

Licence Pro - Sécurité - CM 1

Université de Caen

Jean Fromentin

<mailto:jfroment@info.unicaen.fr>

<http://www.info.unicaen.fr/~jfroment>

Cryptographie : définition

- **Définition :** La cryptographie traditionnelle traite de la transmission confidentielle de données. C'est l'étude de méthodes permettant de transmettre des messages sous forme déguisée, de telle sorte que seuls les destinataires autorisés soient capables de les lire.

Cryptographie : définition

- **Définition :** La cryptographie traditionnelle traite de la transmission confidentielle de données. C'est l'étude de méthodes permettant de transmettre des messages sous forme déguisée, de telle sorte que seuls les destinataires autorisés soient capables de les lire.
- **Définition :** Le message à envoyer est appelé message en clair.

Cryptographie : définition

- **Définition :** La cryptographie traditionnelle traite de la transmission confidentielle de données. C'est l'étude de méthodes permettant de transmettre des messages sous forme déguisée, de telle sorte que seuls les destinataires autorisés soient capables de les lire.
- **Définition :** Le message à envoyer est appelé message en clair.
On note \mathcal{M} l'ensemble des messages en clair.

Cryptographie : définition

- **Définition** : La cryptographie traditionnelle traite de la transmission confidentielle de données. C'est l'étude de méthodes permettant de transmettre des messages sous forme déguisée, de telle sorte que seuls les destinataires autorisés soient capables de les lire.

- **Définition** : Le message à envoyer est appelé message en clair.
On note \mathcal{M} l'ensemble des messages en clair.

- **Définition** : Le message déguisé est dit chiffré.

Cryptographie : définition

- **Définition :** La **cryptographie traditionnelle** traite de la transmission confidentielle de données. C'est l'étude de méthodes permettant de transmettre des messages sous forme déguisée, de telle sorte que seuls les destinataires autorisés soient capables de les lire.

- **Définition :** Le message à envoyer est appelé **message en clair**.
On note \mathcal{M} l'ensemble des messages en clair.

- **Définition :** Le message déguisé est dit **chiffré**.
On note \mathcal{C} l'ensemble des messages chiffrés.

Cryptographie : définition

- **Définition :** La **cryptographie traditionnelle** traite de la transmission confidentielle de données. C'est l'étude de méthodes permettant de transmettre des messages sous forme déguisée, de telle sorte que seuls les destinataires autorisés soient capables de les lire.

- **Définition :** Le message à envoyer est appelé **message en clair**.
On note \mathcal{M} l'ensemble des messages en clair.

- **Définition :** Le message déguisé est dit **chiffré**.
On note \mathcal{C} l'ensemble des messages chiffrés.

- **Définition :** Une **fonction de chiffrement** est donc une bijection
$$f : \mathcal{M} \rightarrow \mathcal{C}$$

Cryptographie : définition

- **Définition :** La **cryptographie traditionnelle** traite de la transmission confidentielle de données. C'est l'étude de méthodes permettant de transmettre des messages sous forme déguisée, de telle sorte que seuls les destinataires autorisés soient capables de les lire.

- **Définition :** Le message à envoyer est appelé **message en clair**.
On note \mathcal{M} l'ensemble des messages en clair.

- **Définition :** Le message déguisé est dit **chiffré**.
On note \mathcal{C} l'ensemble des messages chiffrés.

- **Définition :** Une **fonction de chiffrement** est donc une bijection
$$f : \mathcal{M} \rightarrow \mathcal{C}$$
L'application f^{-1} est la **fonction de déchiffrement**.

Fonction de chiffrement : exemple

- Exemple : Ecriture du message en clair à l'envers :

Fonction de chiffrement : exemple

- Exemple : Ecriture du message en clair à l'envers :

$f(\text{Au mon dieu ! Ils ont tues Kenny}) =$

Fonction de chiffrement : exemple

- **Exemple** : Ecriture du message en clair à l'envers :

$f(\text{Au mon dieu ! Ils ont tues Kenny}) = \text{ynneK seut tno sll ! ueid nom uA}$

Fonction de chiffrement : exemple

- **Exemple** : Ecriture du message en clair à l'envers :

$f(\text{Au mon dieu ! Ils ont tues Kenny}) = \text{ynneK seut tno sll ! ueid nom uA}$

- **Exemple** : Décalage de lettres ($f(a) = b, f(b) = c, \dots, f(z) = a$) :

Fonction de chiffrement : exemple

- **Exemple** : Ecriture du message en clair à l'envers :

$f(\text{Au mon dieu ! Ils ont tues Kenny}) = \text{ynneK seut tno sll ! ueid nom uA}$

- **Exemple** : Décalage de lettres ($f(a) = b, f(b) = c, \dots, f(z) = a$) :

$f(\text{Au mon dieu ! Ils ont tues Kenny}) = \text{Bv npo ejfv ! Jmt pou uvft Lfooz}$

Fonction de chiffrement : exemple

- **Exemple** : Ecriture du message en clair à l'envers :

$f(\text{Au mon dieu ! Ils ont tues Kenny}) = \text{ynneK seut tno sll ! ueid nom uA}$

- **Exemple** : Décalage de lettres ($f(a) = b, f(b) = c, \dots, f(z) = a$) :

$f(\text{Au mon dieu ! Ils ont tues Kenny}) = \text{Bv npo ejfv ! Jmt pou uvft Lfooz}$

- **Exemple** : Mélange des deux :

Fonction de chiffrement : exemple

- **Exemple** : Ecriture du message en clair à l'envers :

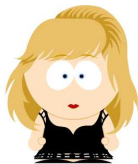
$f(\text{Au mon dieu ! Ils ont tues Kenny}) = \text{ynneK seut tno sll ! ueid nom uA}$

- **Exemple** : Décalage de lettres ($f(a) = b, f(b) = c, \dots, f(z) = a$) :

$f(\text{Au mon dieu ! Ils ont tues Kenny}) = \text{Bv npo ejfv ! Jmt pou uvft Lfooz}$

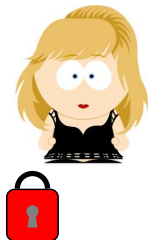
- **Exemple** : Mélange des deux :

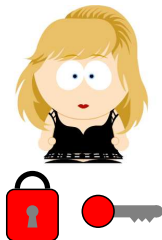
$f(\text{Au mon dieu ! Ils ont tues Kenny}) = \text{zoofL tfvu uop tmJ ! vfje opn vB}$



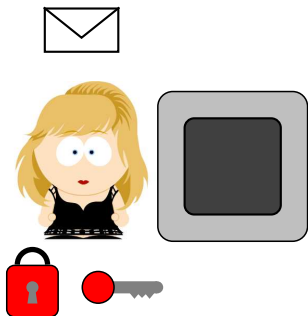


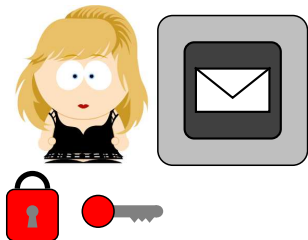


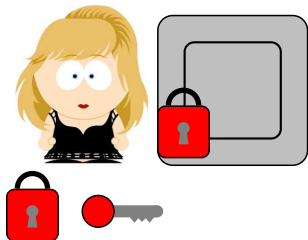


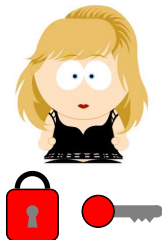


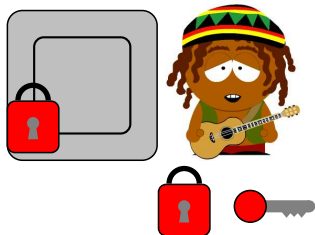
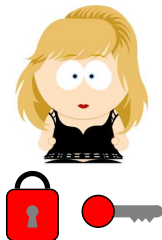


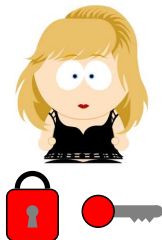


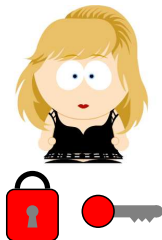












L'histoire a montré que chaque fois qu'une **fonction de chiffrement f** est destinée à être utilisée un nombre important de fois, il devient de plus en plus difficile de la maintenir complètement secrète.

L'histoire a montré que chaque fois qu'une **fonction de chiffrement** f est destinée à être utilisée un nombre important de fois, il devient de plus en plus difficile de la maintenir complètement secrète.

↪ Il faut changer régulièrement la **fonction de chiffrement**.

L'histoire a montré que chaque fois qu'une **fonction de chiffrement** f est destinée à être utilisée un nombre important de fois, il devient de plus en plus difficile de la maintenir complètement secrète.

↪ Il faut changer régulièrement la **fonction de chiffrement**.

- **Définition:** Un **système de chiffrement** est une famille finie $\mathcal{F} = (f_K)_{K \in \mathcal{K}}$ de fonctions de chiffrement. Chacune étant déterminée par une valeur de K , appelée clé.

L'histoire a montré que chaque fois qu'une **fonction de chiffrement** f est destinée à être utilisée un nombre important de fois, il devient de plus en plus difficile de la maintenir complètement secrète.

↪ Il faut changer régulièrement la **fonction de chiffrement**.

• **Définition:** Un **système de chiffrement** est une famille finie $\mathcal{F} = (f_K)_{K \in \mathcal{K}}$ de fonctions de chiffrement. Chacune étant déterminée par une valeur de K , appelée clé.

↪ K est la **K**ouleur de la clé et du cadena.

L'histoire a montré que chaque fois qu'une **fonction de chiffrement** f est destinée à être utilisée un nombre important de fois, il devient de plus en plus difficile de la maintenir complètement secrète.

↪ Il faut changer régulièrement la **fonction de chiffrement**.

• **Définition:** Un **système de chiffrement** est une famille finie $\mathcal{F} = (f_K)_{K \in \mathcal{K}}$ de fonctions de chiffrement. Chacune étant déterminée par une valeur de K , appelée clé.

↪ K est la **K**ouleur de la clé et du cadena.

↪ Oscar a un gros problème de vue : il ne voit pas les couleurs

↪ surtout celle des cadenas.

- Exemple :

$$f_k(\text{Au mon dieu ! Ils ont tues Kenny}) = \left\{ \right.$$

- Exemple :

$$f_k(\text{Au mon dieu ! Ils ont tues Kenny}) = \left\{ \begin{array}{l} \text{Bv npo ejfv ! Jmt pou uvft Lfooz} \\ k = 1 \end{array} \right.$$

- Exemple :

$$f_k(\text{Au mon dieu ! Ils ont tues Kenny}) = \begin{cases} \text{Bv npo ejfv ! Jmt pou uvft Lfooz} & k = 1 \\ \text{Cw oqp fkgw ! Knu qpv vwgu Mgppa} & k = 2 \end{cases}$$

- Exemple :

$$f_k(\text{Au mon dieu ! Ils ont tues Kenny}) = \begin{cases} \text{Bv npo ejfv ! Jmt pou uvft Lfooz} & k = 1 \\ \text{Cw oqp fkgw ! Knu qpv vwgu Mgppa} & k = 2 \\ \text{Dx prq glhx ! Lov rqw wxhv Nhqqb} & k = 3 \end{cases}$$

- Exemple :

$$f_k(\text{Au mon dieu ! Ils ont tues Kenny}) = \begin{cases} \text{Bv npo ejfv ! Jmt pou uvft Lfooz} & k = 1 \\ \text{Cw oqp fkgw ! Knu qpv vwgu Mgppa} & k = 2 \\ \text{Dx prq glhx ! Lov rqw wxhv Nhqqb} & k = 3 \\ \vdots \end{cases}$$

- Exemple :

$$f_k(\text{Au mon dieu ! Ils ont tues Kenny}) = \begin{cases} \text{Bv npo ejfv ! Jmt pou uvft Lfooz} & k = 1 \\ \text{Cw oqp fkgw ! Knu qpv vwgu Mgppa} & k = 2 \\ \text{Dx prq glhx ! Lov rqw wxhv Nhqqb} & k = 3 \\ \vdots \\ \text{Ys kml bgcs ! Gjq mlr rscq lcllw} & k = 24 \end{cases}$$

- Exemple :

$$f_k(\text{Au mon dieu ! Ils ont tues Kenny}) = \begin{cases} \text{Bv npo ejfv ! Jmt pou uvft Lfooz} & k = 1 \\ \text{Cw oqp fkgw ! Knu qpv vwgu Mgppa} & k = 2 \\ \text{Dx prq glhx ! Lov rqw wxhv Nhqqb} & k = 3 \\ \vdots & \\ \text{Ys kml bgcs ! Gjq mlr rscq lcllw} & k = 24 \\ \text{Zt Inm chdt ! Hkr nms stdr Jdmmx} & k = 25 \end{cases}$$

- Exemple :

$$f_k(\text{Au mon dieu ! Ils ont tues Kenny}) = \begin{cases} \text{Bv npo ejfv ! Jmt pou uvft Lfooz} & k = 1 \\ \text{Cw oqp fkgw ! Knu qpv vwgu Mgppa} & k = 2 \\ \text{Dx prq glhx ! Lov rqw wxhv Nhqqb} & k = 3 \\ \vdots & \\ \text{Ys kml bgcs ! Gjq mlr rscq lcllw} & k = 24 \\ \text{Zt Inm chdt ! Hkr nms stdr Jdmmx} & k = 25 \\ \text{Au mon dieu ! Ils ont tues Kenny} & k = 26 \end{cases}$$

Systeme de Vernam

- Soit Σ un alphabet de cardinalité m .

Systeme de Vernam

- Soit Σ un alphabet de cardinalité m .
- On code chaque lettre de Σ par sa position

Systeme de Vernam

- Soit Σ un alphabet de cardinalité m .
- On code chaque lettre de Σ par sa position
↪ c.-à-d. un élément de $\mathbb{Z}/m\mathbb{Z}$.

Système de Vernam

- Soit Σ un alphabet de cardinalité m .
- On code chaque lettre de Σ par sa position
 \rightsquigarrow c.-à-d. un élément de $\mathbb{Z}/m\mathbb{Z}$.
- Un message de n lettres est donc un élément de $(\mathbb{Z}/m\mathbb{Z})^n$.

Système de Vernam

- Soit Σ un alphabet de cardinalité m .
- On code chaque lettre de Σ par sa position
 \rightsquigarrow c.-à-d. un élément de $\mathbb{Z}/m\mathbb{Z}$.
- Un message de n lettres est donc un élément de $(\mathbb{Z}/m\mathbb{Z})^n$.
- Une clé K est un n -uple (k_1, \dots, k_n) tiré aléatoirement dans $(\mathbb{Z}/m\mathbb{Z})^n$

Système de Vernam

- Soit Σ un alphabet de cardinalité m .
- On code chaque lettre de Σ par sa position
 \rightsquigarrow c.-à-d. un élément de $\mathbb{Z}/m\mathbb{Z}$.
- Un message de n lettres est donc un élément de $(\mathbb{Z}/m\mathbb{Z})^n$.
- Une clé K est un n -uple (k_1, \dots, k_n) tiré aléatoirement dans $(\mathbb{Z}/m\mathbb{Z})^n$

- La fonction de chiffrement est :

$$f_K : \begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^n & \rightarrow & (\mathbb{Z}/m\mathbb{Z})^n \\ (\ell_1, \ell_2, \dots, \ell_n) & \mapsto & (\ell'_1, \ell'_2, \dots, \ell'_n) \end{array}$$

Système de Vernam

- Soit Σ un alphabet de cardinalité m .
- On code chaque lettre de Σ par sa position
 \rightsquigarrow c.-à-d. un élément de $\mathbb{Z}/m\mathbb{Z}$.
- Un message de n lettres est donc un élément de $(\mathbb{Z}/m\mathbb{Z})^n$.
- Une clé K est un n -uple (k_1, \dots, k_n) tiré aléatoirement dans $(\mathbb{Z}/m\mathbb{Z})^n$

- La fonction de chiffrement est :

$$\begin{aligned} f_K : \quad (\mathbb{Z}/m\mathbb{Z})^n &\rightarrow (\mathbb{Z}/m\mathbb{Z})^n \\ (\ell_1, \ell_2, \dots, \ell_n) &\mapsto (\ell'_1, \ell'_2, \dots, \ell'_n) \end{aligned}$$

où $\ell'_i = \ell_i + k_i \pmod{m}$.

Système de Vernam

- Soit Σ un alphabet de cardinalité m .
- On code chaque lettre de Σ par sa position
 \rightsquigarrow c.-à-d. un élément de $\mathbb{Z}/m\mathbb{Z}$.
- Un message de n lettres est donc un élément de $(\mathbb{Z}/m\mathbb{Z})^n$.
- Une clé K est un n -uple (k_1, \dots, k_n) tiré aléatoirement dans $(\mathbb{Z}/m\mathbb{Z})^n$

- La fonction de chiffrement est :

$$\begin{aligned} f_K : \quad (\mathbb{Z}/m\mathbb{Z})^n &\rightarrow (\mathbb{Z}/m\mathbb{Z})^n \\ (\ell_1, \ell_2, \dots, \ell_n) &\mapsto (\ell'_1, \ell'_2, \dots, \ell'_n) \end{aligned}$$

où $\ell'_i = \ell_i + k_i \pmod{m}$.

- C'est un système *parfait*.

Système de Vernam

- Soit Σ un alphabet de cardinalité m .
- On code chaque lettre de Σ par sa position
 \rightsquigarrow c.-à-d. un élément de $\mathbb{Z}/m\mathbb{Z}$.
- Un message de n lettres est donc un élément de $(\mathbb{Z}/m\mathbb{Z})^n$.
- Une clé K est un n -uple (k_1, \dots, k_n) tiré aléatoirement dans $(\mathbb{Z}/m\mathbb{Z})^n$

- La fonction de chiffrement est :

$$\begin{aligned} f_K : \quad (\mathbb{Z}/m\mathbb{Z})^n &\rightarrow (\mathbb{Z}/m\mathbb{Z})^n \\ (\ell_1, \ell_2, \dots, \ell_n) &\mapsto (\ell'_1, \ell'_2, \dots, \ell'_n) \end{aligned}$$

où $\ell'_i = \ell_i + k_i \pmod{m}$.

- C'est un système *parfait*.
- Une clé K ne doit jamais être réutilisée : très lourd.

Comment faire sans partager une clé ?



Comment faire sans partager une clé ?



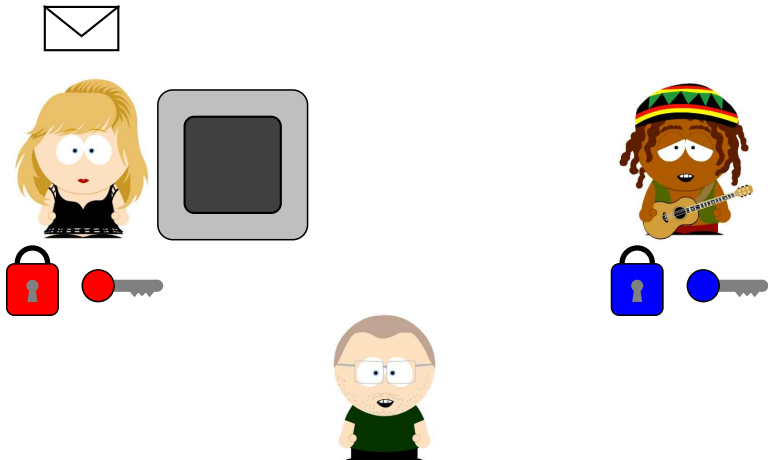
Comment faire sans partager une clé ?



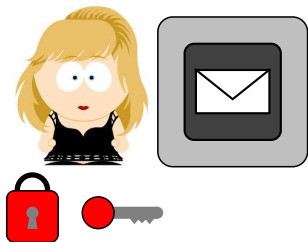
Comment faire sans partager une clé ?



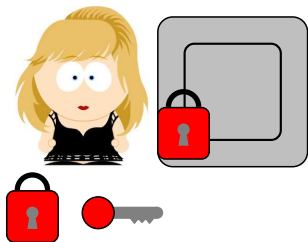
Comment faire sans partager une clé ?



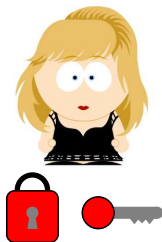
Comment faire sans partager une clé ?



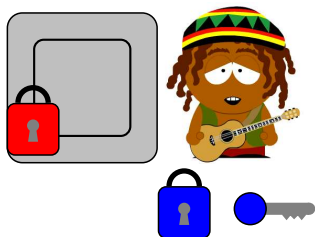
Comment faire sans partager une clé ?



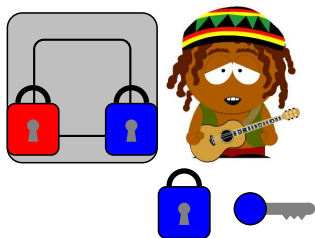
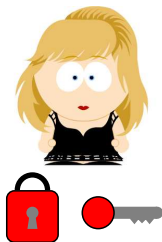
Comment faire sans partager une clé ?



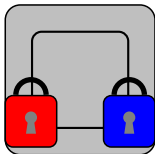
Comment faire sans partager une clé ?



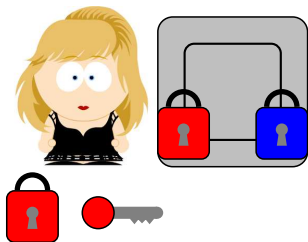
Comment faire sans partager une clé ?



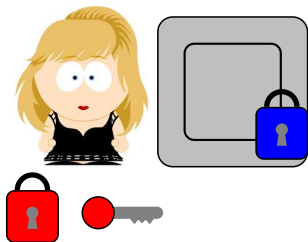
Comment faire sans partager une clé ?



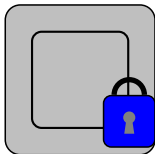
Comment faire sans partager une clé ?



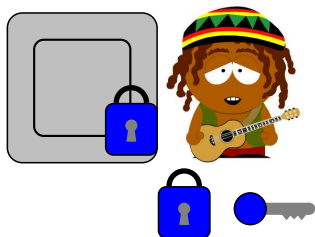
Comment faire sans partager une clé ?



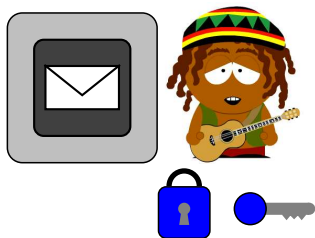
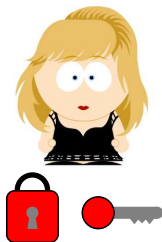
Comment faire sans partager une clé ?



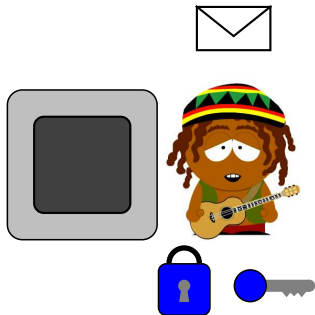
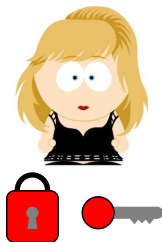
Comment faire sans partager une clé ?



Comment faire sans partager une clé ?



Comment faire sans partager une clé ?



Cryptographie à clé publique

- **Définition :** La **cryptographie à clé publique** est une méthode de chiffrement reposant sur l'utilisation d'une clé **publique** et d'une clé **privée**. L'une permettant de coder le message et l'autre de le décoder.

- **Principe:** N'importe qui peut chiffrer le message (grâce à la clé publique), mais une seule personne peut le déchiffrer (grâce à la clé secrète).

↑
ou l'inverse

- **Utilisation :**
 - Partage de clé secrète
 - Paiement sécurisé
 - Authentification
 - ...

Cryptographie à clé publique : 1^{er} schéma



Cryptographie à clé publique : 1^{er} schéma



Cryptographie à clé publique : 1^{er} schéma



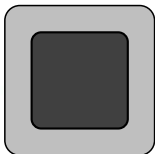
Cryptographie à clé publique : 1^{er} schéma



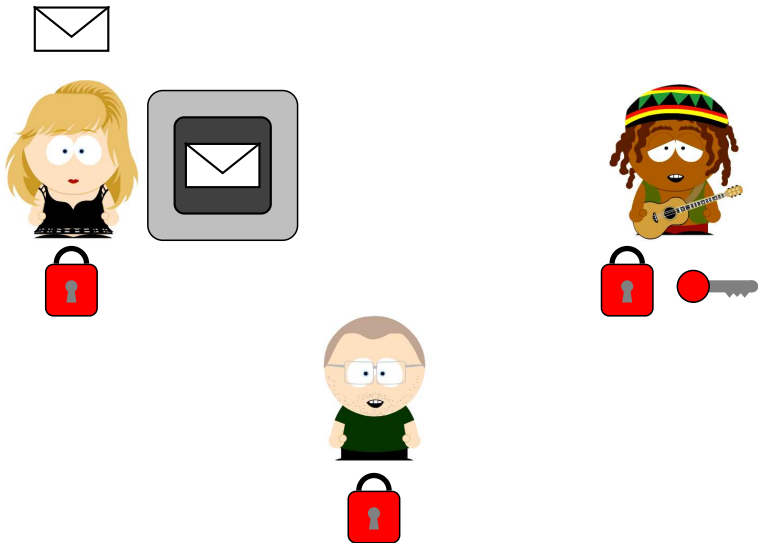
Cryptographie à clé publique : 1^{er} schéma



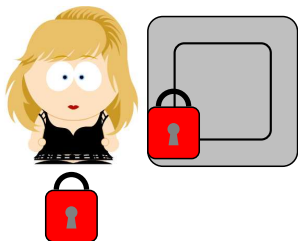
Cryptographie à clé publique : 1^{er} schéma



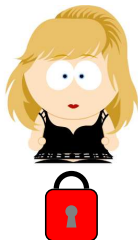
Cryptographie à clé publique : 1^{er} schéma



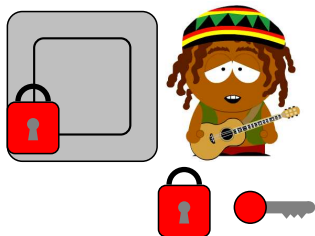
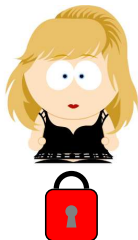
Cryptographie à clé publique : 1^{er} schéma



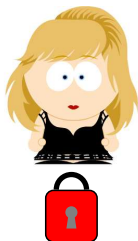
Cryptographie à clé publique : 1^{er} schéma



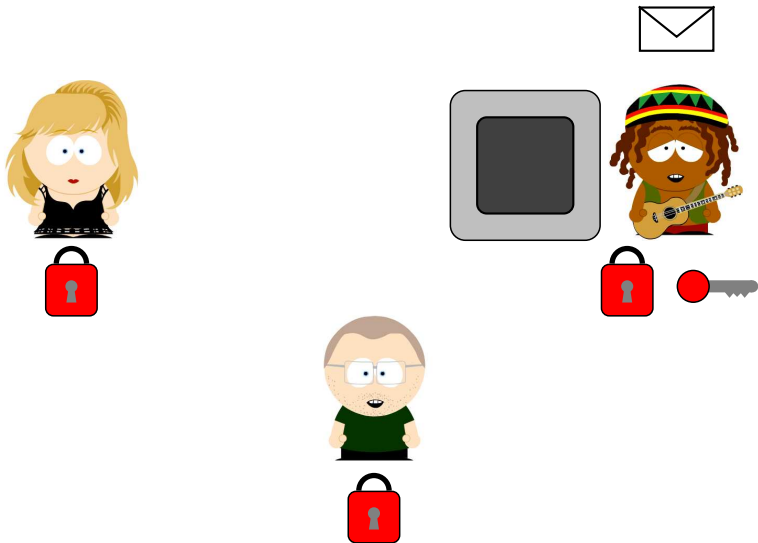
Cryptographie à clé publique : 1^{er} schéma



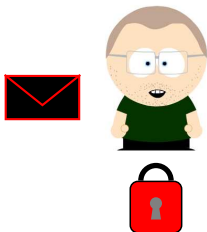
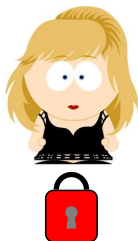
Cryptographie à clé publique : 1^{er} schéma



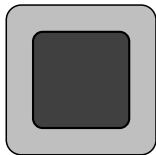
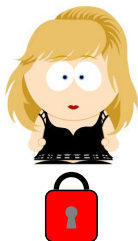
Cryptographie à clé publique : 1^{er} schéma



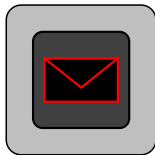
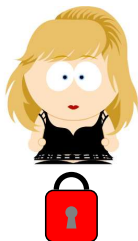
Cryptographie à clé publique : 1^{er} schéma



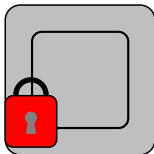
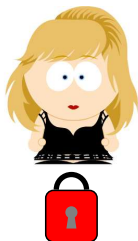
Cryptographie à clé publique : 1^{er} schéma



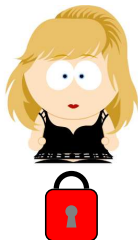
Cryptographie à clé publique : 1^{er} schéma



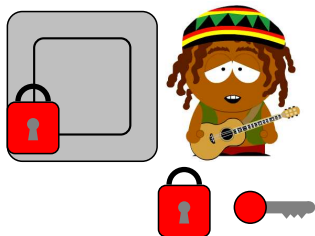
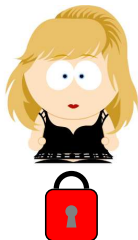
Cryptographie à clé publique : 1^{er} schéma



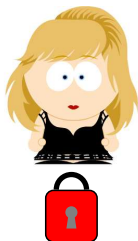
Cryptographie à clé publique : 1^{er} schéma



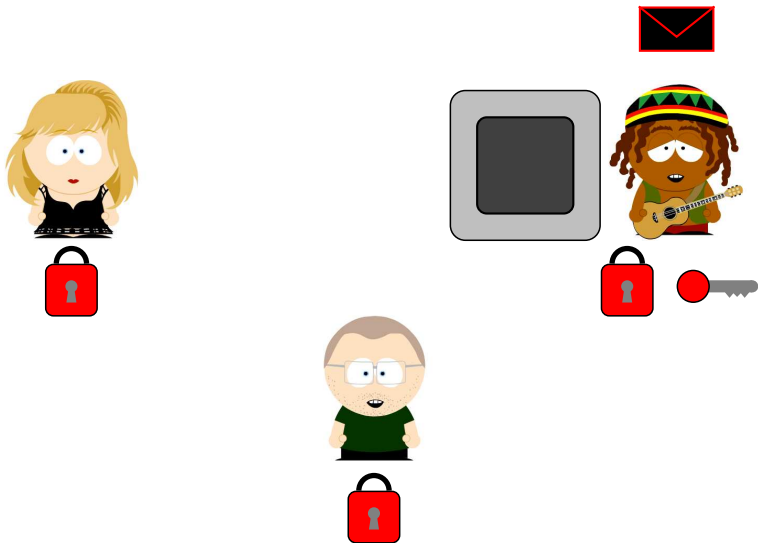
Cryptographie à clé publique : 1^{er} schéma



Cryptographie à clé publique : 1^{er} schéma



Cryptographie à clé publique : 1^{er} schéma



Cryptographie à clé publique : 2^e schéma



Cryptographie à clé publique : 2^e schéma



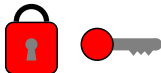
Cryptographie à clé publique : 2^e schéma



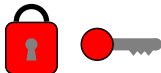
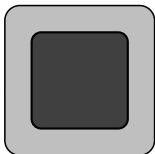
Cryptographie à clé publique : 2^e schéma



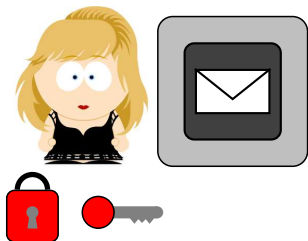
Cryptographie à clé publique : 2^e schéma



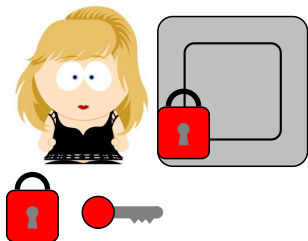
Cryptographie à clé publique : 2^e schéma



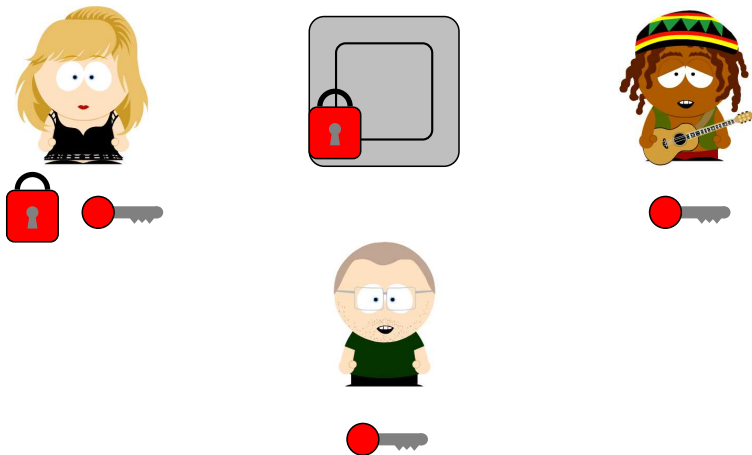
Cryptographie à clé publique : 2^e schéma



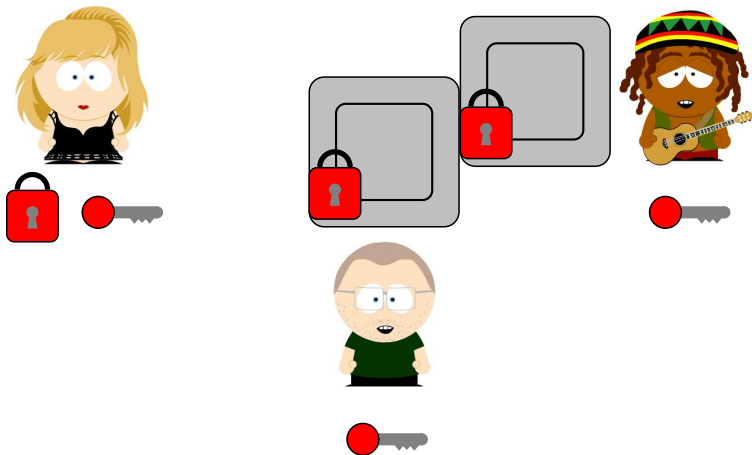
Cryptographie à clé publique : 2^e schéma



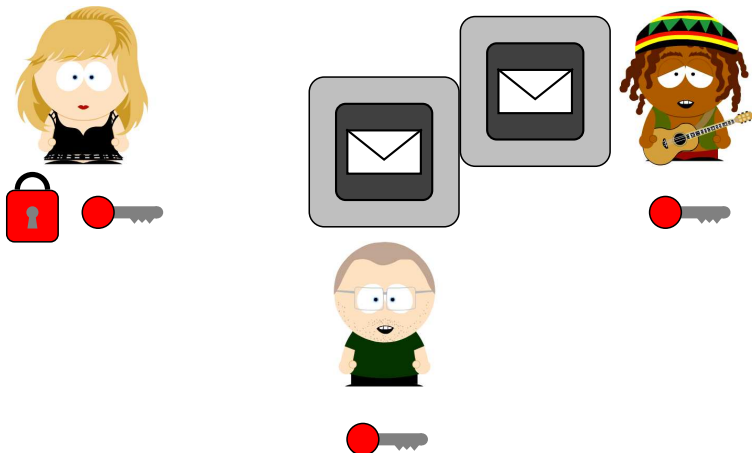
Cryptographie à clé publique : 2^e schéma



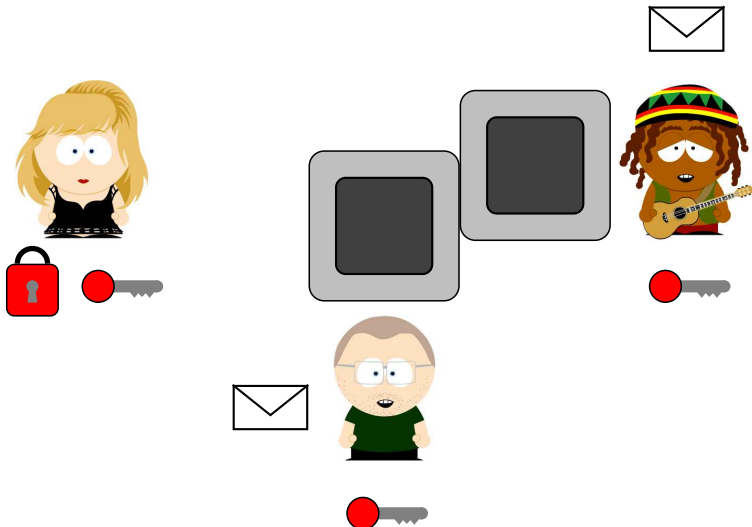
Cryptographie à clé publique : 2^e schéma



Cryptographie à clé publique : 2^e schéma



Cryptographie à clé publique : 2^e schéma



Fonction à sens unique

Fonction à sens unique

- **Définition** : Une **fonction à sens unique** est une fonction qui peut être facilement calculée, mais difficile à inverser.

Fonction à sens unique

- **Définition** : Une **fonction à sens unique** est une fonction qui peut être facilement calculée, mais difficile à inverser.

↪ facile voulant dire appartenant à la classe P

Fonction à sens unique

● **Définition** : Une **fonction à sens unique** est une fonction qui peut être facilement calculée, mais difficile à inverser.

↪ facile voulant dire appartenant à la classe P

↪ difficile voulant dire n'appartenant pas à la classe P

Fonction à sens unique

- **Définition** : Une **fonction à sens unique** est une fonction qui peut être facilement calculée, mais difficile à inverser.

↪ facile voulant dire appartenant à la classe P

↪ difficile voulant dire n'appartenant pas à la classe P

- **Fait** : L'existence d'une fonction à sens unique est équivalente au problème $P \neq NP$, dont la résolution sera récompensé par l'institut Clay avec 1 000 000 de \$.

Fonction à sens unique

● **Définition** : Une **fonction à sens unique** est une fonction qui peut être facilement calculée, mais difficile à inverser.

↪ facile voulant dire appartenant à la classe P

↪ difficile voulant dire n'appartenant pas à la classe P

● **Fait** : L'existence d'une fonction à sens unique est équivalente au problème $P \neq NP$, dont la résolution sera récompensé par l'institut Clay avec 1 000 000 de \$.

↪ on ne sait pas si de telles fonctions existent

Fonction à sens unique

● **Définition** : Une **fonction à sens unique** est une fonction qui peut être facilement calculée, mais difficile à inverser.

↪ facile voulant dire appartenant à la classe P

↪ difficile voulant dire n'appartenant pas à la classe P

● **Fait** : L'existence d'une fonction à sens unique est équivalente au problème $P \neq NP$, dont la résolution sera récompensé par l'institut Clay avec 1 000 000 de \$.

↪ on ne sait pas si de telles fonctions existent

↪ on donne alors une autre notion de *difficile*

Fonction à sens unique : exemple

- Exemple : [Le cryptosystème RSA]

Fonction à sens unique : exemple

- Exemple : [Le cryptosystème RSA]
 - on choisit deux nombres premiers distincts p et q gardés secrets

Fonction à sens unique : exemple

- Exemple : [Le cryptosystème RSA]
 - on choisit deux nombres premiers distincts p et q gardés secrets
 - on calcule la clé publique $n = p \times q$ et on choisit $e = 3$ (ou $e = 65537$)

Fonction à sens unique : exemple

- Exemple : [Le cryptosystème RSA]
 - on choisit deux nombres premiers distincts p et q gardés secrets
 - on calcule la clé publique $n = p \times q$ et on choisit $e = 3$ (ou $e = 65537$)
 - on code un message M de $\mathbb{Z}/n\mathbb{Z}$ par $M^e \pmod n$

Fonction à sens unique : exemple

- Exemple : [Le cryptosystème RSA]
 - on choisit deux nombres premiers distincts p et q gardés secrets
 - on calcule la clé publique $n = p \times q$ et on choisit $e = 3$ (ou $e = 65537$)
 - on code un message M de $\mathbb{Z}/n\mathbb{Z}$ par $M^e \pmod n$
- Question : Où est la fonction à sens unique ?

Fonction à sens unique : exemple

- **Exemple** : [Le cryptosystème RSA]
 - on choisit deux nombres premiers distincts p et q gardés secrets
 - on calcule la clé publique $n = p \times q$ et on choisit $e = 3$ (ou $e = 65537$)
 - on code un message M de $\mathbb{Z}/n\mathbb{Z}$ par $M^e \pmod n$
- **Question** : Où est la fonction à sens unique ?
- **Réponse** : C'est la fonction exponentiation modulaire :

Fonction à sens unique : exemple

- **Exemple** : [Le cryptosystème RSA]
 - on choisit deux nombres premiers distincts p et q gardés secrets
 - on calcule la clé publique $n = p \times q$ et on choisit $e = 3$ (ou $e = 65537$)
 - on code un message M de $\mathbb{Z}/n\mathbb{Z}$ par $M^e \pmod n$

- **Question** : Où est la fonction à sens unique ?

- **Réponse** : C'est la fonction exponentiation modulaire :

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto M^e \end{aligned}$$

Fonction à sens unique : exemple

- **Exemple** : [Le cryptosystème RSA]
 - on choisit deux nombres premiers distincts p et q gardés secrets
 - on calcule la clé publique $n = p \times q$ et on choisit $e = 3$ (ou $e = 65537$)
 - on code un message M de $\mathbb{Z}/n\mathbb{Z}$ par $M^e \bmod n$

- **Question** : Où est la fonction à sens unique ?

- **Réponse** : C'est la fonction exponentiation modulaire :

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto M^e \end{aligned}$$

On *suppose* que inverser f revient à trouver la décomposition $n = p \times q$.

Fonction à sens unique : exemple

- **Exemple** : [Le cryptosystème RSA]
 - on choisit deux nombres premiers distincts p et q gardés secrets
 - on calcule la clé publique $n = p \times q$ et on choisit $e = 3$ (ou $e = 65537$)
 - on code un message M de $\mathbb{Z}/n\mathbb{Z}$ par $M^e \pmod n$

- **Question** : Où est la fonction à sens unique ?

- **Réponse** : C'est la fonction exponentiation modulaire :

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto M^e \end{aligned}$$

On *suppose* que inverser f revient à trouver la décomposition $n = p \times q$.

↪ et une fois qu'on a trouvé p et q ?

Fonction à sens unique à brèche secrète

Fonction à sens unique à brèche secrète

- **Définition :** Une fonction à sens unique à brèche secrète est une fonction à sens unique f particulière. En effet la connaissance d'un secret rend l'inversion de f facile.

Fonction à sens unique à brèche secrète

- **Définition :** Une fonction à sens unique à brèche secrète est une fonction à sens unique f particulière. En effet la connaissance d'un **secret** rend l'inversion de f facile.

↪ de telles fonctions sont difficile à trouver

- **Exemple :**

Fonction à sens unique à brèche secrète

- **Définition :** Une fonction à sens unique à brèche secrète est une fonction à sens unique f particulière. En effet la connaissance d'un secret rend l'inversion de f facile.

↪ de telles fonctions sont difficile à trouver

- **Exemple :**
 - exponentiation modulaire

Fonction à sens unique à brèche secrète

- **Définition :** Une fonction à sens unique à brèche secrète est une fonction à sens unique f particulière. En effet la connaissance d'un **secret** rend l'inversion de f facile.

↪ de telles fonctions sont difficile à trouver

- **Exemple :**
 - exponentiation modulaire
 - ...

Fonction à sens unique à brèche secrète : retour à RSA

- **Définition** : La fonction indicatrice d'Euler ϕ est définié par

Fonction à sens unique à brèche secrète : retour à RSA

- **Définition :** La fonction indicatrice d'Euler ϕ est définié par
 - $\phi(p) = p - 1$ si p est premier

Fonction à sens unique à brèche secrète : retour à RSA

- **Définition :** La fonction indicatrice d'Euler ϕ est définié par
 - $\phi(p) = p - 1$ si p est premier
 - $\phi(p^k) = p^k - p^{k-1}$ si p est premier

Fonction à sens unique à brèche secrète : retour à RSA

- **Définition :** La fonction indicatrice d'Euler ϕ est définié par
 - $\phi(p) = p - 1$ si p est premier
 - $\phi(p^k) = p^k - p^{k-1}$ si p est premier
 - $\phi(u \times v) = \phi(u) \times \phi(v)$ si u et v sont premiers entre eux

- **Exemple :**

Fonction à sens unique à brèche secrète : retour à RSA

- **Définition :** La fonction indicatrice d'Euler ϕ est définié par
 - $\phi(p) = p - 1$ si p est premier
 - $\phi(p^k) = p^k - p^{k-1}$ si p est premier
 - $\phi(u \times v) = \phi(u) \times \phi(v)$ si u et v sont premiers entre eux

- **Exemple :** Pour p et q deux nombres premiers distincts :

$$\phi(p \times q) = (p - 1) \times (q - 1)$$

Fonction à sens unique à brèche secrète : retour à RSA

- **Définition :** La fonction indicatrice d'Euler ϕ est défini par
 - $\phi(p) = p - 1$ si p est premier
 - $\phi(p^k) = p^k - p^{k-1}$ si p est premier
 - $\phi(u \times v) = \phi(u) \times \phi(v)$ si u et v sont premiers entre eux

- **Exemple :** Pour p et q deux nombres premiers distincts :

$$\phi(p \times q) = (p - 1) \times (q - 1)$$

- **Théorème :** Si M est premier à n alors $M^{\phi(n)} \equiv 1 \pmod{n}$.

Fonction à sens unique à brèche secrète : retour à RSA

Fonction à sens unique à brèche secrète : retour à RSA

- On a $n = p \times q$ et $e = 3$ ou $e = 65537$

Fonction à sens unique à brèche secrète : retour à RSA

- On a $n = p \times q$ et $e = 3$ ou $e = 65537$

$$\begin{aligned} f: \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto C = M^e \end{aligned}$$

Fonction à sens unique à brèche secrète : retour à RSA

- On a $n = p \times q$ et $e = 3$ ou $e = 65537$

$$\begin{aligned} f: \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto C = M^e \end{aligned}$$

- Question : Comment inverser f ?

Fonction à sens unique à brèche secrète : retour à RSA

- On a $n = p \times q$ et $e = 3$ ou $e = 65537$

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto C = M^e \end{aligned}$$

- Question : Comment inverser f ?

- Réponse :
 - On calcule $\phi(n) = (p - 1) \times (q - 1)$

Fonction à sens unique à brèche secrète : retour à RSA

- On a $n = p \times q$ et $e = 3$ ou $e = 65537$

$$\begin{aligned} f: \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto C = M^e \end{aligned}$$

- Question : Comment inverser f ?

- Réponse :

- On calcule $\phi(n) = (p - 1) \times (q - 1)$
- Par *Bezout*, on calcule d tel que $ed \equiv 1 \pmod{\phi(n)}$

Fonction à sens unique à brèche secrète : retour à RSA

- On a $n = p \times q$ et $e = 3$ ou $e = 65537$

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto C = M^e \end{aligned}$$

- Question : Comment inverser f ?

- Réponse :

- On calcule $\phi(n) = (p - 1) \times (q - 1)$
- Par *Bezout*, on calcule d tel que $ed \equiv 1 \pmod{\phi(n)}$
- On a

$$C^d =$$

Fonction à sens unique à brèche secrète : retour à RSA

- On a $n = p \times q$ et $e = 3$ ou $e = 65537$

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto C = M^e \end{aligned}$$

- Question : Comment inverser f ?

- Réponse :

- On calcule $\phi(n) = (p - 1) \times (q - 1)$
- Par *Bezout*, on calcule d tel que $ed \equiv 1 \pmod{\phi(n)}$
- On a

$$C^d = (M^e)^d$$

Fonction à sens unique à brèche secrète : retour à RSA

- On a $n = p \times q$ et $e = 3$ ou $e = 65537$

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto C = M^e \end{aligned}$$

- Question : Comment inverser f ?

- Réponse :

- On calcule $\phi(n) = (p - 1) \times (q - 1)$
- Par *Bezout*, on calcule d tel que $ed \equiv 1 \pmod{\phi(n)}$
- On a

$$C^d = (M^e)^d = M^{ed+k\phi(n)}$$

Fonction à sens unique à brèche secrète : retour à RSA

- On a $n = p \times q$ et $e = 3$ ou $e = 65537$

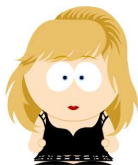
$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto C = M^e \end{aligned}$$

- Question : Comment inverser f ?

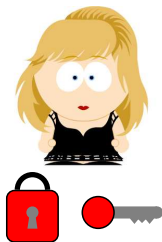
- Réponse :

- On calcule $\phi(n) = (p - 1) \times (q - 1)$
- Par *Bezout*, on calcule d tel que $ed \equiv 1 \pmod{\phi(n)}$
- On a

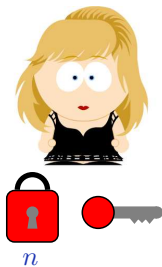
$$C^d = (M^e)^d = M^{ed+k\phi(n)} = M \pmod{n}$$



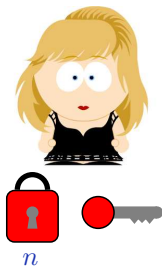


(p, q) 

$$(p, q); n = p \times q$$



$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1)$$



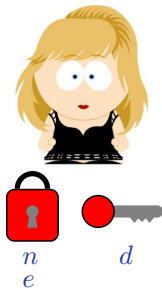
$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1); e$$



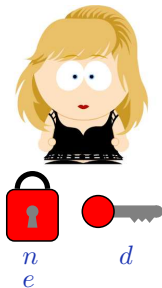
n
 e



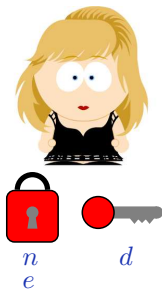
$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1); e; ed \equiv 1 \pmod{n}$$



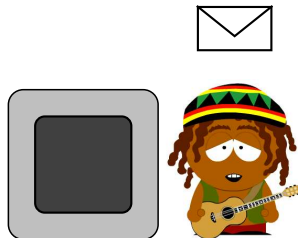
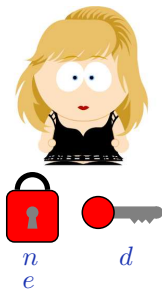
$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1); e; ed \equiv 1 \pmod{n}$$



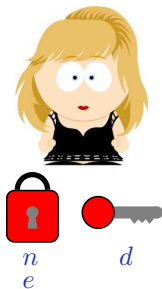
$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1); e; ed \equiv 1 \pmod{n}$$



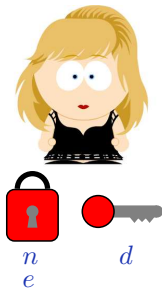
$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1); e; ed \equiv 1 \pmod n$$



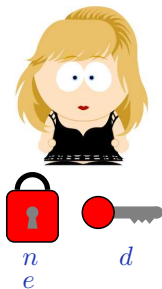
$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1); e; ed \equiv 1 \pmod n$$



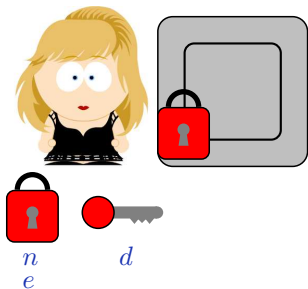
$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1); e; ed \equiv 1 \pmod{n}$$



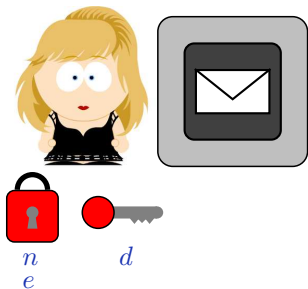
$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1); e; ed \equiv 1 \pmod n$$



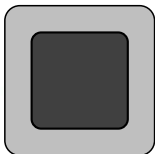
$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1); e; ed \equiv 1 \pmod n$$



$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1); e; ed \equiv 1 \pmod n$$



$$(p, q); n = p \times q; \phi(n) = (p - 1) \times (q - 1); e; ed \equiv 1 \pmod n$$

 n
 e  d 

Une fonction à sens unique est difficile à inverser mais, pour une image donnée, elle peut avoir plusieurs antécédants.

Une fonction à sens unique est difficile à inverser mais, pour une image donnée, elle peut avoir plusieurs antécédants.

↪ L'image d'une fonction à sens unique ou de **hachage** est souvent appelée **condensat**.

Une fonction à sens unique est difficile à inverser mais, pour une image donnée, elle peut avoir plusieurs antécédants.

↪ L'image d'une fonction à sens unique ou de **hachage** est souvent appelée **condensat**.

- **Fait** : Le condensat *caractérise* la donnée mais ne peut la reconstruire.

Une fonction à sens unique est difficile à inverser mais, pour une image donnée, elle peut avoir plusieurs antécédants.

↪ L'image d'une fonction à sens unique ou de **hachage** est souvent appelée **condensat**.

- **Fait** : Le condensat *caractérise* la donnée mais ne peut la reconstruire.

- **Utilisation** :

Une fonction à sens unique est difficile à inverser mais, pour une image donnée, elle peut avoir plusieurs antécédants.

↪ L'image d'une fonction à sens unique ou de **hachage** est souvent appelée **condensat**.

- **Fait** : Le condensat *caractérise* la donnée mais ne peut la reconstruire.

- **Utilisation** :
 - somme de contrôle

Une fonction à sens unique est difficile à inverser mais, pour une image donnée, elle peut avoir plusieurs antécédants.

↪ L'image d'une fonction à sens unique ou de **hachage** est souvent appelée **condensat**.

- **Fait** : Le condensat *caractérise* la donnée mais ne peut la reconstruire.

- **Utilisation** :
 - somme de contrôle
 - enregistrement de mot de passe

Une fonction à sens unique est difficile à inverser mais, pour une image donnée, elle peut avoir plusieurs antécédants.

↪ L'image d'une fonction à sens unique ou de **hachage** est souvent appelée **condensat**.

- **Fait** : Le condensat *caractérise* la donnée mais ne peut la reconstruire.

- **Utilisation** :
 - somme de contrôle
 - enregistrement de mot de passe
 - signature de fichier

Une fonction à sens unique est difficile à inverser mais, pour une image donnée, elle peut avoir plusieurs antécédants.

↪ L'image d'une fonction à sens unique ou de **hachage** est souvent appelée **condensat**.

- **Fait** : Le condensat *caractérise* la donnée mais ne peut la reconstruire.

- **Utilisation** :

- somme de contrôle
- enregistrement de mot de passe
- signature de fichier
- table de hachage

Les fonctions de hachages connues

Voici les fonctions de hachages les plus connues :

Les fonctions de hachages connues

Voici les fonctions de hachages les plus connues :

- DES, clé de 56 bits

Les fonctions de hachages connues

Voici les fonctions de hachages les plus connues :

- DES, clé de 56 bits
- 3DES, clé de 112 bits

Les fonctions de hachages connues

Voici les fonctions de hachages les plus connues :

- DES, clé de 56 bits
- 3DES, clé de 112 bits
- MD5, clé de 128 bits

Les fonctions de hachages connues

Voici les fonctions de hachages les plus connues :

- DES, clé de 56 bits
- 3DES, clé de 112 bits
- MD5, clé de 128 bits
- SHA1, clé de 160 bits

Les fonctions de hachages connues

Voici les fonctions de hachages les plus connues :

- DES, clé de 56 bits
- 3DES, clé de 112 bits
- MD5, clé de 128 bits
- SHA1, clé de 160 bits
- SHA2, clé de 256 bits

Comment inverser une fonction de hachage

Par force brut : on calcul le haché de toutes les entrées possibles.

Comment inverser une fonction de hachage

Par force brut : on calcul le haché de toutes les entrées possibles.

Par dictionnaire : on calcul le haché de mots présents dans un dictionnaire.

Comment inverser une fonction de hachage

Par force brut : on calcul le haché de toutes les entrées possibles.

Par dictionnaire : on calcul le haché de mots présents dans un dictionnaire.

Par table arc-en-ciel : mélange les idées des deux méthodes précédentes.

Fonction de hachage et mot de passe

Afin d'augmenter la sécurité, on ne hache pas directement un mot de passe. En effet, on hache le mot de passe augmenté d'un **sel**.

Le **sel** peut être un haché obtenu à partir :

Fonction de hachage et mot de passe

Afin d'augmenter la sécurité, on ne hache pas directement un mot de passe. En effet, on hache le mot de passe augmenté d'un **sel**.

Le **sel** peut être un haché obtenu à partir :

- du nom d'utilisateur,

Fonction de hachage et mot de passe

Afin d'augmenter la sécurité, on ne hache pas directement un mot de passe. En effet, on hache le mot de passe augmenté d'un **sel**.

Le **sel** peut être un haché obtenu à partir :

- du nom d'utilisateur,
- de la date de création du compte,

Fonction de hachage et mot de passe

Afin d'augmenter la sécurité, on ne hache pas directement un mot de passe. En effet, on hache le mot de passe augmenté d'un **sel**.

Le **sel** peut être un haché obtenu à partir :

- du nom d'utilisateur,
- de la date de création du compte,
- du numéro d'utilisateur.

Fonction de hachage et mot de passe

Afin d'augmenter la sécurité, on ne hache pas directement un mot de passe. En effet, on hache le mot de passe augmenté d'un **sel**.

Le **sel** peut être un haché obtenu à partir :

- du nom d'utilisateur,
- de la date de création du compte,
- du numéro d'utilisateur.

↪ Grâce au **sel**, si deux utilisateurs ont le même mot de pass, les hachés seront différents.

Fonction de hachage et mot de passe

Afin d'augmenter la sécurité, on ne hache pas directement un mot de passe. En effet, on hache le mot de passe augmenté d'un **sel**.

Le **sel** peut être un haché obtenu à partir :

- du nom d'utilisateur,
- de la date de création du compte,
- du numéro d'utilisateur.

↪ Grâce au **sel**, si deux utilisateurs ont le même mot de pass, les hachés seront différents.

↪ L'attaque par dictionnaire ou table arc-en-ciel devient pratiquement impossible.

Définition

- **Définition** : La **signature numérique** est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité.

Définition

- **Définition** : La **signature numérique** est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité.

Utilisation :

Définition

• **Définition** : La **signature numérique** est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité.

Utilisation :

- Prouver que je suis l'auteur d'un document.

Définition

• **Définition** : La **signature numérique** est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité.

Utilisation :

- Prouver que je suis l'auteur d'un document.
- Permettre à un tiers de prouver que je suis l'auteur d'un document.

Définition

• **Définition** : La **signature numérique** est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité.

Utilisation :

- Prouver que je suis l'auteur d'un document.
- Permettre à un tiers de prouver que je suis l'auteur d'un document.
- ...

Définition

• **Définition** : La **signature numérique** est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité.

Utilisation :

- Prouver que je suis l'auteur d'un document.
- Permettre à un tiers de prouver que je suis l'auteur d'un document.
- ...

Le schéma de signatures est constitués de :

- un algorithme de **signature**, utilisant la clé privée de l'expéditeur

Définition

• **Définition** : La **signature numérique** est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité.

Utilisation :

- Prouver que je suis l'auteur d'un document.
- Permettre à un tiers de prouver que je suis l'auteur d'un document.
- ...

Le schéma de signatures est constitués de :

- un algorithme de **signature**, utilisant la clé privée de l'expéditeur
- un algorithme de **vérification**, utilisant la clé publique de l'expéditeur

• **Fait** : On ne signe jamais directement un message mais son haché.

Certificat

- **Problème** : Il n'y a pas de correspondance entre une personne physique et une **paire de clés**.

Certificat

- **Problème** : Il n'y a pas de correspondance entre une personne physique et une **paire de clés**.

- **Définition** : Un **certificat** est un document électronique qui atteste traditionnellement qu'une clé publique est bien liée à une organisation ou une personne.

Certificat

- **Problème** : Il n'y a pas de correspondance entre une personne physique et une **paire de clés**.

- **Définition** : Un **certificat** est un document électronique qui atteste traditionnellement qu'une clé publique est bien liée à une organisation ou une personne.

Le certificat répond à la question : Qu'est-ce qui me prouve que M. X est bien le détenteur de la clé publique qu'il m'a fournie pour vérifier la signature de ces messages (par exemple).

Certificat

- **Définition:** Une infrastructure à clé publique (ou **PKI**) est un ensemble de technologies et politiques permettant de créer et d'utiliser des certificats.

Certificat

- **Définition:** Une infrastructure à clé publique (ou **PKI**) est un ensemble de technologies et politiques permettant de créer et d'utiliser des certificats.

Elle est composée d'une :

Certificat

- **Définition:** Une infrastructure à clé publique (ou **PKI**) est un ensemble de technologies et politiques permettant de créer et d'utiliser des certificats.

Elle est composée d'une :

- autorité de certification (**CA** ou **AC**) qui signe les certificats (après qu'on ait formulé une demande de signature, **CSR**).

Certificat

- **Définition:** Une infrastructure à clé publique (ou **PKI**) est un ensemble de technologies et politiques permettant de créer et d'utiliser des certificats.

Elle est composée d'une :

- autorité de certification (**CA** ou **AC**) qui signe les certificats (après qu'on ait formulé une demande de signature, **CSR**).
- autorité d'enregistrement (**AE** ou **RA**) qui gènes les certificats et fait les certifications d'usage.

Certificat

- **Définition:** Une infrastructure à clé publique (ou **PKI**) est un ensemble de technologies et politiques permettant de créer et d'utiliser des certificats.

Elle est composée d'une :

- autorité de certification (**CA** ou **AC**) qui signe les certificats (après qu'on ait formulé une demande de signature, **CSR**).
- autorité d'enregistrement (**AE** ou **RA**) qui gènes les certificats et fait les certifications d'usage.
- autorité de dépôt qui stocke les certificats et gère les listes de révocation

Certificat

- **Définition:** Une infrastructure à clé publique (ou **PKI**) est un ensemble de technologies et politiques permettant de créer et d'utiliser des certificats.

Elle est composée d'une :

- autorité de certification (**CA** ou **AC**) qui signe les certificats (après qu'on ait formulé une demande de signature, CSR).
- autorité d'enregistrement (**AE** ou **RA**) qui gènères les certificats et fait les certifications d'usage.
- autorité de dépôt qui stocke les certificats et gère les listes de révocation
- l'entité finale, qui est le sujet du certificat.

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :
 - classe 1 : adresse électronique du demandeur requise

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :
 - classe 1 : adresse électronique du demandeur requise
 - classe 2 : preuve de l'identité requise

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :
 - classe 1 : adresse électronique du demandeur requise
 - classe 2 : preuve de l'identité requise
 - classe 3 : présence physique du demandeur

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :
 - classe 1 : adresse électronique du demandeur requise
 - classe 2 : preuve de l'identité requise
 - classe 3 : présence physique du demandeur
 - class 3+ : comme la classe 3, mais le certificat est stocké sur un support physique (clé USB à puce, carte à puce, ...)

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :
 - classe 1 : adresse électronique du demandeur requise
 - classe 2 : preuve de l'identité requise
 - classe 3 : présence physique du demandeur
 - class 3+ : comme la classe 3, mais le certificat est stocké sur un support physique (clé USB à puce, carte à puce, ...)
- Il contient en outre :

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :
 - classe 1 : adresse électronique du demandeur requise
 - classe 2 : preuve de l'identité requise
 - classe 3 : présence physique du demandeur
 - class 3+ : comme la classe 3, mais le certificat est stocké sur un support physique (clé USB à puce, carte à puce, ...)
- Il contient en outre :
 - un numéro de série

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :
 - classe 1 : adresse électronique du demandeur requise
 - classe 2 : preuve de l'identité requise
 - classe 3 : présence physique du demandeur
 - class 3+ : comme la classe 3, mais le certificat est stocké sur un support physique (clé USB à puce, carte à puce, ...)
- Il contient en outre :
 - un numéro de série
 - identification algorithme signature

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :
 - classe 1 : adresse électronique du demandeur requise
 - classe 2 : preuve de l'identité requise
 - classe 3 : présence physique du demandeur
 - class 3+ : comme la classe 3, mais le certificat est stocké sur un support physique (clé USB à puce, carte à puce, ...)
- Il contient en outre :
 - un numéro de série
 - identification algorithme signature
 - désignation de l'autorité de certification

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :
 - classe 1 : adresse électronique du demandeur requise
 - classe 2 : preuve de l'identité requise
 - classe 3 : présence physique du demandeur
 - class 3+ : comme la classe 3, mais le certificat est stocké sur un support physique (clé USB à puce, carte à puce, ...)
- Il contient en outre :
 - un numéro de série
 - identification algorithme signature
 - désignation de l'autorité de certification
 - période de validité

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :
 - classe 1 : adresse électronique du demandeur requise
 - classe 2 : preuve de l'identité requise
 - classe 3 : présence physique du demandeur
 - class 3+ : comme la classe 3, mais le certificat est stocké sur un support physique (clé USB à puce, carte à puce, ...)
- Il contient en outre :
 - un numéro de série
 - identification algorithme signature
 - désignation de l'autorité de certification
 - période de validité
 - nom du titulaire de la clé publique

Certificat : contenu

- Il existe 4 types de certificats en fonction du niveau de sécurité :
 - classe 1 : adresse électronique du demandeur requise
 - classe 2 : preuve de l'identité requise
 - classe 3 : présence physique du demandeur
 - class 3+ : comme la classe 3, mais le certificat est stocké sur un support physique (clé USB à puce, carte à puce, ...)
- Il contient en outre :
 - un numéro de série
 - identification algorithme signature
 - désignation de l'autorité de certification
 - période de validité
 - nom du titulaire de la clé publique
 - ...