CryptoExperts

WE INNOVATE TO SECURE YOUR BUSINESS

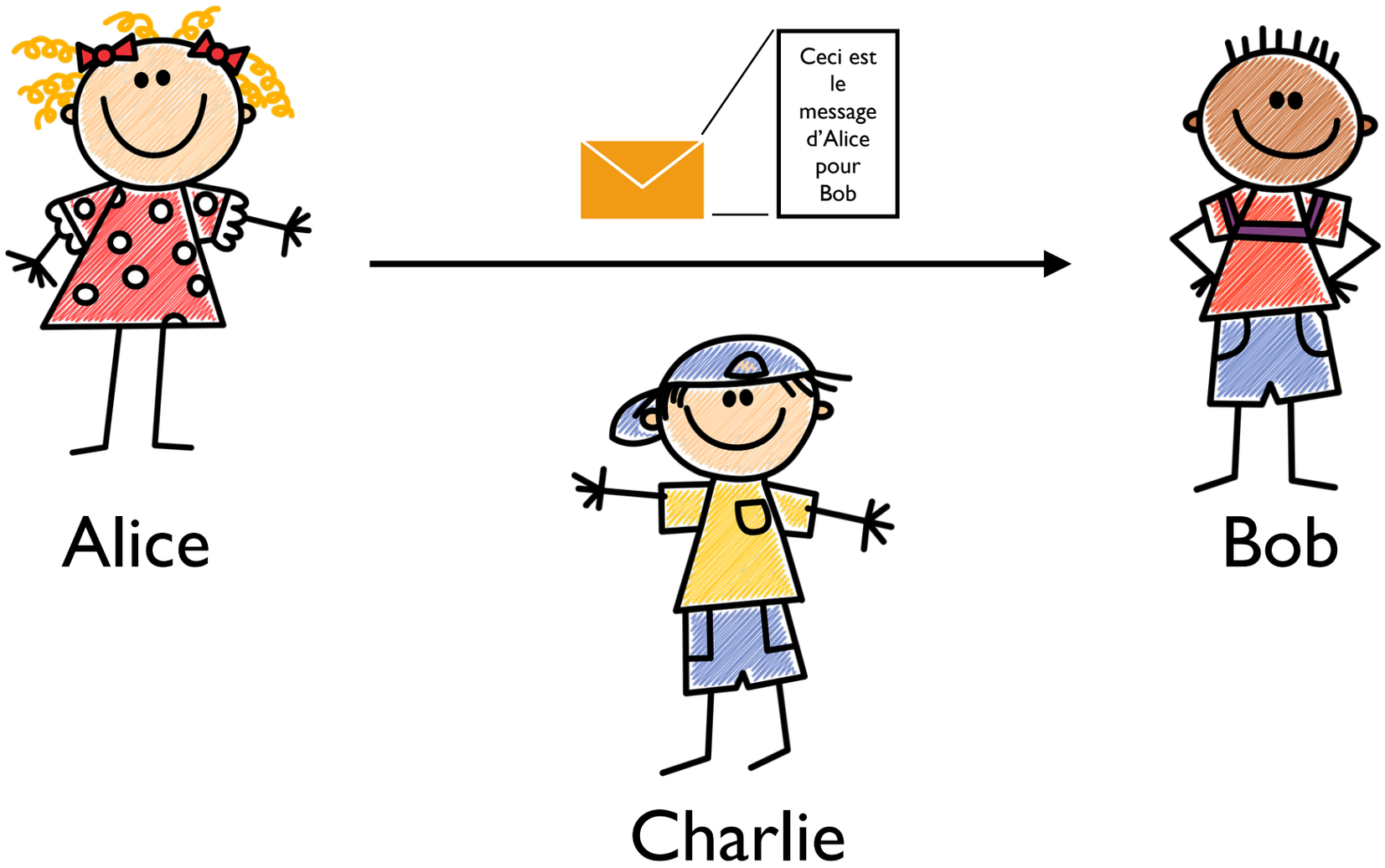
Introduction à la cryptographie

Sonia Belaïd

Tunis, 3 janvier 2025

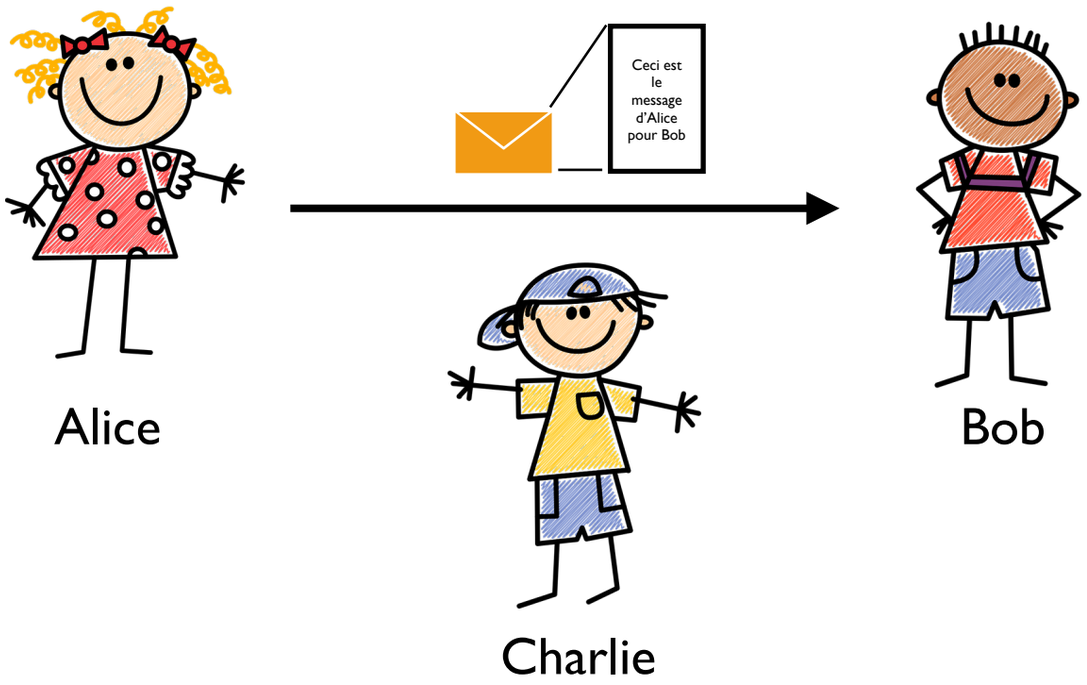
Qu’est-ce que la cryptographie ?

Qu'est-ce que la cryptographie ?



Définition : La cryptographie est la science et l'art de protéger les informations, malgré les attaques extérieures

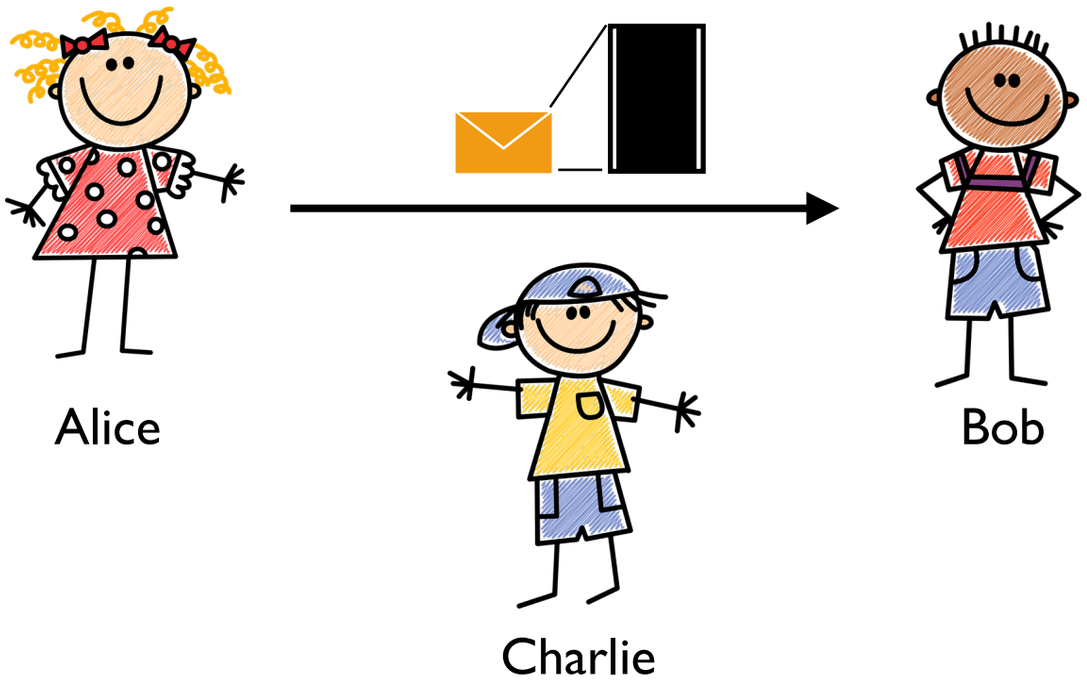
Qu’est-ce que la cryptographie ?



3 objectifs principaux

- Confidentialité
- Authentification
- Intégrité

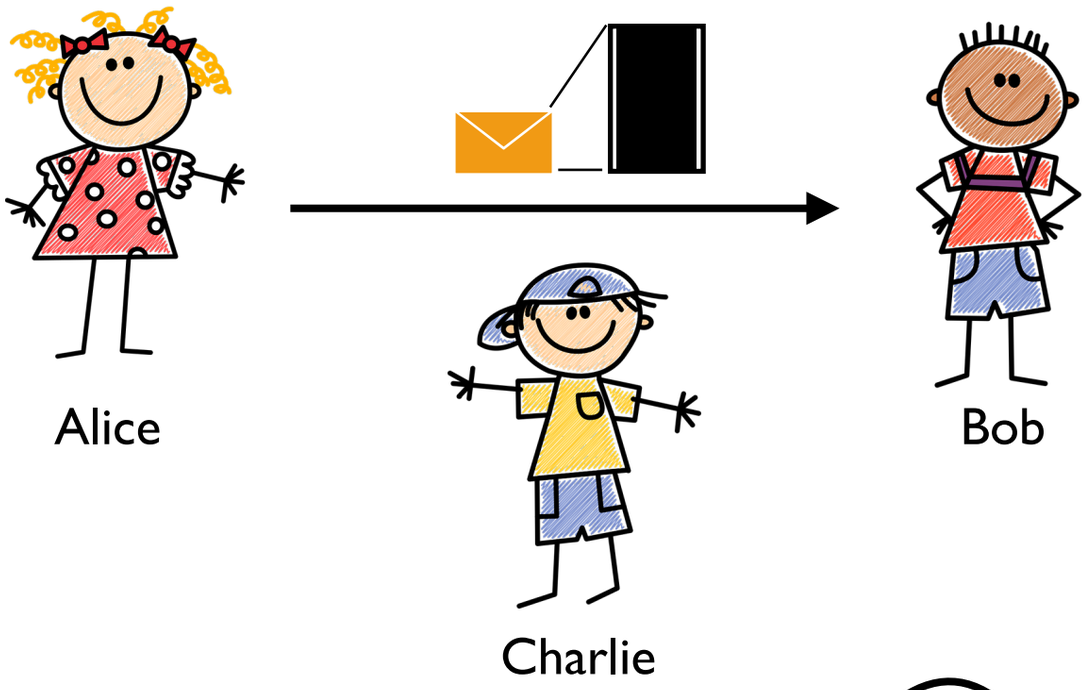
Qu'est-ce que la cryptographie ?



3 objectifs principaux

- **Confidentialité**
- Authentification
- Intégrité

Qu'est-ce que la cryptographie ?

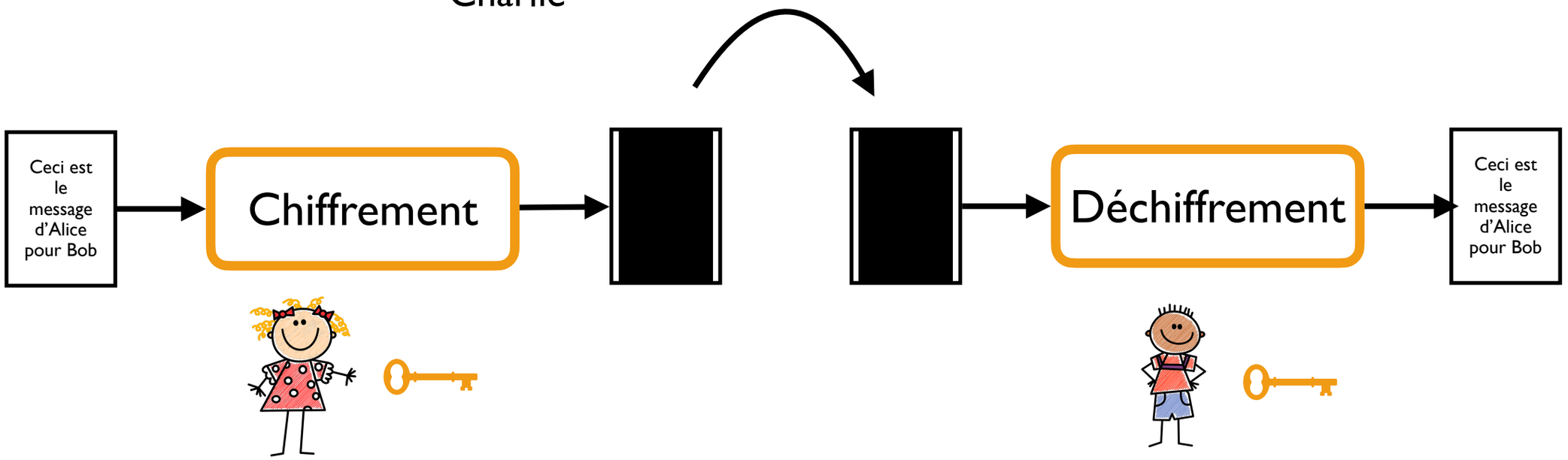


3 objectifs principaux

Confidentialité

Authentification

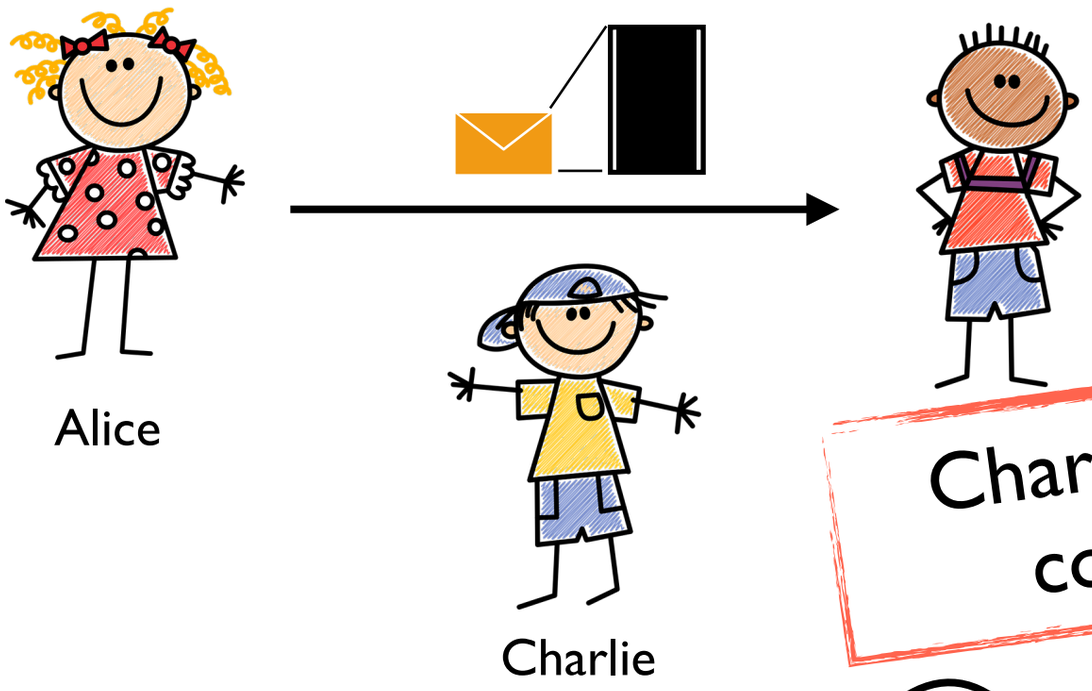
Intégrité



CryptoExperts

Qu'est-ce que la cryptographie ?

3 objectifs principaux

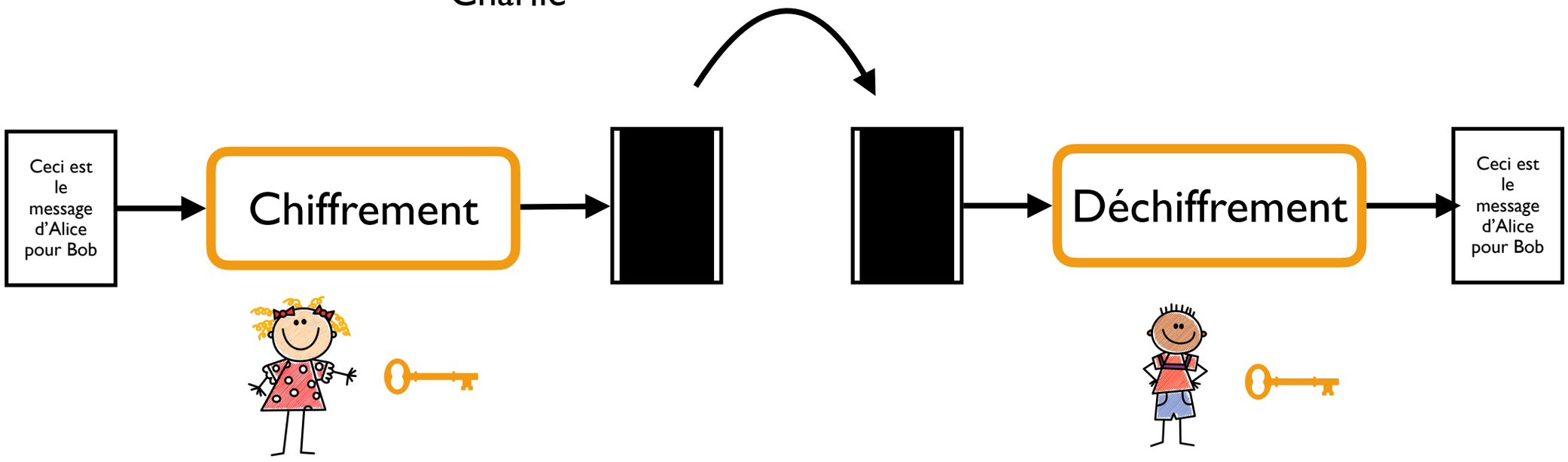


Confidentialité

tion

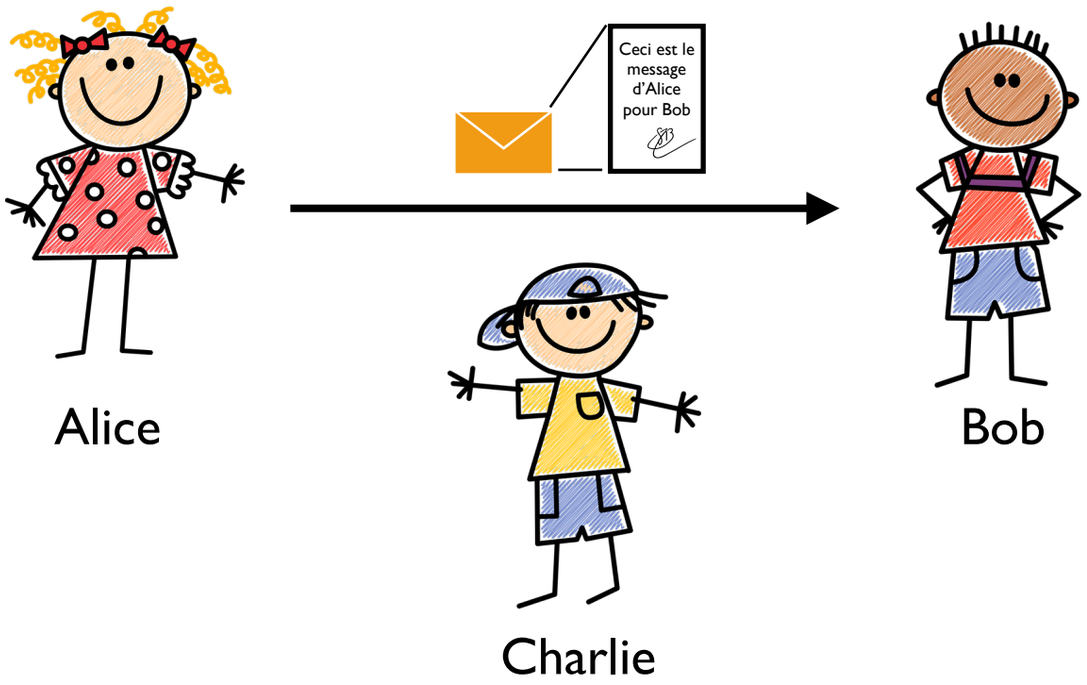
Charlie ne peut pas lire le contenu du message

Intégrité



CryptoExperts

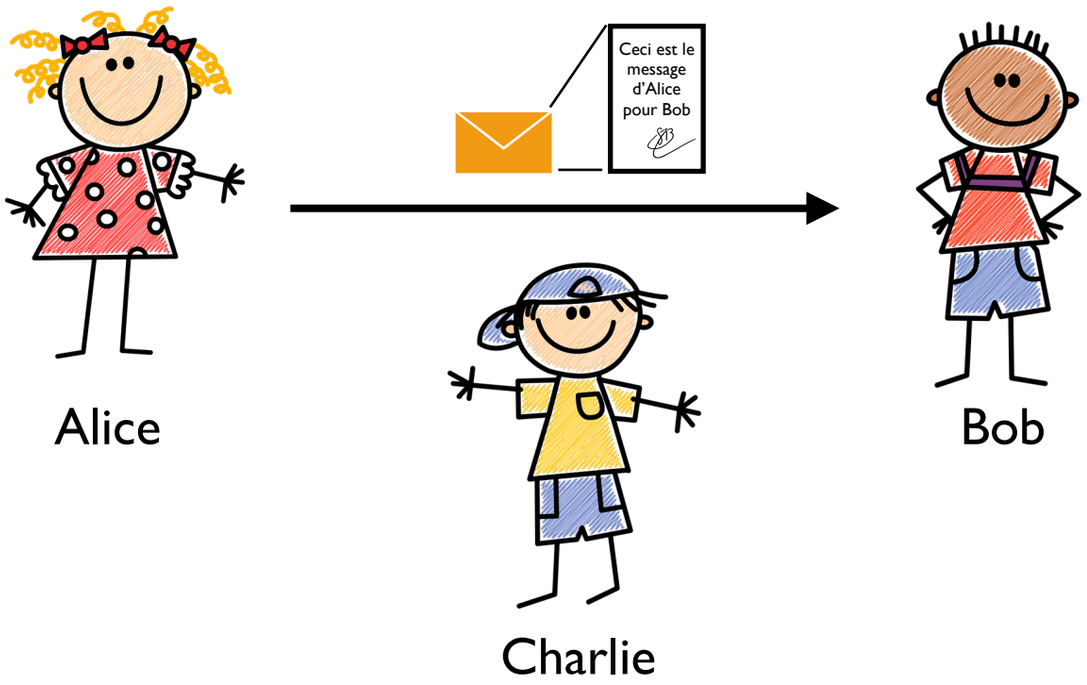
Qu'est-ce que la cryptographie ?



3 objectifs principaux

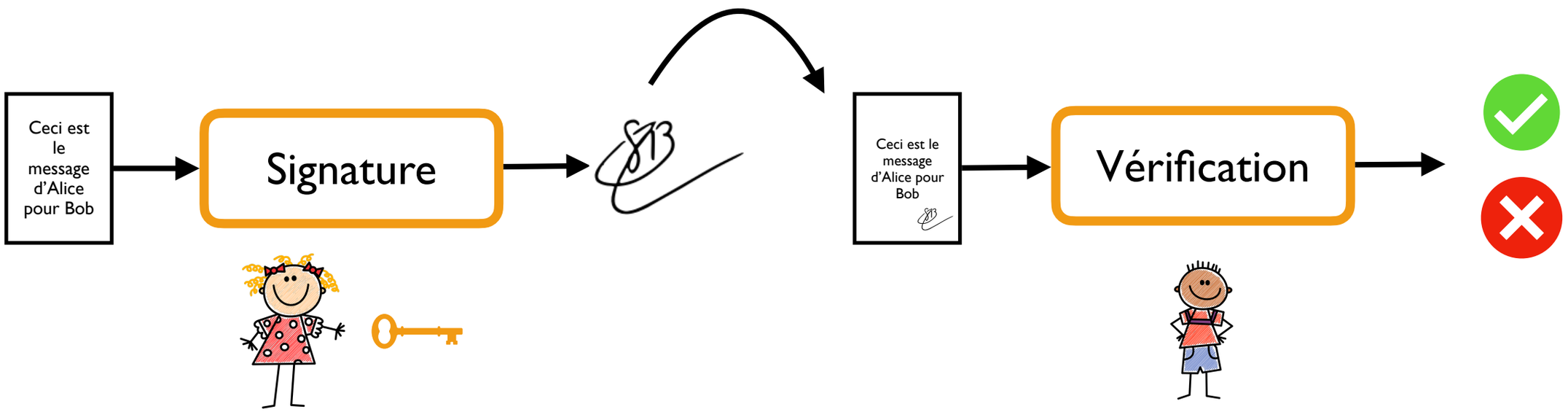
- Confidentialité
- **Authentification**
- Intégrité

Qu’est-ce que la cryptographie ?



3 objectifs principaux

- Confidentialité
- Authentification
- Intégrité

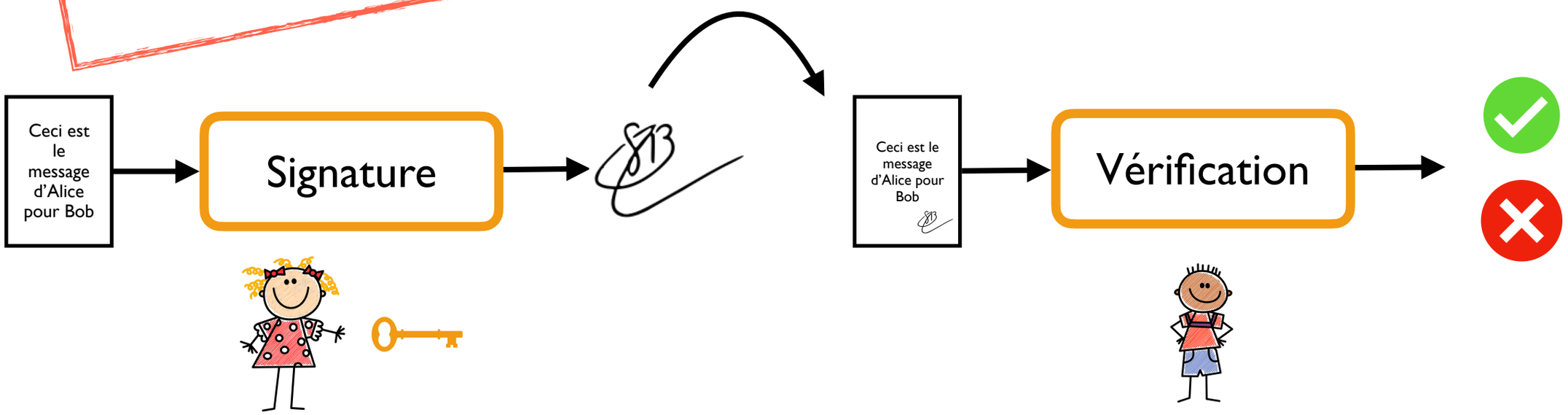


CryptoExperts

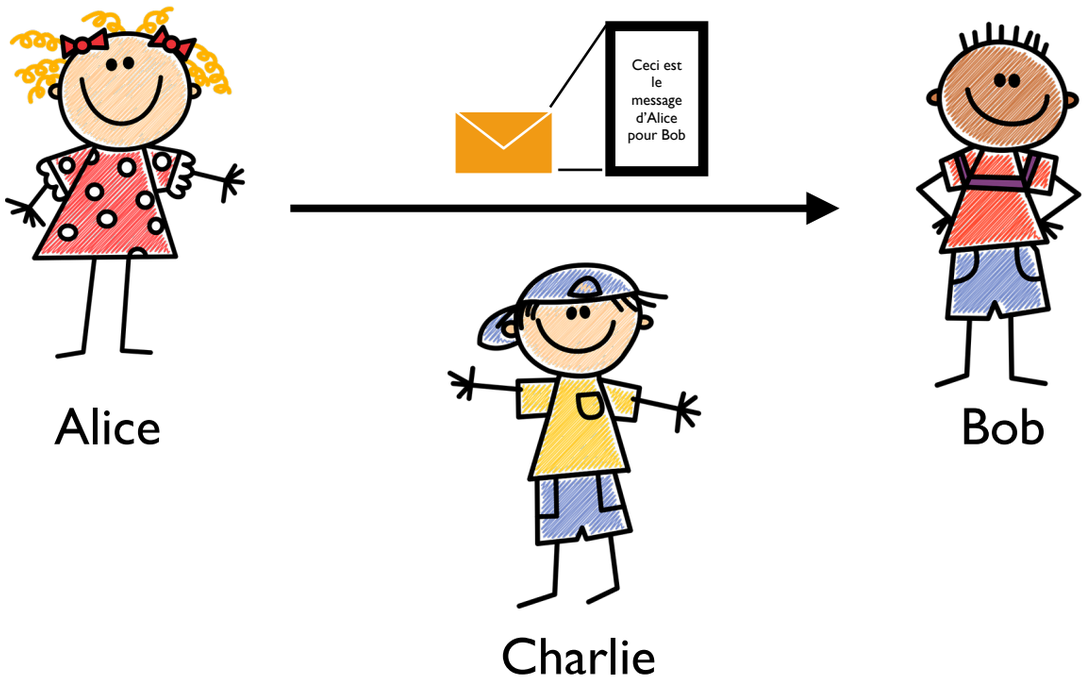
Qu’est-ce que la cryptographie ?

3 objectifs principaux

- Confidentialité
- **Authentification**
- Intégrité



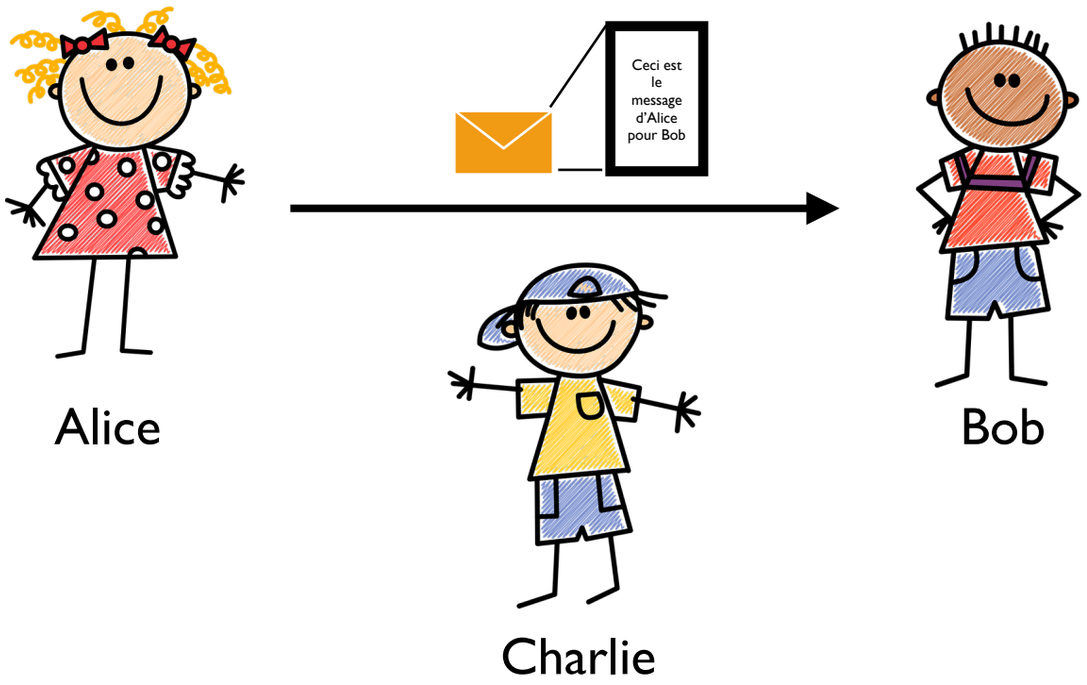
Qu’est-ce que la cryptographie ?



3 objectifs principaux

- Confidentialité
- Authentification
- Intégrité

Qu’est-ce que la cryptographie ?

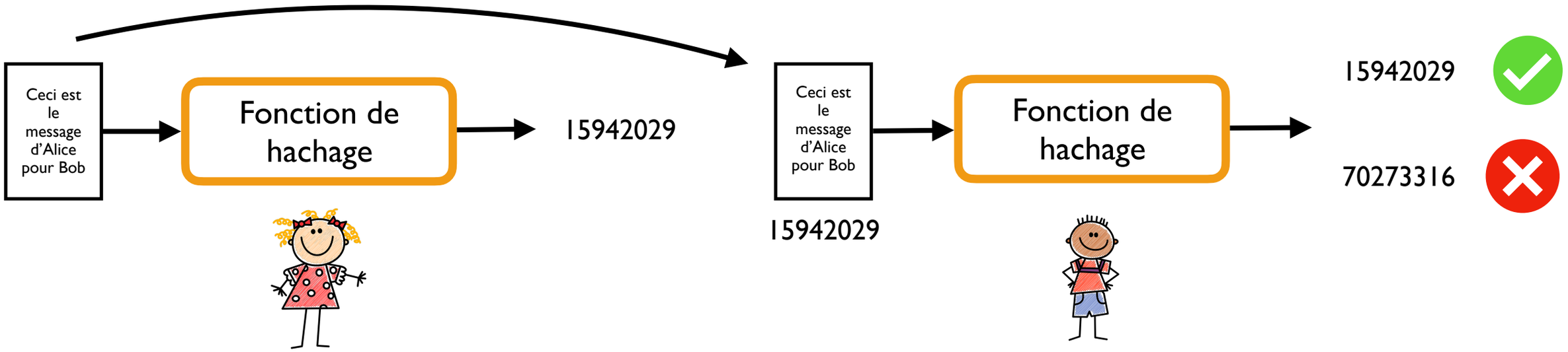


3 objectifs principaux

Confidentialité

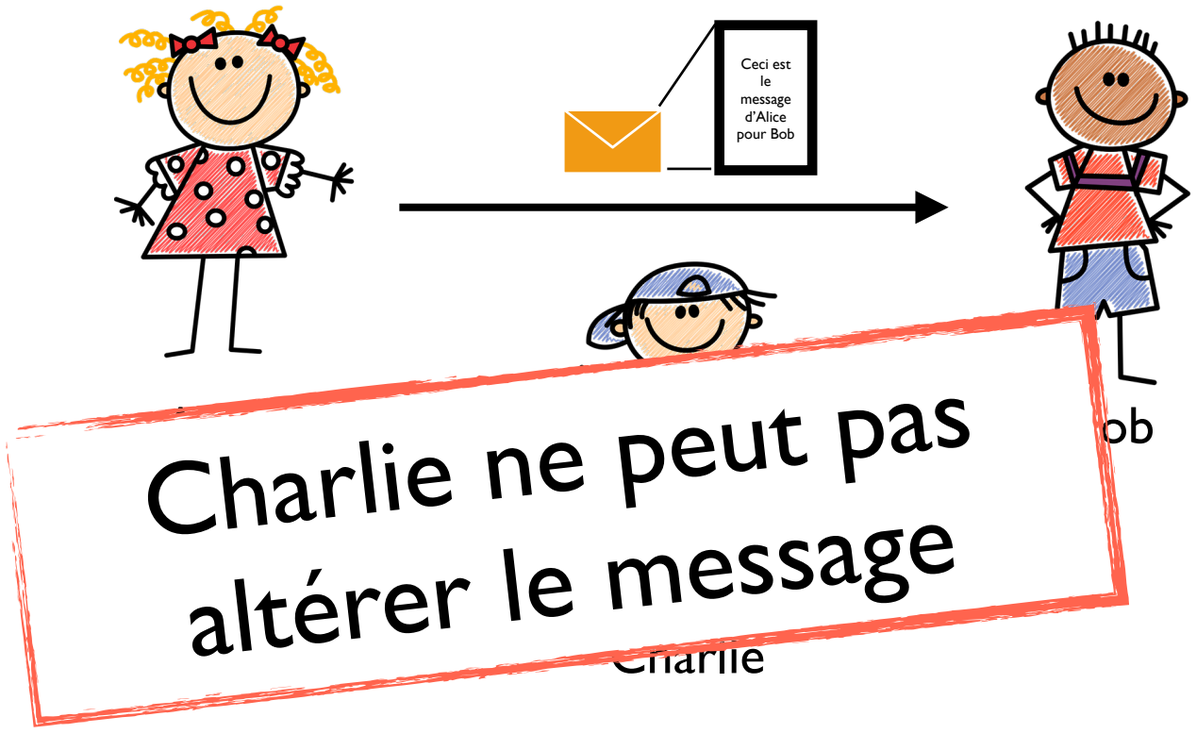
Authentification

Intégrité



CryptoExperts

Qu'est-ce que la cryptographie ?

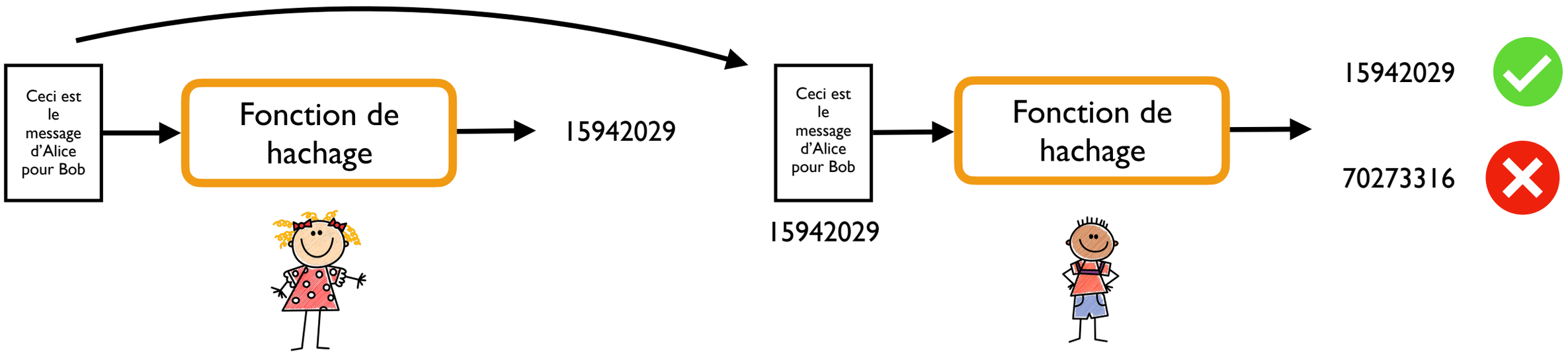


3 objectifs principaux

Confidentialité

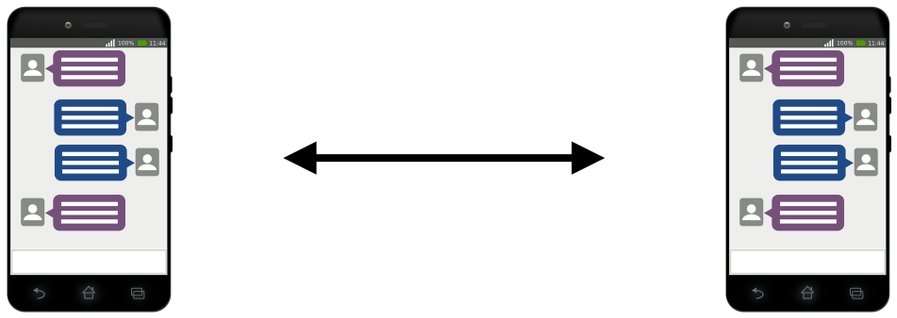
Authentification

Intégrité



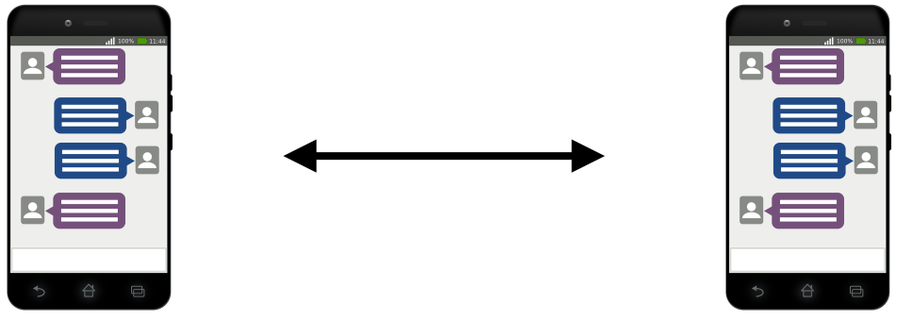
CryptoExperts

La cryptographie dans notre quotidien



Messageries sécurisées : chiffrement de bout en bout pour protéger les messages échangés

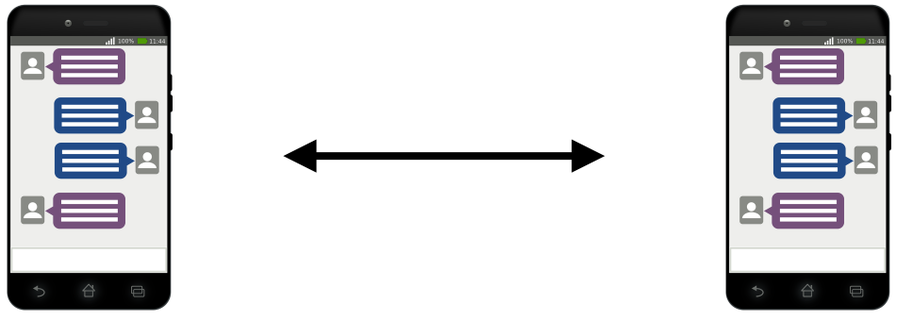
La cryptographie dans notre quotidien



Messageries sécurisées : chiffrement de bout en bout pour protéger les messages échangés

Sites Web sécurisés (HTTPS) : chiffrement des connexions et des données sensibles (e.g., données bancaires) entre le navigateur et les serveurs

La cryptographie dans notre quotidien



Messageries sécurisées : chiffrement de bout en bout pour protéger les messages échangés

Sites Web sécurisés (HTTPS) : chiffrement des connexions et des données sensibles (e.g., données bancaires) entre le navigateur et les serveurs

Crypto-monnaies : la technologie blockchain utilise la cryptographie pour sécuriser les transactions et contrôler la création de nouvelles unités monétaires.

La cryptographie de l'antiquité à nos jours

Histoire de la cryptographie

Chiffrement de César

Stéganographie

Chiffrement de Vigenère

Enigma

Cryptographie moderne

0 500 1000 1500 2000

*Image extraite de https://www.cryptomuseum.com/crypto/enigma/g/index.htm

Histoire de la cryptographie

Chiffrement de César

Chiffrement de Vigenère

Stéganographie

Enigma

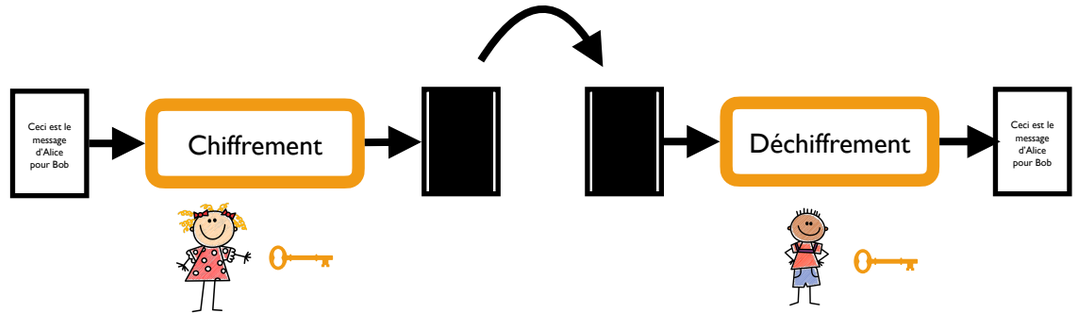
Cryptographie moderne

0 500 1000 1500 2000

*Image extraite de https://www.cryptomuseum.com/crypto/enigma/g/index.htm

Chiffrement de César

Principe : décaler chaque lettre du message de x positions dans l'alphabet.



Exemple : on choisit un décalage de $x = 3$

A → D, B → E, C → F, …

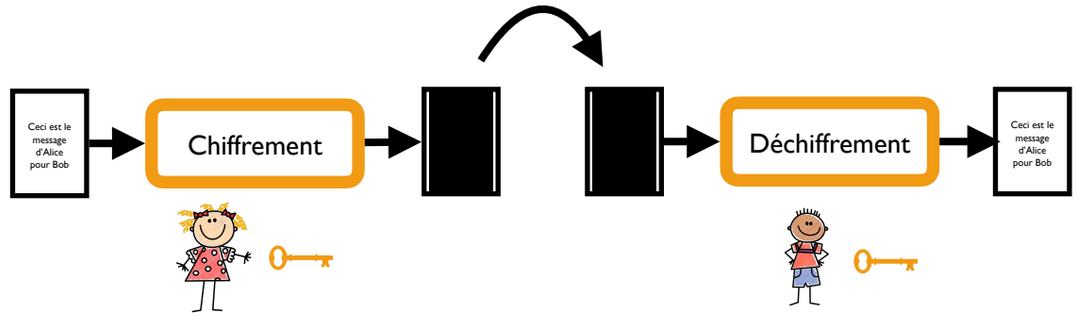
J'AIME LA CRYPTOGRAPHIE

+3 ↓

M'DLPH OD FUBSWRJUDSKLH

Chiffrement de César

Principe : décaler chaque lettre du message de x positions dans l'alphabet.



Exemple : on choisit un décalage de $x = 3$

$$A \rightarrow D,\ B \rightarrow E,\ C \rightarrow F,\ \ldots$$

Inconvénients / Attaques : Recherche exhaustive : 25 possibilités seulement

Chiffrement par substitution

Chiffrement de César (décalage de $x = 3$)

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
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

Autre substitution (clavier qwerty)

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

J’AIME LA CRYPTOGRAPHIE

↓

P’QODT SQ EUNHZGUKQHIOT

Chiffrement par substitution

Chiffrement de César (décalage de $x = 3$)

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
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

Autre substitution (clavier qwerty)

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

Inconvénients / Attaques

Chiffrement par substitution

Chiffrement de César (décalage de $x = 3$)

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
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

Autre substitution (clavier qwerty)

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

Inconvénients / Attaques

Recherche exhaustive ? $\Rightarrow$ $26! \approx 2^{88}$ possibilités, soit environ 10 milliards d'années pour un ordinateur cadencé à 1GHz

Chiffrement par substitution

Chiffrement de César (décalage de $x = 3$)

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

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

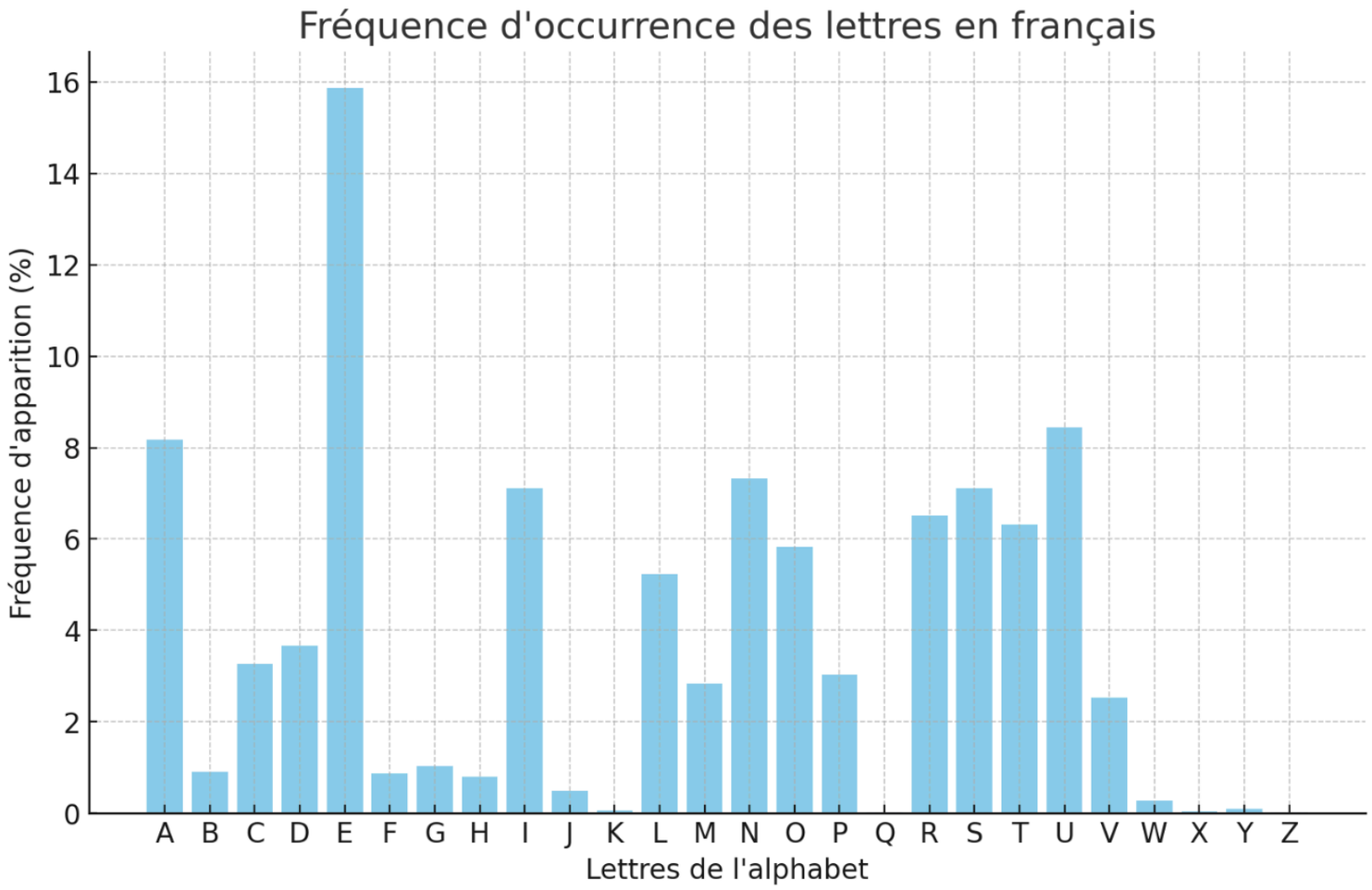
Autre substitution (cla

A B C D E F G H I -

Q W E R T Y U I O P

Inconvénients / Attaques

Analyse fréquentielle ⇒



Histoire de la cryptographie

Chiffrement de César

Chiffrement de Vigenère

Enigma

Cryptographie moderne

Stéganographie

0

500

1000

1500

2000

*Image extraite de https://www.cryptomuseum.com/crypto/enigma/g/index.htm

Stéganographie

Principe : *cacher* un message → la méthode (ou l'algorithme) constitue le secret

Ecriture sur le cuir chevelu des messagers

Encre invisible

Texte caché dans un livre

Stéganographie

Principe : *cacher* un message → la méthode (ou l'algorithme) constitue le secret

Musique, tu me fus un palais enchanté
Au seuil duquel menaient d'insignes avenues
Nuit et jour, des vitraux aux flammes continues,
Glissait une adorable et vibrante clarté.

Et des chœurs alternant, – dames de volupté,
Oréades, ondins, faunes, prêtresses nues, –
Toute la joie ardente essorait vers les nues,
Et toute la langueur et toute la beauté.

Sur un seul vœu de moi, désir chaste ou lyrique,
Ta fertile magie a toujours, ô musique :
Bercé mon tendre songe ou mon brillant désir.

Et quand viendra l'instant ténébreux et suprême,
Tu sauras me donner le bonheur de mourir,
En refermant les bras sur le Rêve que j'aime !

Sonnet publié par Auguste Mangeot publia dans Le *Monde musical*, envoyé par un correspondant anonyme

Stéganographie

Principe : *cacher* un message → la méthode (ou l'algorithme) constitue le secret

Musique, tu me fus un palais enchanté
Au seuil duquel menaient d'insignes avenues
Nuit et jour, des vitraux aux flammes continues,
Glissait une adorable et vibrante clarté.

Et des chœurs alternant, – dames de volupté,
Oréades, ondins, faunes, prêtresses nues, –
Toute la joie ardente essorait vers les nues,
Et toute la langueur et toute la beauté.

Sur un seul vœu de moi, désir chaste ou lyrique,
Ta fertile magie a toujours, ô musique :
Bercé mon tendre songe ou mon brillant désir.

Et quand viendra l'instant ténébreux et suprême,
Tu sauras me donner le bonheur de mourir,
En refermant les bras sur le Rêve que j'aime !

Sonnet publié par Auguste Mangeot publia dans Le *Monde musical*, envoyé par un correspondant anonyme

Histoire de la cryptographie

Chiffrement de César

Chiffrement de Vigenère

Stéganographie

Enigma

Cryptographie moderne

0

500

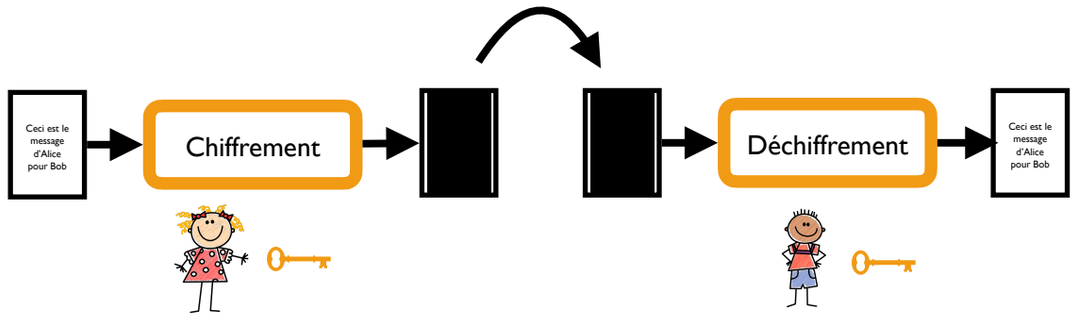
1000

1500

2000

*Image extraite de https://www.cryptomuseum.com/crypto/enigma/g/index.htm

Chiffrement de Vigenère



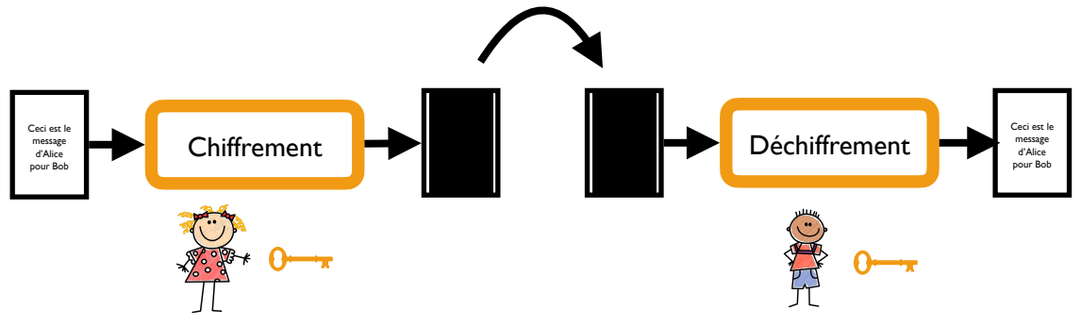
Principe : chiffrement par substitution avec une clef

Exemple : on choisit une clef, par exemple « CLEF »

J’AIME LA CRYPTOGRAPHIE

C’LEFC LE FCLEFCLEFCLEF

Chiffrement de Vigenère



Principe : chiffrement par substitution avec une clef

Exemple : on choisit une clef, par exemple « CLEF »

+2

J'AIME LA CRYPTOGRAPHIE

C'LEFC LE FCLEFCLEFCLEF

L'LMRG WE HTJTYQRVFRSMJ

Histoire de la cryptographie

Chiffrement de César

Stéganographie

Chiffrement de Vigenère

Enigma

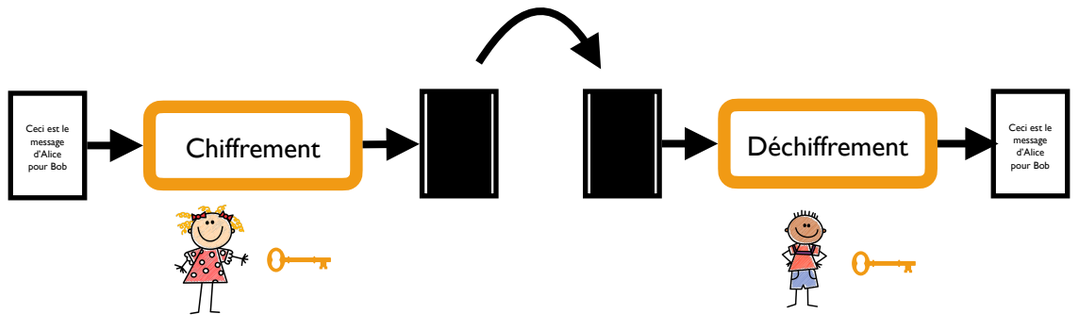
Cryptographie moderne

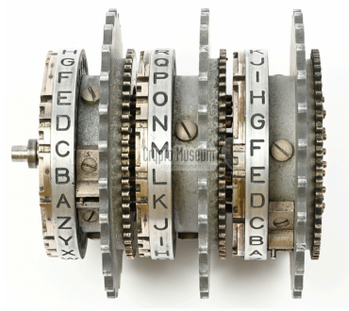
0 500 1000 1500 2000

*Image extraite de https://www.cryptomuseum.com/crypto/enigma/g/index.htm

Enigma

- Machine Enigma
  - Inventée en 1918 par Arthur Scherbius.
  - Utilisée par les forces armées allemandes pendant la Seconde Guerre mondiale.
  - But : Chiffrer des messages.
- Fonctionnement
  - Rotors : Utilisés pour substituer les lettres du message de manière dynamique
  - Clef : Configuration des rotors et positions initiales.
- Vulnérabilités
  - Enigma a été cassée grâce au travail de Alan Turing et de son équipe.
  - La cryptanalyse d'Enigma a contribué à écourter la guerre et a marqué un tournant dans l'histoire de la cryptologie.





*Images extraites de https://www.cryptomuseum.com/crypto/enigma/g/index.htm

Histoire de la cryptographie

Chiffrement de César

Stéganographie

Chiffrement de Vigenère

Enigma

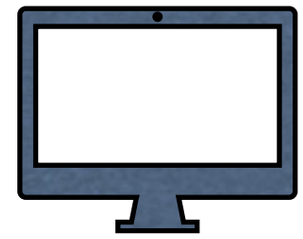
Cryptographie moderne

0 500 1000 1500 2000

*Image extraite de https://www.cryptomuseum.com/crypto/enigma/g/index.htm

Et aujourd'hui ?

- Moyens : Essor des ordinateurs et de l'informatique dans les années 70

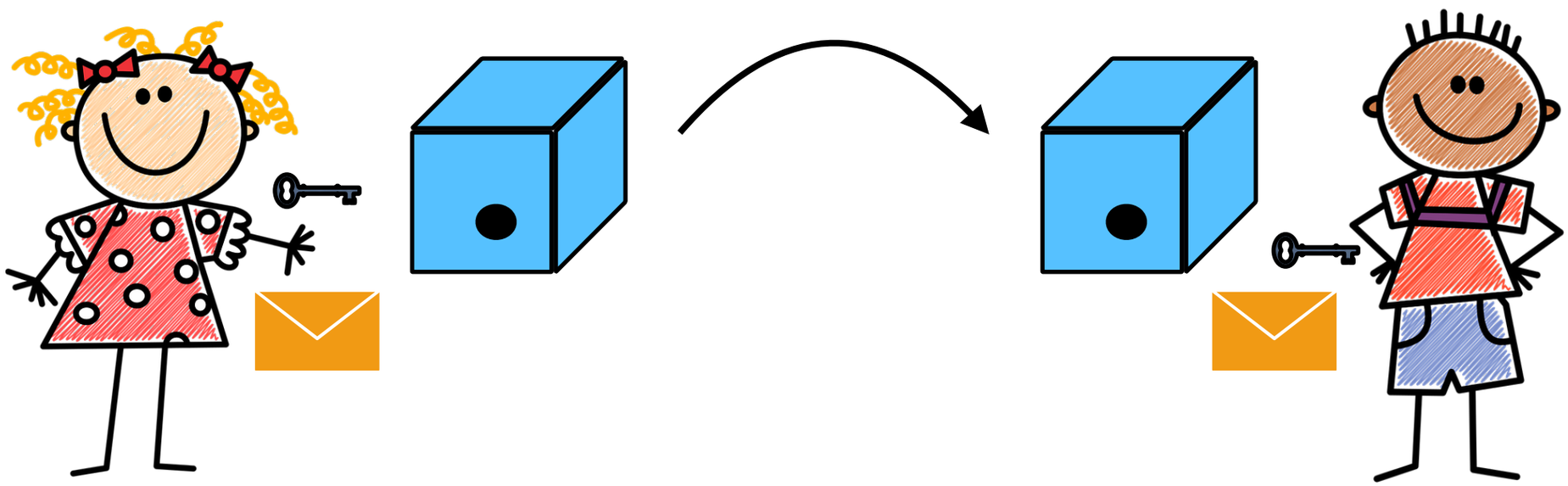


- Nouveaux défis : Sécuriser les communications sur des réseaux mondiaux (ex : Internet)

Cryptographie symétrique

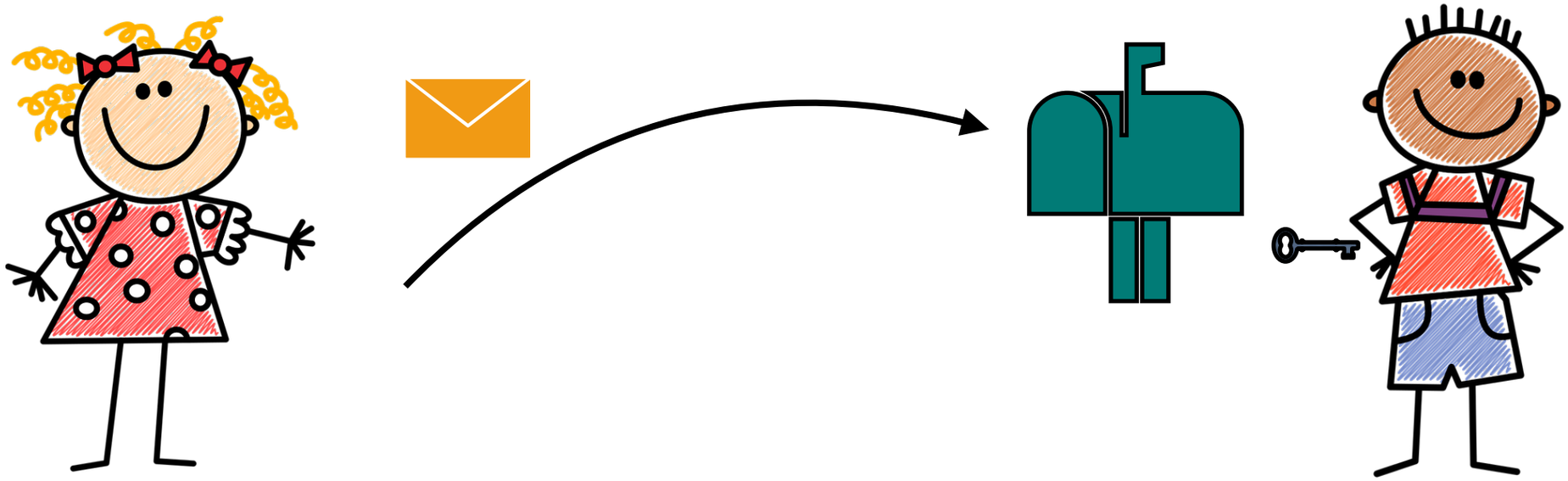
- Principe : Utilisation d'une clef secrète partagée entre l'émetteur et le récepteur
- Exemples : Chiffrement de César, chiffrement de Vigenère, et maintenant le standard AES (Advanced Encryption Standard)

🔑 - Clef secrète partagée : grand nombre de 128, 192 ou 256 bits

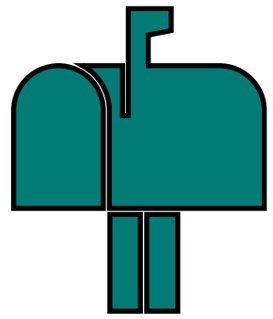


Cryptographie asymétrique

- Origines
  - Échange de clef Diffie-Hellman en 1976
  - Chiffrement RSA (Rivest, Shamir et Adleman) en 1977
- Principe : utilisation d'une fonction mathématique *à sens unique*
  - Clef publique (par exemple, l'adresse de Bob)
  - Clef privée (par exemple, la clef de boîte aux lettres de Bob)

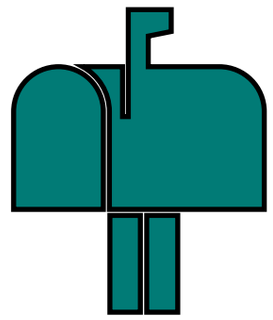


Cryptographie asymétrique



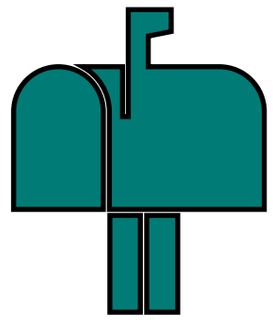
- Principaux problèmes mathématiques
  - La factorisation de grands entiers
  - Le logarithme discret
- Exemple : factorisation d'un produits de nombres premiers
  - $21 = \ ?$

Cryptographie asymétrique



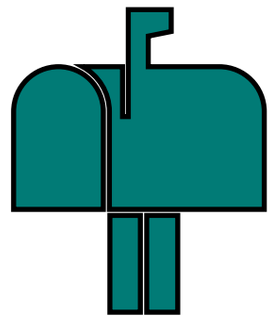
- Principaux problèmes mathématiques
  - La factorisation de grands entiers
  - Le logarithme discret
- Exemple : factorisation d'un produits de nombres premiers
  - $21 = 3 \times 7$

Cryptographie asymétrique



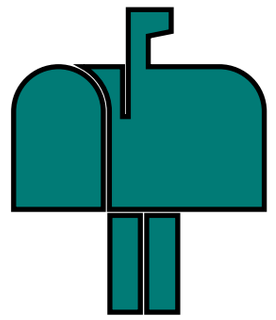
- Principaux problèmes mathématiques
  - La factorisation de grands entiers
  - Le logarithme discret
- Exemple : factorisation d'un produits de nombres premiers
  - $21 = 3 \times 7$
  - $187 = ?$

Cryptographie asymétrique



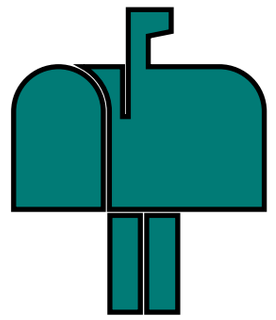
- Principaux problèmes mathématiques
  - La factorisation de grands entiers
  - Le logarithme discret
- Exemple : factorisation d'un produits de nombres premiers
  - $21 = 3 \times 7$
  - $187 = 11 \times 17$

Cryptographie asymétrique



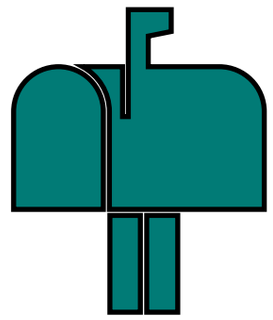
- Principaux problèmes mathématiques
  - La factorisation de grands entiers
  - Le logarithme discret
- Exemple : factorisation d'un produits de nombres premiers
  - $21 = 3 \times 7$
  - $187 = 11 \times 17$
  - $2623 = ?$

Cryptographie asymétrique



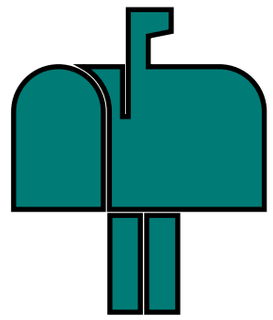
- Principaux problèmes mathématiques
  - La factorisation de grands entiers
  - Le logarithme discret
- Exemple : factorisation d'un produits de nombres premiers
  - $21 = 3 \times 7$
  - $187 = 11 \times 17$
  - $2623 = 43 \times 61$

Cryptographie asymétrique



- Principaux problèmes mathématiques
  - La factorisation de grands entiers
  - Le logarithme discret
- Exemple : factorisation d'un produits de nombres premiers
  - $21 = 3 \times 7$
  - $187 = 11 \times 17$
  - $2623 = 43 \times 61$
  - $79272739271639267827560599152164840663$?

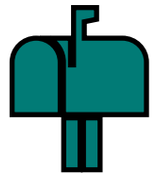
Cryptographie asymétrique



- Principaux problèmes mathématiques
  - La factorisation de grands entiers
  - Le logarithme discret
- Exemple : factorisation d'un produits de nombres premiers
  - $21 = 3 \times 7$
  - $187 = 11 \times 17$
  - $2623 = 43 \times 61$
  - $79272739271639267827560599152164840663$?

RSA : clef privée contient deux premiers p et q
clef publique contient $N = p \times q$

Chiffrement RSA

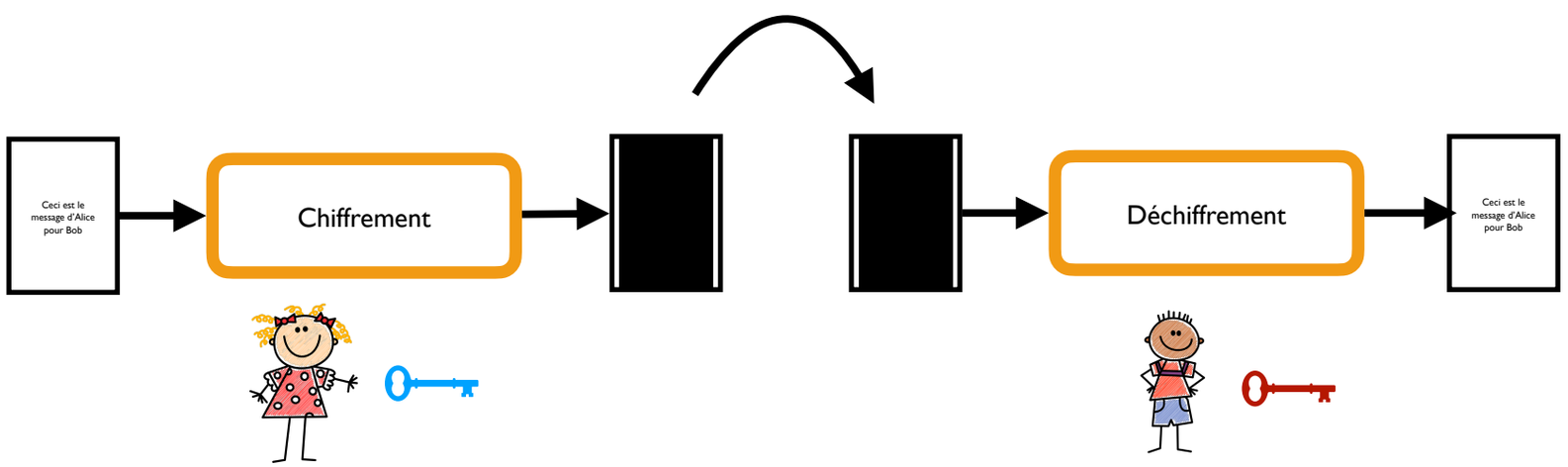


Bob choisit : $p = 3$ et $q = 11$

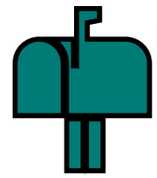
Bob calcule $N = p \times q = 33$ et
$\phi(N) = (p-1) \times (q-1) = 20$

Bob choisit un premier avec $\phi(N)$: $e = 3$

Bob calcule $d = e^{-1} \mod \phi(N) = 7$



Chiffrement RSA



Bob choisit : $p = 3$ et $q = 11$

Bob calcule $N = p \times q = 33$ et
$\phi(N) = (p-1) \times (q-1) = 20$

Bob choisit un premier avec $\phi(N)$: $e = 3$

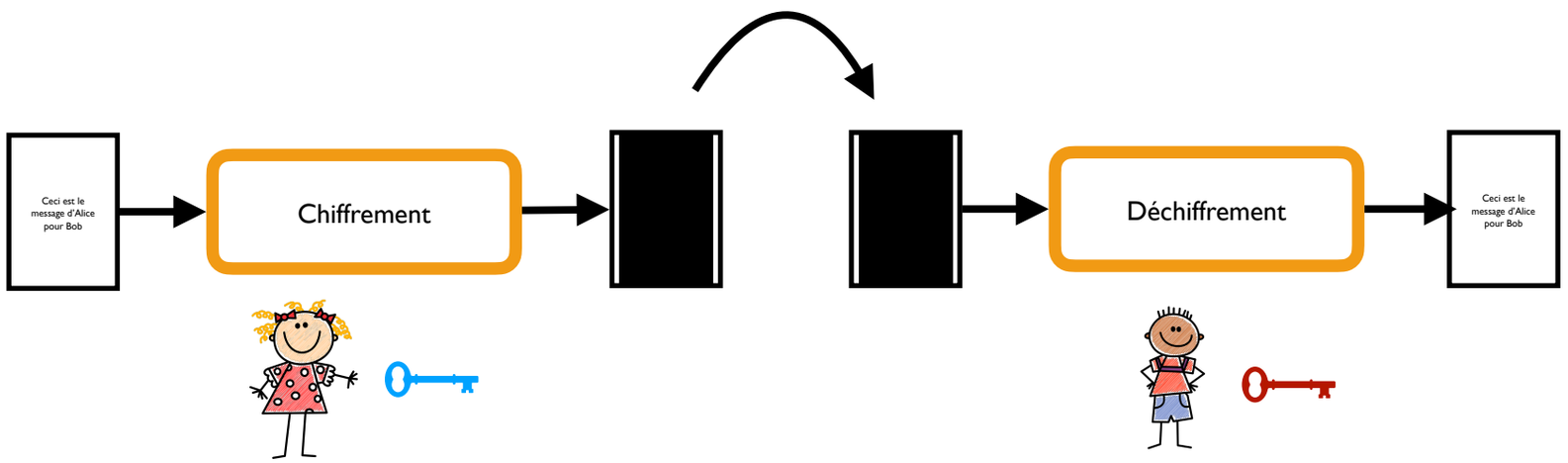
Bob calcule $d = e^{-1} \mod \phi(N) = 7$

(N, e) ←

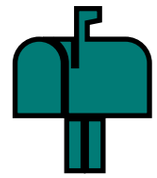
Alice veut envoyer son message
$m = 4$

Alice calcule

$$c = m^e \mod N$$
$$= 4^3 \mod 33 = 31$$



Chiffrement RSA



Bob choisit : $p = 3$ et $q = 11$

Bob calcule $N = p \times q = 33$ et
$\phi(N) = (p-1) \times (q-1) = 20$

Bob choisit un premier avec $\phi(N)$: $e = 3$

Bob calcule $d = e^{-1} \mod \phi(N) = 7$

(N, e) ←

Alice veut envoyer son message
$m = 4$

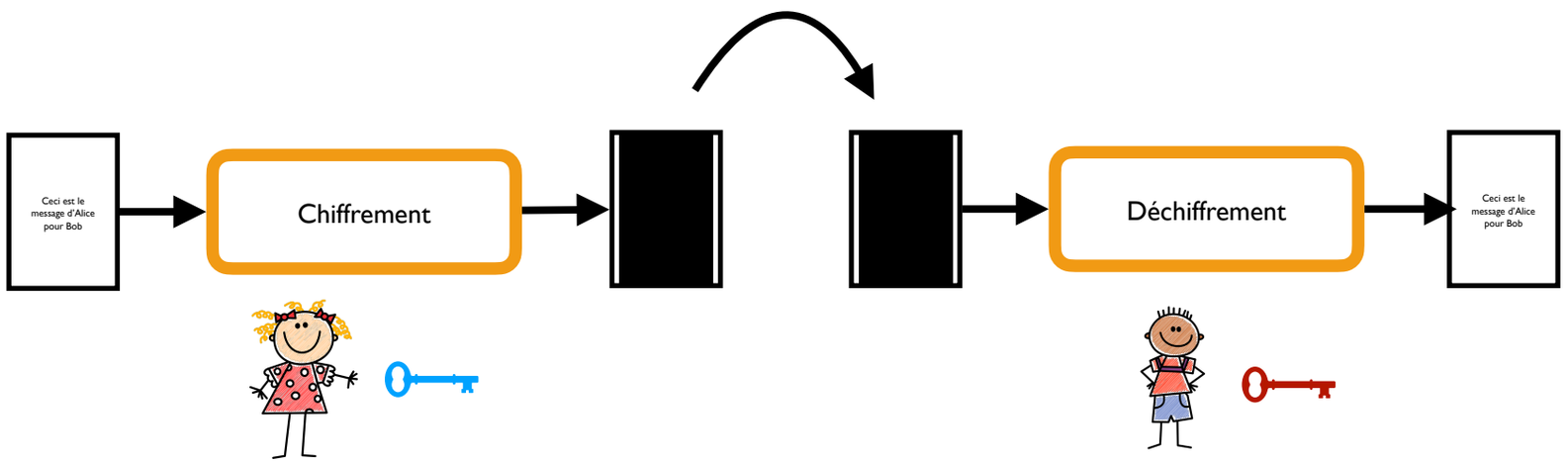
Alice calcule

$c = m^e \mod N$
$= 4^3 \mod 33 = 31$

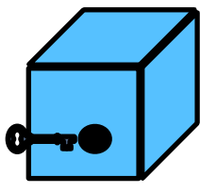
c →

Bob calcule

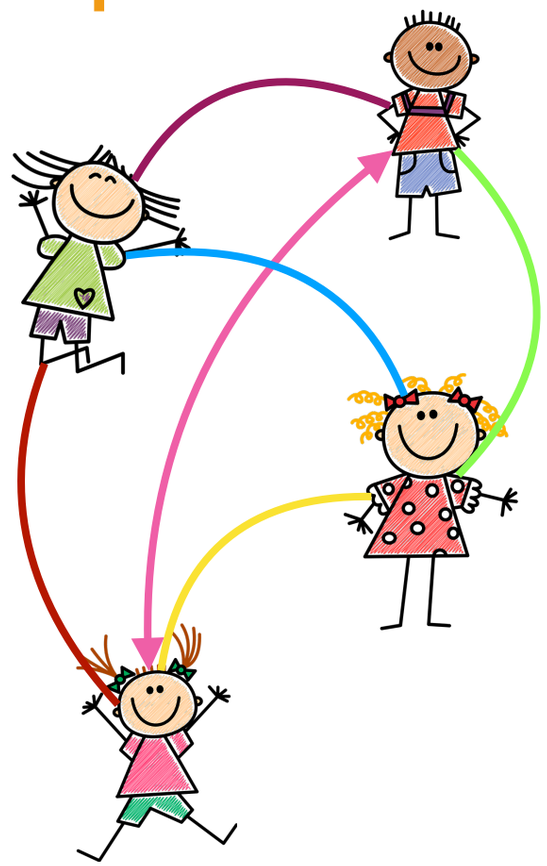
$m = c^d \mod N$
$= 31^7 \mod 33 = 4$

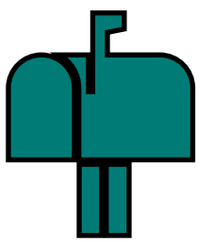


Cryptographie symétrique ou asymétrique ?



- Cryptographie symétrique
  - - Une clef par couple de personnes
  - - Requiert un échange de clef au préalable
  - + Rapide



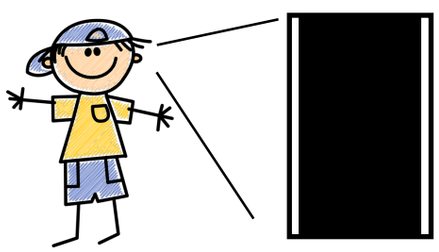


- Cryptographie asymétrique
  - - Plus lent
  - + Pas d'échange de clef préalable

- Solution : cryptographie asymétrique pour l'échange de clef, puis cryptographie symétrique

Cryptographie symétrique ou asymétrique ?

Confidentialité



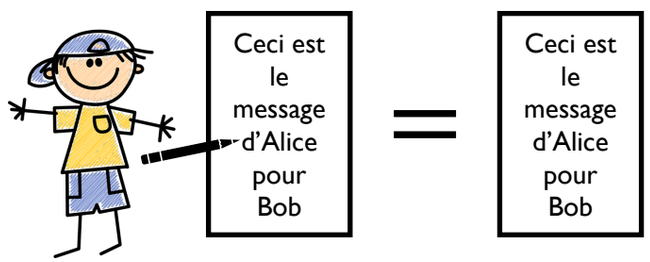
Chiffrement symétrique

Chiffrement asymétrique

Authentification

Certificats

Intégrité



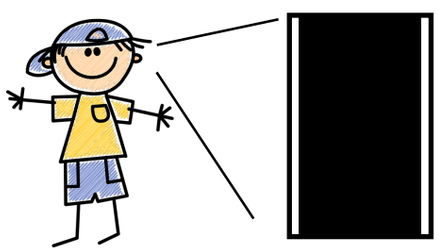
Fonction de hachage

MAC

Signatures

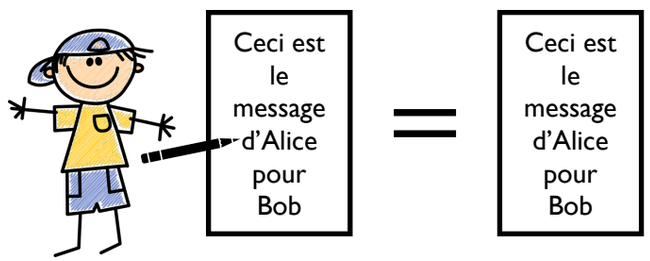
Cryptographie symétrique ou asymétrique ?

Confidentialité



Authentification

Intégrité



Chiffrement symétrique

Chiffrement asymétrique

Certificats

MAC

Signatures

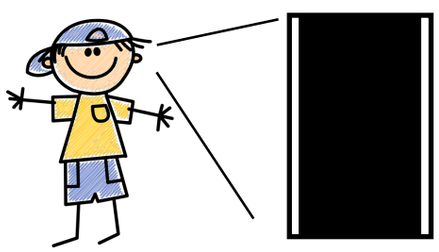
Fonction de hachage

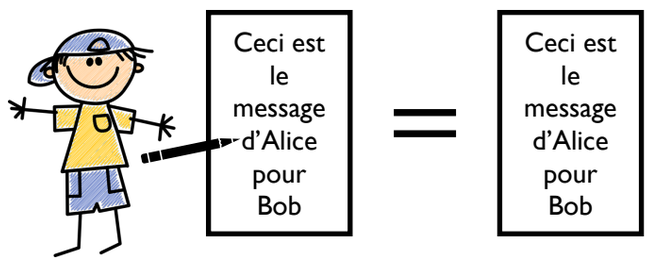
Cryptographie symétrique ou asymétrique ?

Confidentialité

Authentification

Intégrité





Chiffrement symétrique

Certificats

Fonction de hachage

Chiffrement asymétrique

MAC

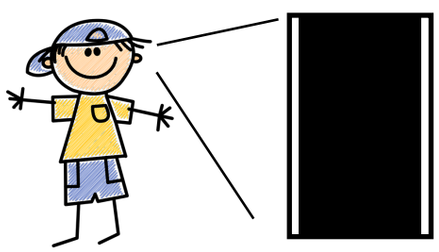
Signatures

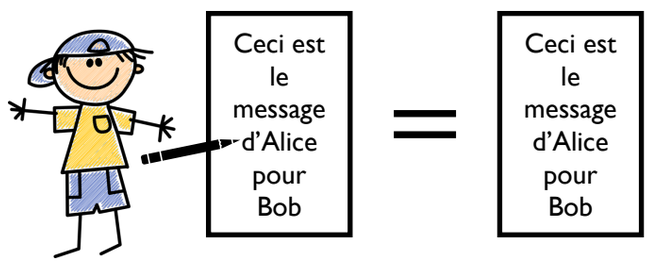
Cryptographie symétrique ou asymétrique ?

Confidentialité

Authentification

Intégrité





Chiffrement symétrique

Certificats

Fonction de hachage

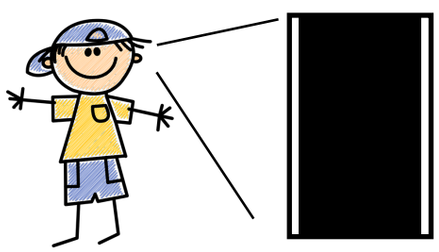
Chiffrement asymétrique

MAC

Signatures

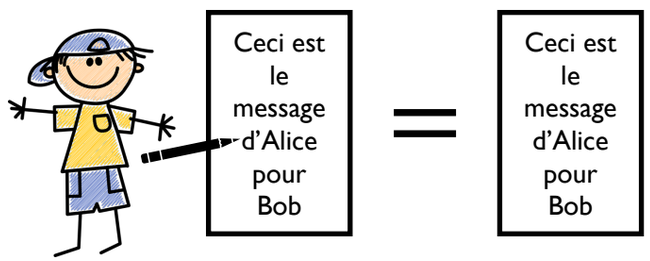
Cryptographie symétrique ou asymétrique ?

Confidentialité



Authentification

Intégrité



Chiffrement symétrique

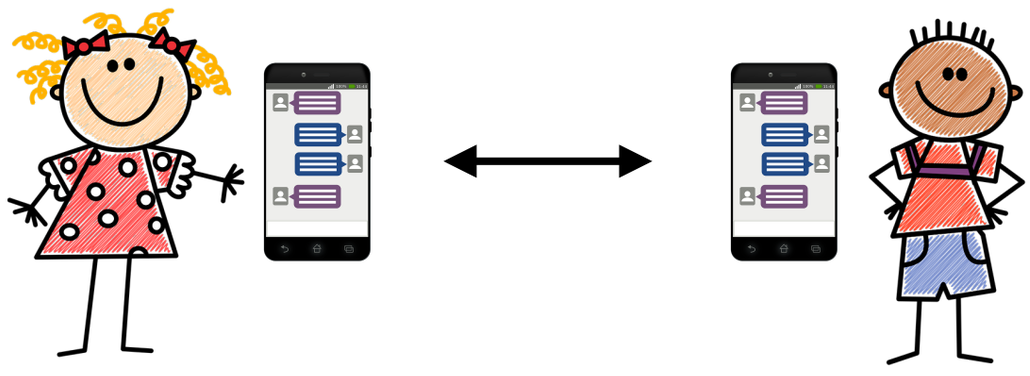
Chiffrement asymétrique

Certificats

MAC

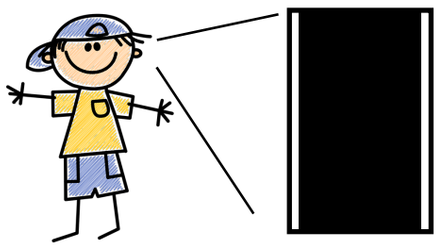
Signatures

Fonction de hachage



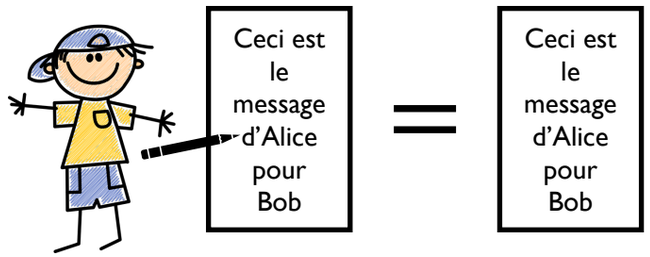
Cryptographie symétrique ou asymétrique ?

Confidentialité



Authentification

Intégrité



Chiffrement symétrique

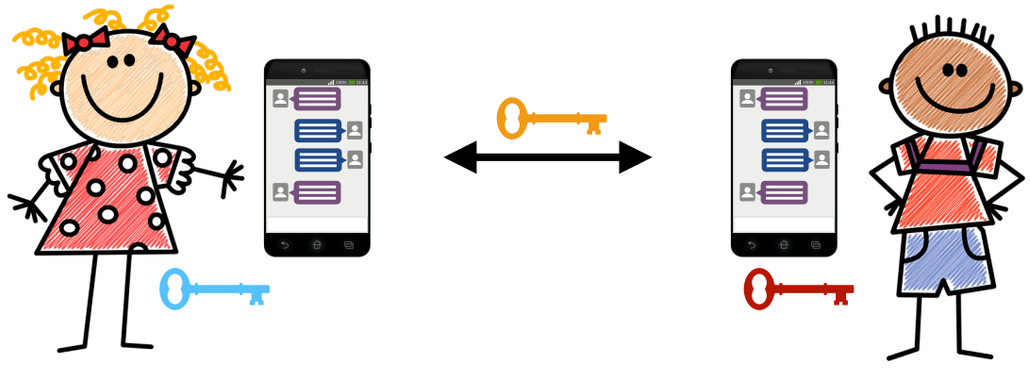
Chiffrement asymétrique

Certificats

Fonction de hachage

MAC

Signatures

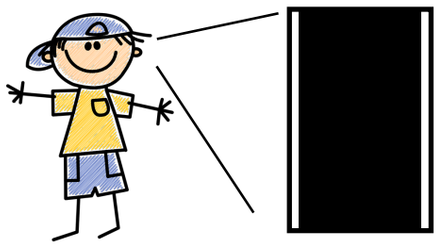


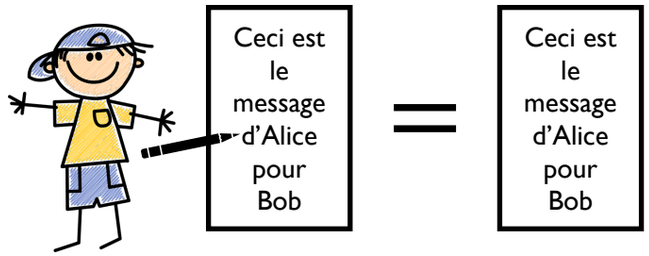
Cryptographie symétrique ou asymétrique ?

Confidentialité

Authentification

Intégrité





Chiffrement symétrique

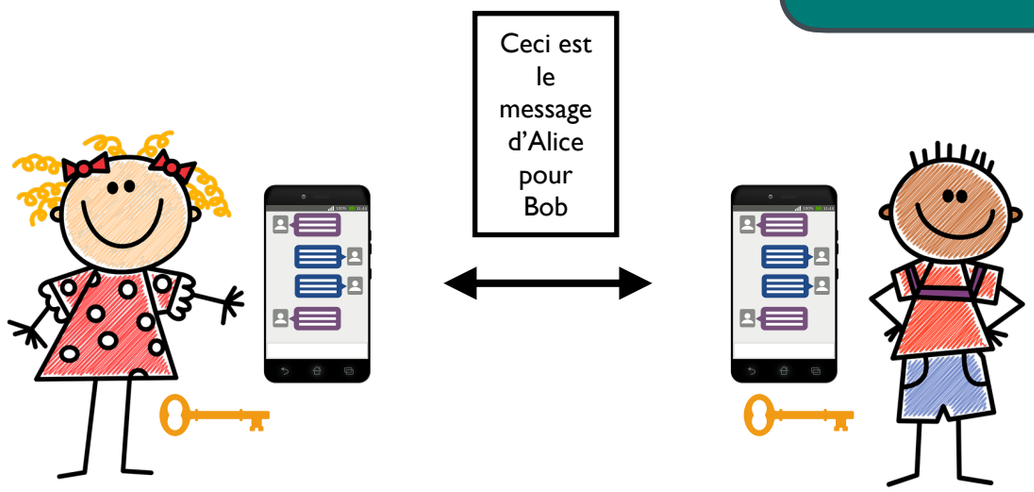
Certificats

Fonction de hachage

Chiffrement asymétrique

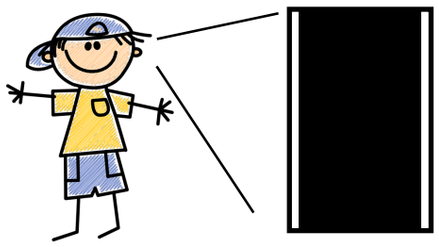
MAC

Signatures



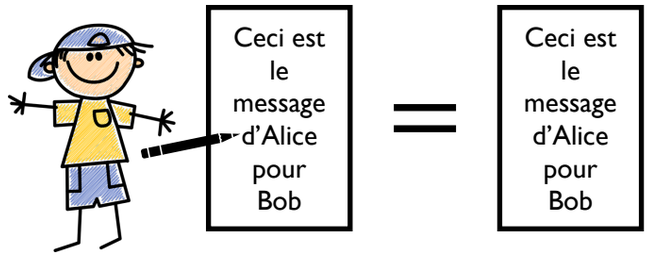
Cryptographie symétrique ou asymétrique ?

Confidentialité



Authentification

Intégrité



Chiffrement symétrique

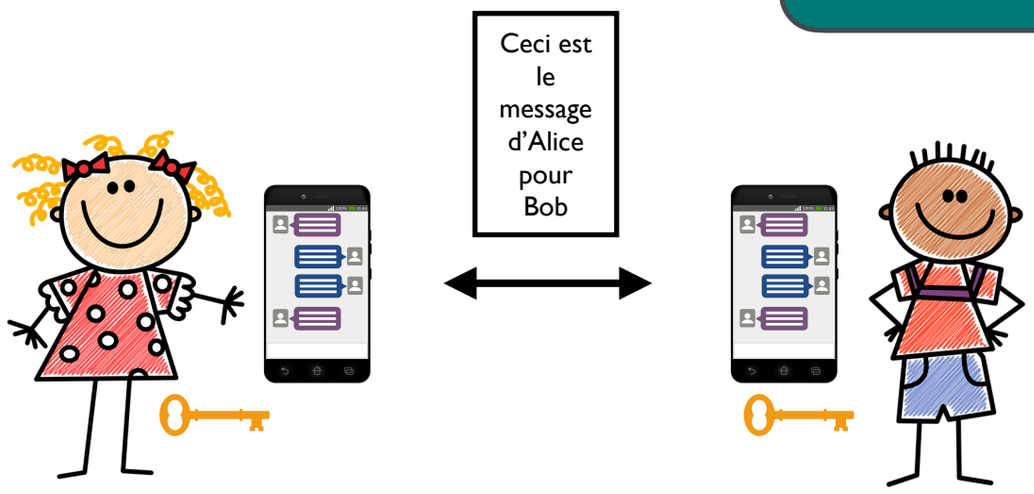
Chiffrement asymétrique

Certificats

MAC

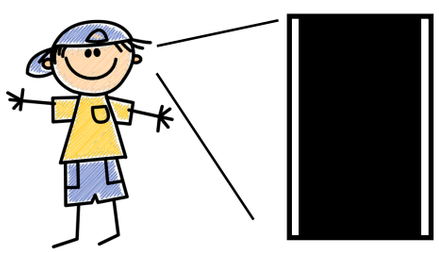
Signatures

Fonction de hachage



Cryptographie symétrique ou asymétrique ?

Confidentialité



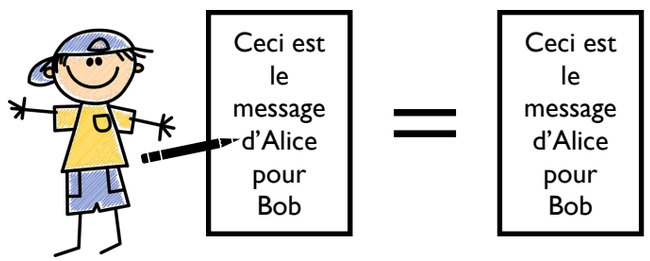
Chiffrement symétrique

Chiffrement asymétrique

Authentification

Certificats

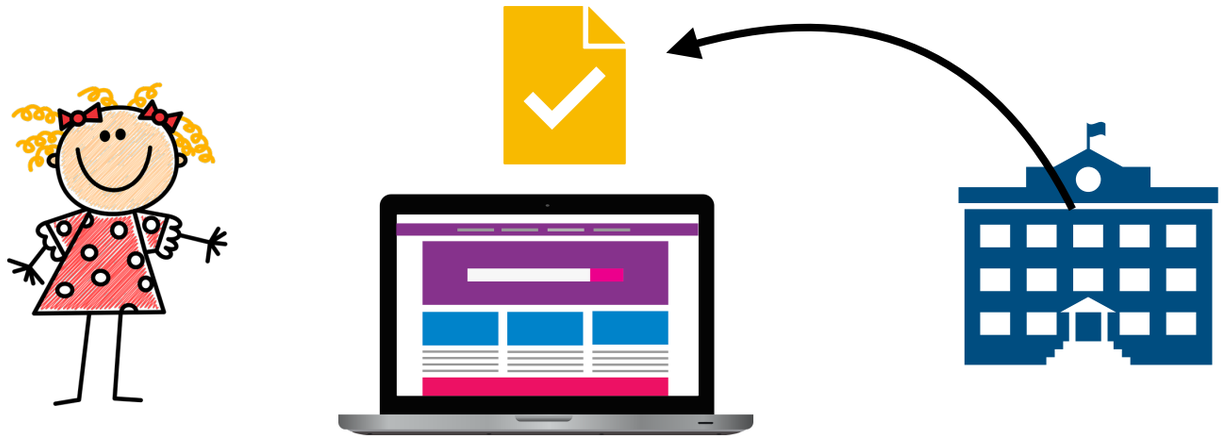
Intégrité



Fonction de hachage

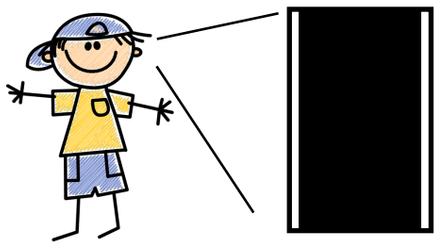
MAC

Signatures



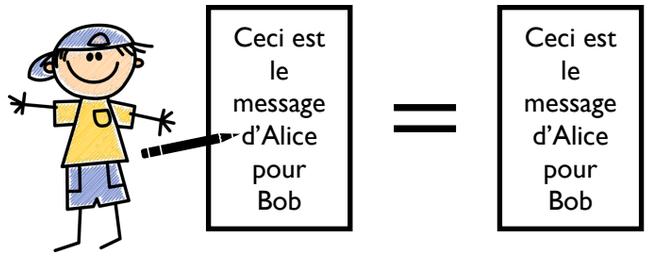
Cryptographie symétrique ou asymétrique ?

Confidentialité



Authentification

Intégrité



Chiffrement symétrique

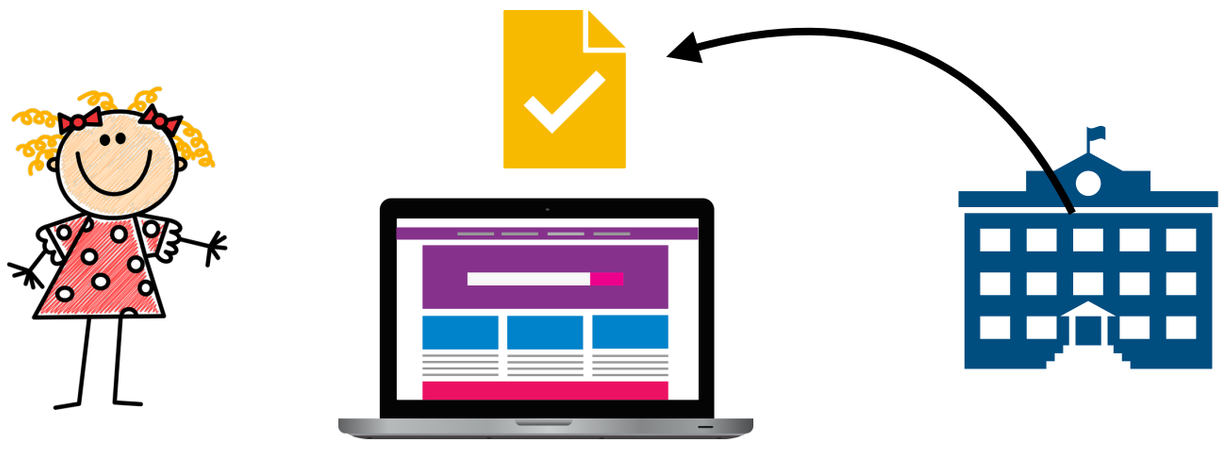
Chiffrement asymétrique

Certificats

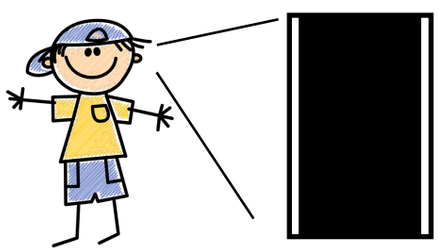
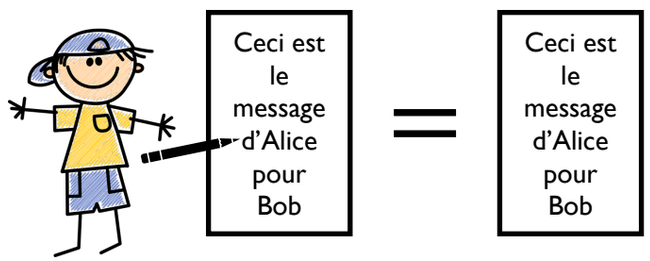
MAC

Fonction de hachage

Signatures

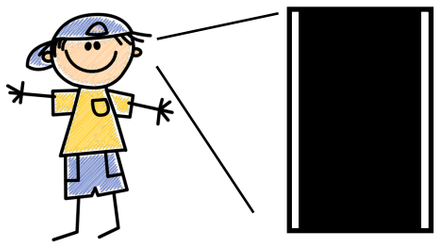


Cryptographie symétrique ou asymétrique ?

Confidentialité	Authentification	Intégrité
		
Chiffrement symétrique	Certificats	Fonction de hachage
Chiffrement asymétrique		MAC
		Signatures

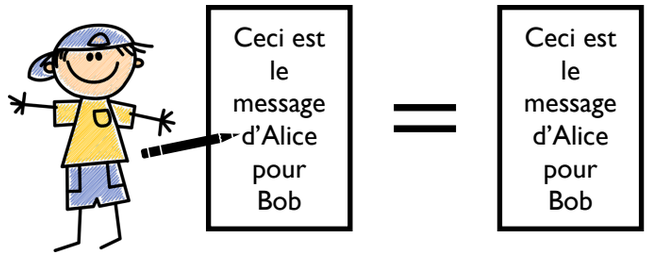
Cryptographie symétrique ou asymétrique ?

Confidentialité



Authentification

Intégrité



Chiffrement symétrique

Chiffrement asymétrique

Certificats

Fonction de hachage

MAC

Signatures

Quelques défis et enjeux actuels

Attaques et vulnérabilités

- Attaques black-box à partir d'entrées/sorties
- Attaques par canaux auxiliaires

Cryptographie post-quantique

- Menace de l'ordinateur quantique (e.g., RSA)
- Conception de nouveaux algorithmes post-quantiques, basés sur d'autres problèmes mathématiques

Enjeux de la règlementation

- RGPD
- Analyse des données personnelles pour détecter des abus

Questions

?

Quelques défis et enjeux actuels

Attaques et vulnérabilités

- Attaques black-box à partir d'entrées/sorties
- Attaques par canaux auxiliaires

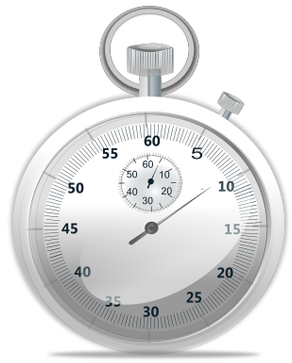
Cryptographie post-quantique

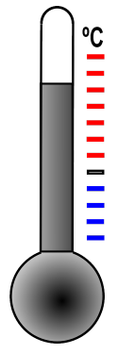
- Menace de l'ordinateur quantique (e.g., RSA)
- Conception de nouveaux algorithmes post-quantiques, basés sur d'autres problèmes mathématiques

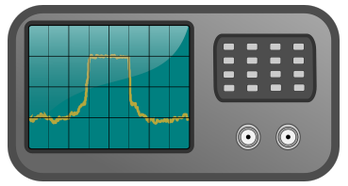
Enjeux de la règlementation

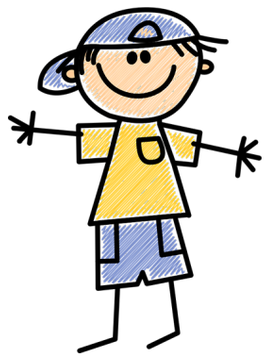
- RGPD
- Analyse des données personnelles pour détecter des abus

Attaques par canaux auxiliaires





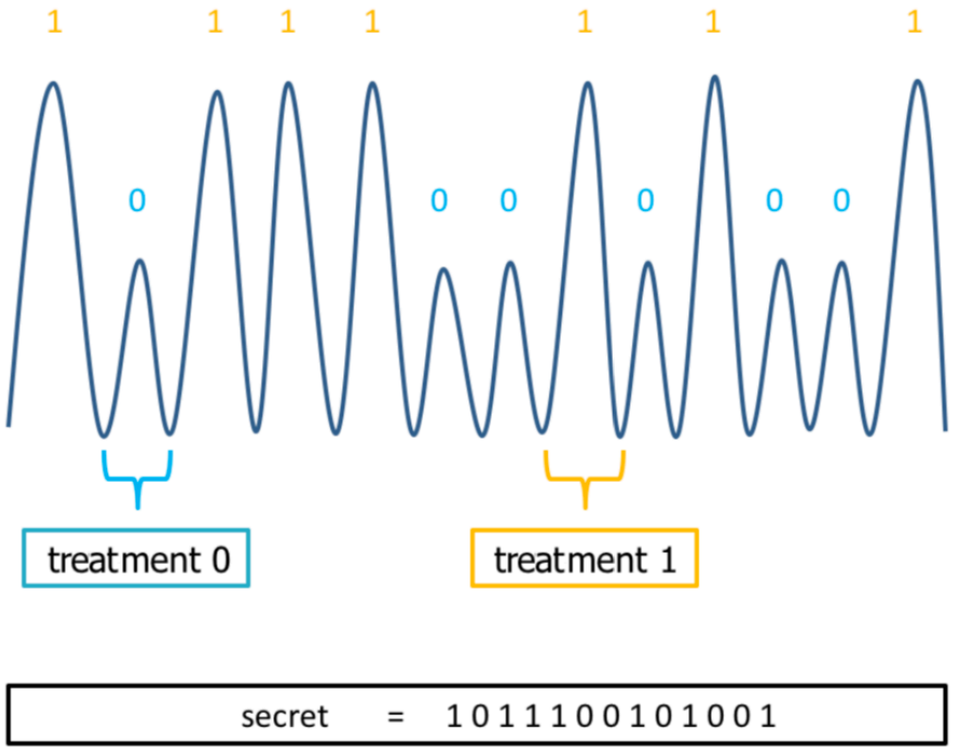




Attaques par canaux auxiliaires

Algorithm 1 Example

for $i = 1$ to n **do**
  if key$[i] = 0$ **then**
    do treatment 0
  else
    do treatment 1
  end if
end for



Questions

?