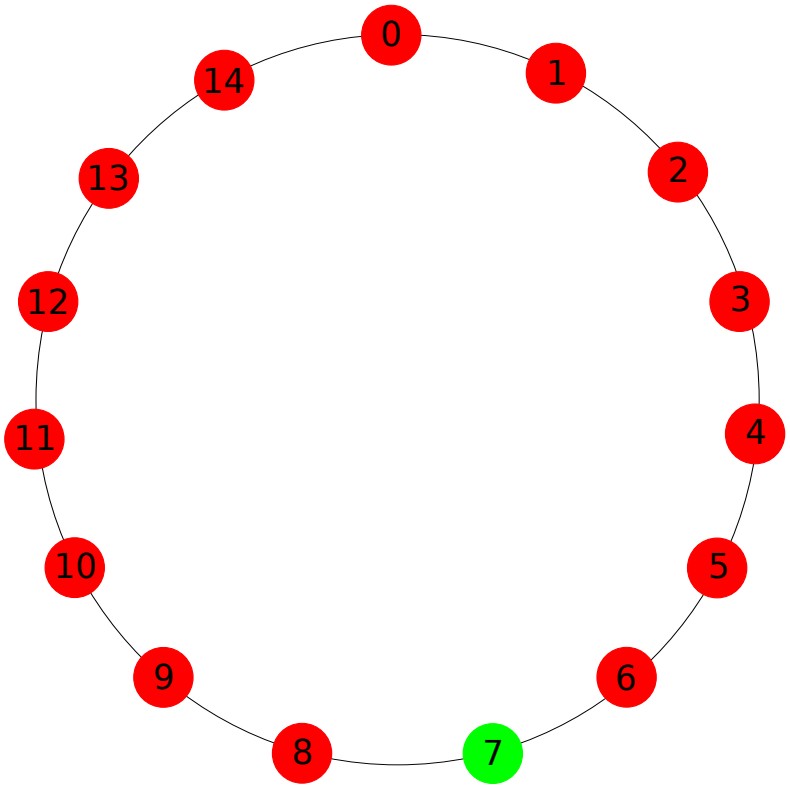


$$87654567 = 29218189 \times 3$$
$$87654567 \equiv 0\ [3]$$

$N = 15$



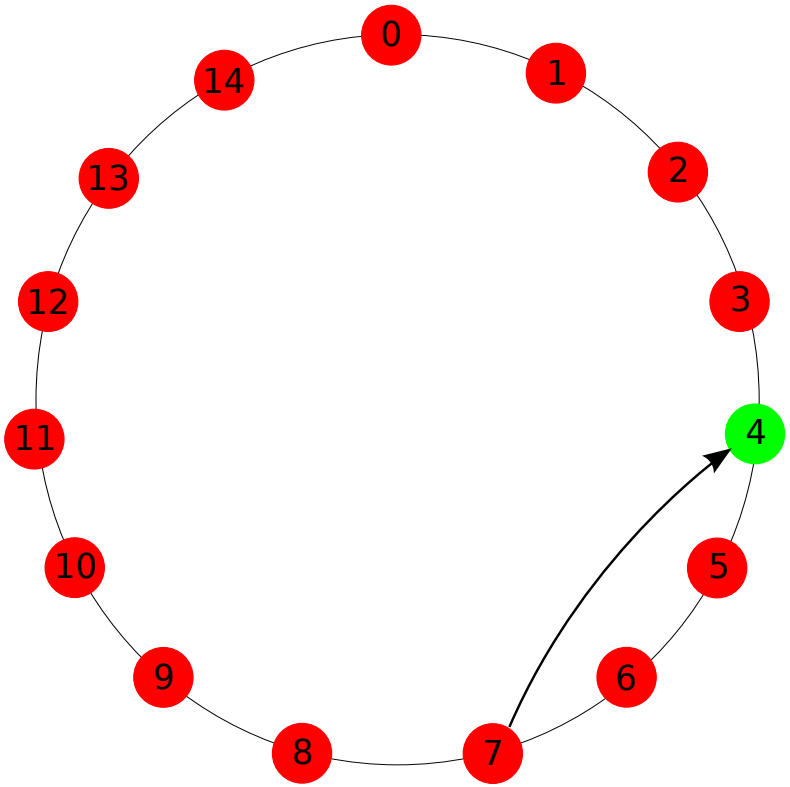
$N = 15$



On calcule

$$7^2\ [15], 7^3\ [15], \ldots$$

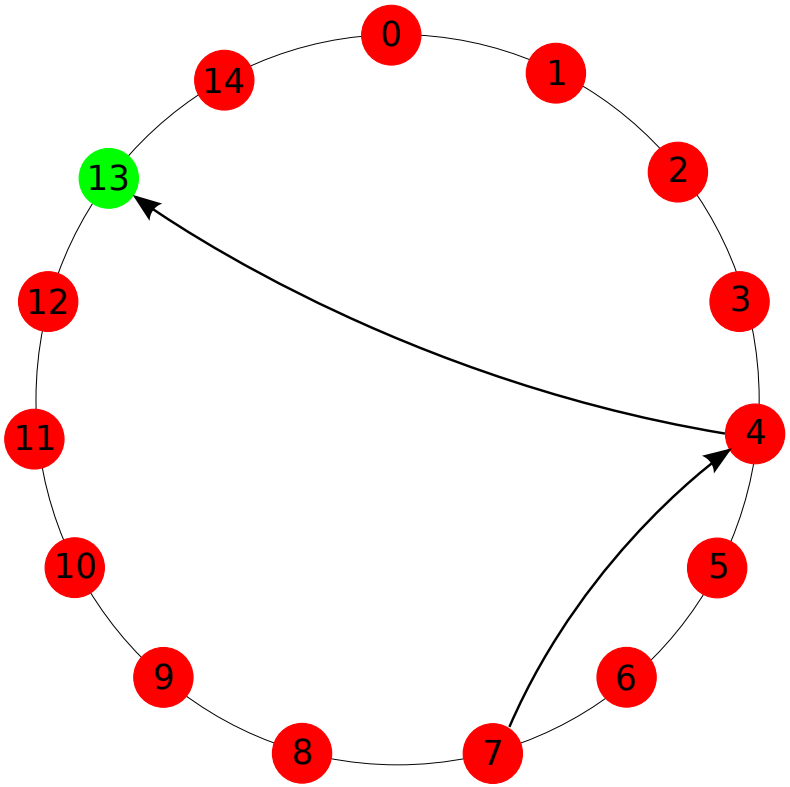
$N = 15$



$$7^2 = 49 = 15 \times 3 + 4$$

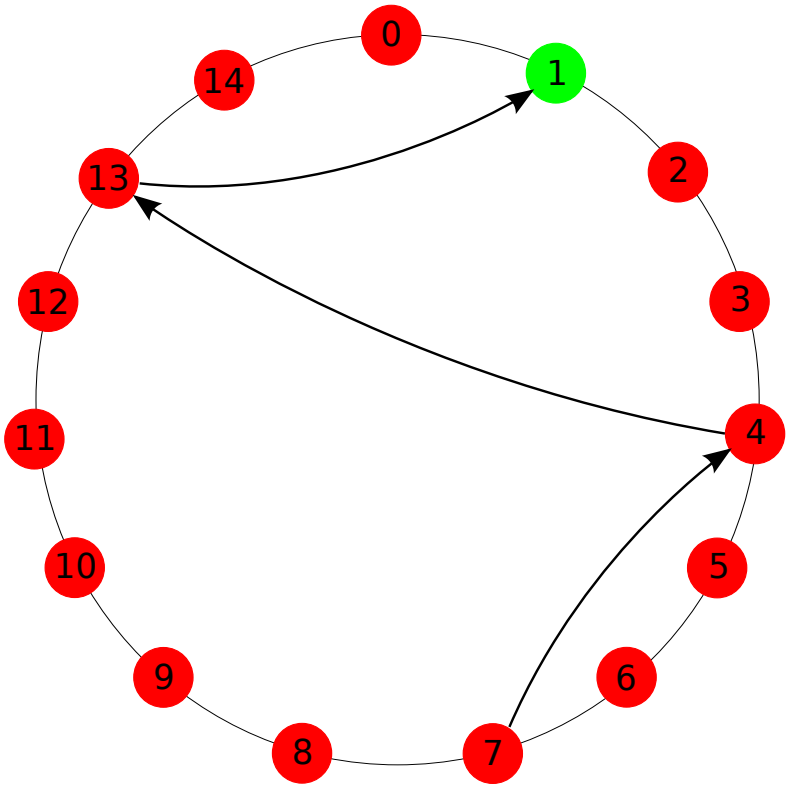
$$7^2 \equiv 4 \ [15]$$

$N = 15$



$$7^2 \equiv 4 \ [15]$$
$$7^3 = 7^2 \times 7 \equiv 7 \times 4 \equiv 13 \ [15]$$

$N = 15$



$$7^3 \equiv 13\ [15]$$
$$7^4 = 7^3 \times 7 \equiv 13 \times 7 \equiv 1\ [15]$$

Le théorème d'Euler-Fermat

On suppose que $N = p \times q$ avec p, q nombres premiers (par ex. $N = 77 = 7 \times 11$).

Le théorème d'Euler-Fermat

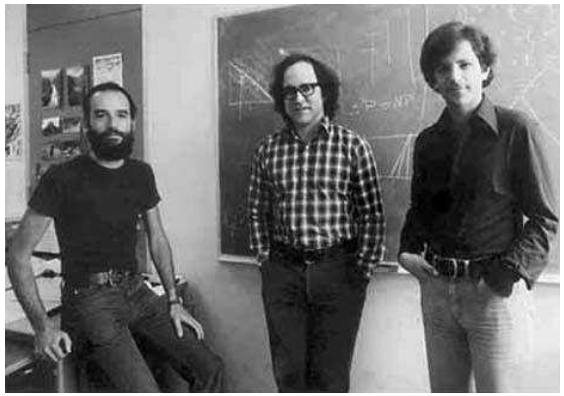
On suppose que $N = p \times q$ avec p, q nombres premiers (par ex. $N = 77 = 7 \times 11$).

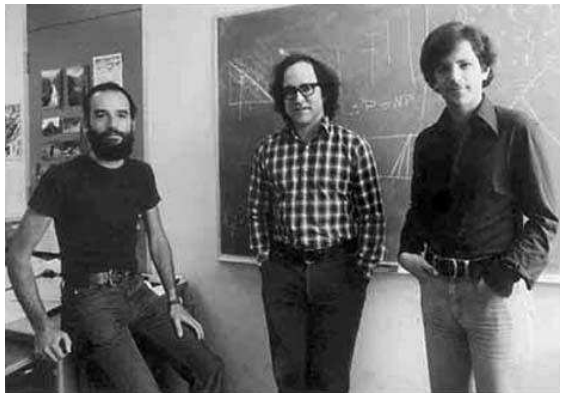
Théorème

Soit un entier $m \geq 1$ et e, d deux entiers tels que $ed \equiv 1\ [(p-1) \times (q-1)]$. Alors

$$m^{ed} \equiv m\ [N].$$

Et alors ? À quoi ça sert ?





"The era of "electronic mail" may soon be upon us ; we must ensure that two important properties of the current "paper mail" system are preserved : (a) messages are private, and (b) messages can be signed . We demonstrate in this paper how to build these capabilities into an electronic mail system."

Rivest, Shamir et Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, 1978.

Données du cryptosystème à clé publique RSA

1. Bob choisit deux très grands nombres premiers p et q puis forme leur produit $N = p \times q$.

Données du cryptosystème à clé publique RSA

1. Bob choisit deux très grands nombres premiers p et q puis forme leur produit $N = p \times q$.
2. Bob calcule $(p-1) \times (q-1)$ et choisit un entier e « convenable » (= tel que $\mathrm{pgcd}(e, (p-1) \times (q-1)) = 1$).

Données du cryptosystème à clé publique RSA

1. Bob choisit deux très grands nombres premiers p et q puis forme leur produit $N = p \times q$.
2. Bob calcule $(p-1) \times (q-1)$ et choisit un entier e « convenable » (= tel que $\mathrm{pgcd}(e, (p-1) \times (q-1)) = 1$).
3. Il calcule un entier d tel que $ed \equiv 1\ [(p-1) \times (q-1)]$ (ça existe !).

Données du cryptosystème à clé publique RSA

1. Bob choisit deux très grands nombres premiers p et q puis forme leur produit $N = p \times q$.
2. Bob calcule $(p-1) \times (q-1)$ et choisit un entier e « convenable » (= tel que $\mathrm{pgcd}(e, (p-1) \times (q-1)) = 1$).
3. Il calcule un entier d tel que $ed \equiv 1\ [(p-1) \times (q-1)]$ (ça existe !).
4. Il rend public le couple (N, e) et garde secret le couple $((p-1) \times (q-1), d)$.

Description des algorithmes de chiffrement/déchiffrement

1. La fonction de chiffrement de Bob (publique) est

$$\begin{array}{rcl} C : \{0,\dots,N-1\} & \longrightarrow & \{0,\dots,N-1\} \\ x & \longmapsto & x^e \ [N]. \end{array}$$

Description des algorithmes de chiffrement/déchiffrement

1. La fonction de chiffrement de Bob (publique) est

$$\begin{array}{rcl} C : \{0,\dots,N-1\} & \longrightarrow & \{0,\dots,N-1\} \\ x & \longmapsto & x^e \ [N]. \end{array}$$

2. La fonction de déchiffrement de Bob (privée) est

$$\begin{array}{rcl} D : \{0,\dots,N-1\} & \longrightarrow & \{0,\dots,N-1\} \\ x & \longmapsto & x^d \ [N]. \end{array}$$

Description des algorithmes de chiffrement/déchiffrement

1. La fonction de chiffrement de Bob (publique) est

$$\begin{array}{rcl} C : \{0,\dots,N-1\} & \longrightarrow & \{0,\dots,N-1\} \\ x & \longmapsto & x^e \ [N]. \end{array}$$

2. La fonction de déchiffrement de Bob (privée) est

$$\begin{array}{rcl} D : \{0,\dots,N-1\} & \longrightarrow & \{0,\dots,N-1\} \\ x & \longmapsto & x^d \ [N]. \end{array}$$

3. Par le théorème d'Euler-Fermat ces deux fonctions sont réciproques l'une de l'autre :

$$(C \circ D)(m) = m \quad \text{et} \quad (D \circ C)(M) = M$$

Description des algorithmes de chiffrement/déchiffrement

1. La fonction de chiffrement de Bob (publique) est

$$\begin{array}{rcl} C : \{0,\dots,N-1\} & \longrightarrow & \{0,\dots,N-1\} \\ x & \longmapsto & x^e \ [N]. \end{array}$$

2. La fonction de déchiffrement de Bob (privée) est

$$\begin{array}{rcl} D : \{0,\dots,N-1\} & \longrightarrow & \{0,\dots,N-1\} \\ x & \longmapsto & x^d \ [N]. \end{array}$$

3. Par le théorème d'Euler-Fermat ces deux fonctions sont réciproques l'une de l'autre :

$$(C \circ D)(m) = m \quad \text{et} \quad (D \circ C)(M) = M$$

4. L'une et l'autre sont très faciles à calculer mais il est impossible en pratique de trouver D à partir de C (et vice-versa).

Pourquoi l'algorithme RSA est-il robuste ?

Pourquoi l'algorithme RSA est-il robuste ?

Connaître la fonction D, c'est connaître l'entier d.

Pourquoi l'algorithme RSA est-il robuste ?

Connaître la fonction D, c'est connaître l'entier d. Or, *a priori* connaître d n'est possible (et facile) qu'à partir de la connaissance de la factorisation de l'entier N.

Pourquoi l'algorithme RSA est-il robuste ?

Connaître la fonction D, c'est connaître l'entier d. Or, *a priori* connaître d n'est possible (et facile) qu'à partir de la connaissance de la factorisation de l'entier N. Mais c'est *à l'heure actuelle* algorithmiquement infaisable !

Pourquoi l'algorithme RSA est-il robuste ?

Connaître la fonction D, c'est connaître l'entier d. Or, *a priori* connaître d n'est possible (et facile) qu'à partir de la connaissance de la factorisation de l'entier N. Mais c'est *à l'heure actuelle* algorithmiquement infaisable !
En décembre 2009, le nombre RSA-768 (232 chiffres en écriture décimale) a été factorisé (par une équipe menée par Kleinjung) :

Pourquoi l'algorithme RSA est-il robuste ?

Connaître la fonction D, c'est connaître l'entier d. Or, *a priori* connaître d n'est possible (et facile) qu'à partir de la connaissance de la factorisation de l'entier N. Mais c'est *à l'heure actuelle* algorithmiquement infaisable !
En décembre 2009, le nombre RSA-768 (232 chiffres en écriture décimale) a été factorisé (par une équipe menée par Kleinjung) :

$$123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3$$

Pourquoi l'algorithme RSA est-il robuste ?

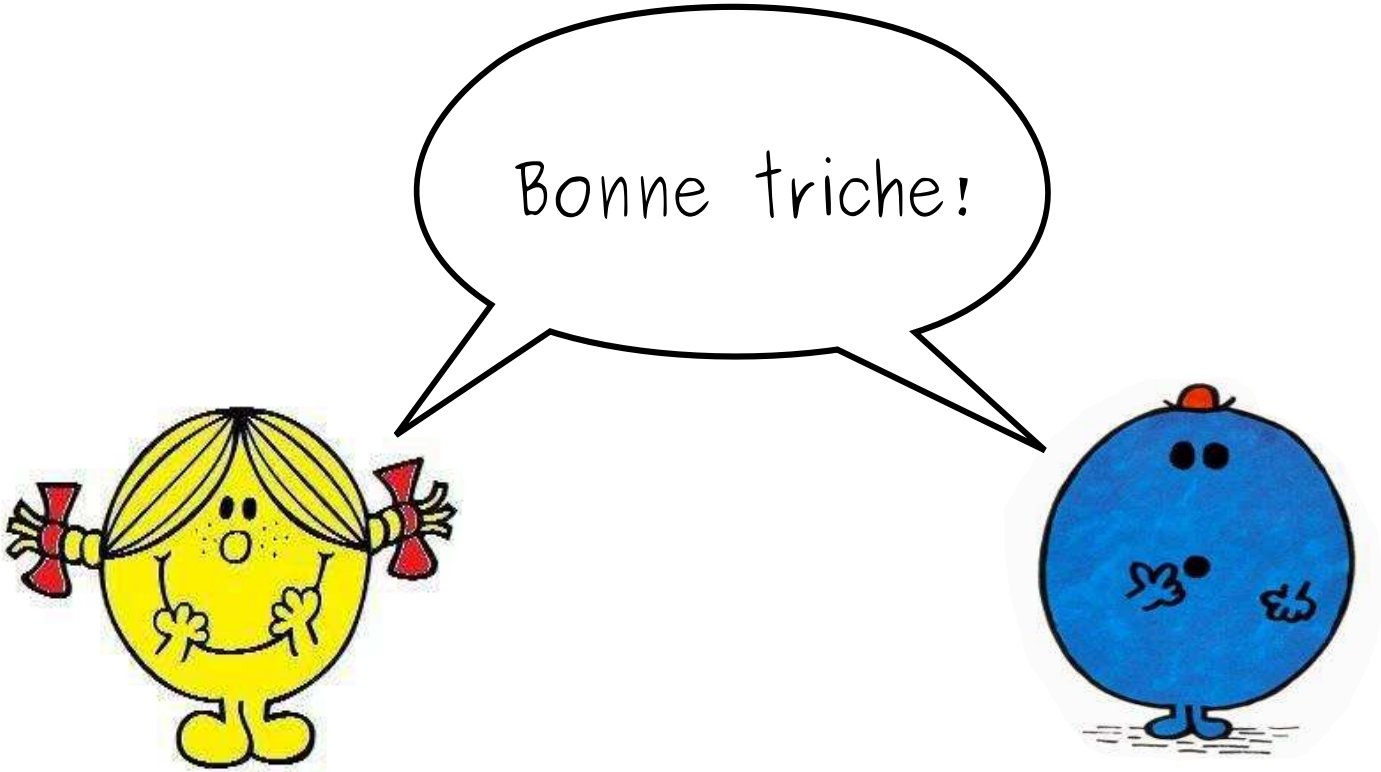
Connaître la fonction D, c'est connaître l'entier d. Or, *a priori* connaître d n'est possible (et facile) qu'à partir de la connaissance de la factorisation de l'entier N. Mais c'est *à l'heure actuelle* algorithmiquement infaisable !
En décembre 2009, le nombre RSA-768 (232 chiffres en écriture décimale) a été factorisé (par une équipe menée par Kleinjung) :

$$123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3$$

Sur un ordinateur personnel (2.2GHz-Opteron-CPU), leurs calculs auraient nécessité 2000 ans !

Sommaire

- F. Bayart, *La Cryptogr@phie expliquée*, `www.bibmath.net/crypto/`
- J. Stern, *La Science du secret*, Odile Jacob, 1979.
- S. Singh, *Histoire des codes secrets*, Le livre de Poche, 2001 (Traduction de *The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Ed., 2000).
- Le site de la société RSA : `www.emc.com/domains/rsa/`
- Le site de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : `www.ssi.gouv.fr/`


Bonne triche!

Sur le chiffrement par substitution

- Combien y a-t-il de permutations de l'alphabet ?

Sur le chiffrement par substitution

- Combien y a-t-il de permutations de l'alphabet ?
- Comment procéder pour « casser » un chiffrement par substitution ?

Sur le chiffrement par substitution

- Combien y a-t-il de permutations de l'alphabet ?
- Comment procéder pour « casser » un chiffrement par substitution ?
- Le chiffrement par substitution est-il sûr ?

Sur le fonctionnement d'un cryptosystème à clé publique

- Comment Alice peut-elle « signer » son message ?

Sur le fonctionnement d'un cryptosystème à clé publique

- Comment Alice peut-elle « signer » son message ?
- Le chiffrement par substitution peut-il constituer un cryptosystème à clé publique ?

Sur le système RSA

- Existe-t-il une infinité de nombres premiers ?

Sur le système RSA

- Existe-t-il une infinité de nombres premiers ?
- Est-il facile de construire des grands nombres premiers ?

Sur le système RSA

- Existe-t-il une infinité de nombres premiers ?
- Est-il facile de construire des grands nombres premiers ?
- Les nombres premiers p et q peuvent-ils être choisis au hasard ?

Sur le système RSA

- Existe-t-il une infinité de nombres premiers ?
- Est-il facile de construire des grands nombres premiers ?
- Les nombres premiers p et q peuvent-ils être choisis au hasard ?
- Comment Alice peut-elle signer son message ?

Sur le système RSA

- Existe-t-il une infinité de nombres premiers ?
- Est-il facile de construire des grands nombres premiers ?
- Les nombres premiers p et q peuvent-ils être choisis au hasard ?
- Comment Alice peut-elle signer son message ?
- Peut-on casser le système RSA autrement qu'en factorisant N ?

Sur le système RSA

- Existe-t-il une infinité de nombres premiers ?
- Est-il facile de construire des grands nombres premiers ?
- Les nombres premiers p et q peuvent-ils être choisis au hasard ?
- Comment Alice peut-elle signer son message ?
- Peut-on casser le système RSA autrement qu'en factorisant N ?
- La factorisation des grands nombres est-elle une tâche aisée ?