Cryptographie : définition

• Définition : La cryptographie traditionelle 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 traditionelle 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 a envoyer est appelé message en clair.

Cryptographie : définition

• Définition : La cryptographie traditionelle 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 a envoyer est appelé message en clair.
On note $\mathcal{M}$ l'ensemble des messages en clair.

Cryptographie : définition

• Définition : La cryptographie traditionelle 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 a 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 traditionelle 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 a 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 traditionelle 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 a 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
$$f : \mathcal{M} \to \mathcal{C}$$

Cryptographie : définition

• Définition : La cryptographie traditionelle 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 a 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
$$f : \mathcal{M} \to \mathcal{C}$$
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 :

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

Fonction de chiffrement : exemple

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

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

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

Fonction de chiffrement : exemple

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

f(Au mon dieu ! Ils ont tues Kenny) = ynneK seut tno sIl ! ueid nom uA

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

f(Au mon dieu ! Ils ont tues Kenny) = Bv npo ejfv ! Jmt pou uvft Lfooz

Fonction de chiffrement : exemple

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

f(Au mon dieu ! Ils ont tues Kenny) = ynneK seut tno sIl ! ueid nom uA

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

f(Au mon dieu ! Ils ont tues Kenny) = 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(Au mon dieu ! Ils ont tues Kenny) = ynneK seut tno sIl ! ueid nom uA

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

f(Au mon dieu ! Ils ont tues Kenny) = Bv npo ejfv ! Jmt pou uvft Lfooz

- Exemple : Mélange des deux :

f(Au mon dieu ! Ils ont tues Kenny) = zoofL tfvu uop tmJ ! vfje opn vB

Le chiffrement par décalage de lettres est souvent appelé chiffrement de César.

Le chiffrement par décalage de lettres est souvent appelé chiffrement de César.

- Jules César employait un décalage de 3 lettres dans ses correspondances secrètes.

Le chiffrement par décalage de lettres est souvent appelé chiffrement de César.

- Jules César employait un décalage de 3 lettres dans ses correspondances secrètes.

– Son neveu Auguste employait quand à lui le décalage

$$a \to b,\ b \to C,\ ..., \$z \to aa.$$

Le chiffrement par décalage de lettres est souvent appelé chiffrement de César.

- Jules César employait un décalage de 3 lettres dans ses correspondances secrètes.

– Son neveu Auguste employait quand à lui le décalage

$$a \to b,\ b \to C,\ ..., \$z \to aa.$$

La méthode de chiffrement par décalage est très faible.

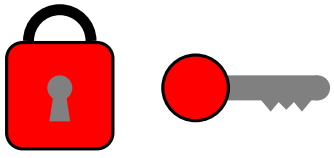
Le chiffrement par décalage de lettres est souvent appelé chiffrement de César.

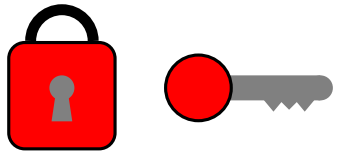
- Jules César employait un décalage de 3 lettres dans ses correspondances secrètes.

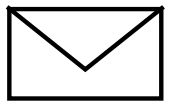
– Son neveu Auguste employait quand à lui le décalage

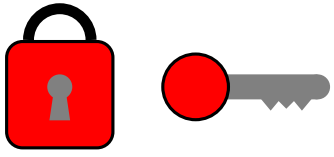
$$a \to b,\ b \to C,\ ..., \$z \to aa.$$

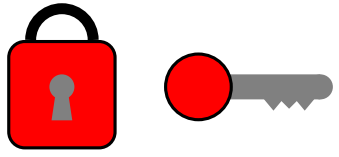
La méthode de chiffrement par décalage est très faible. Elle ne résiste pas aux attaques statistiques.

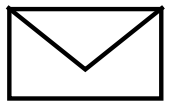


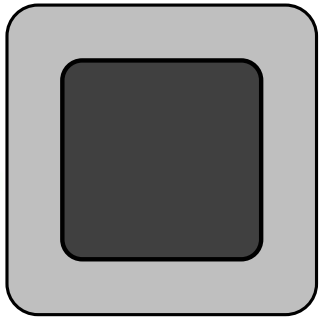


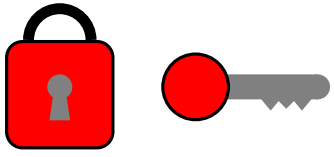


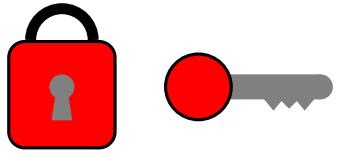


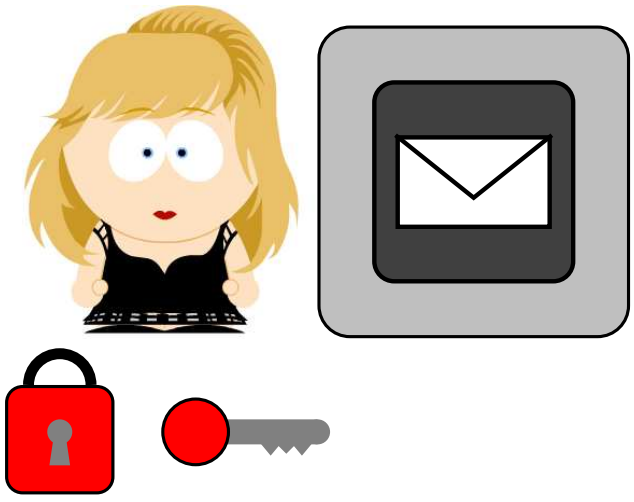


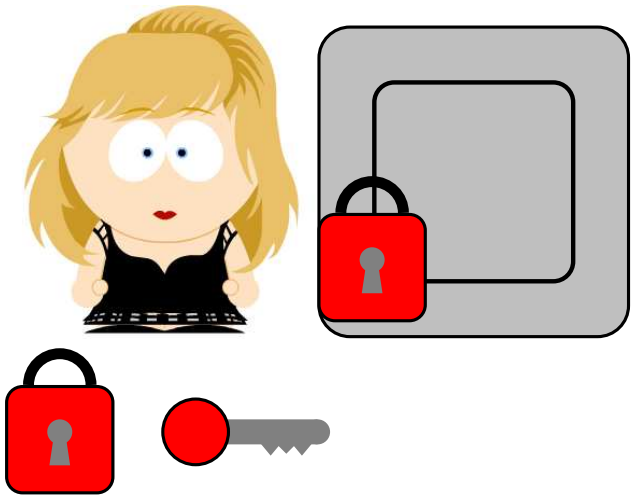


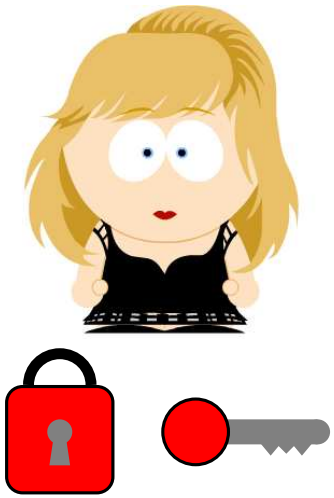


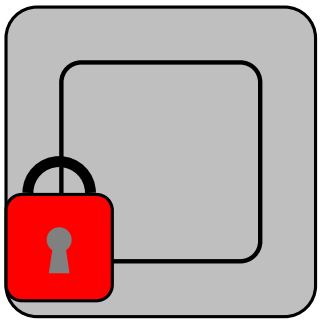


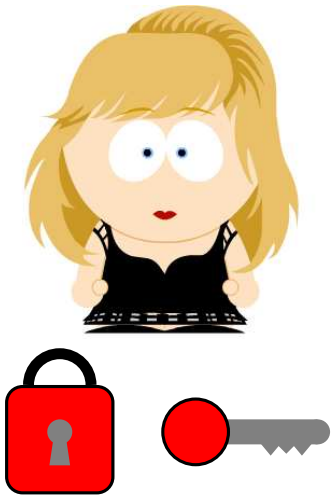


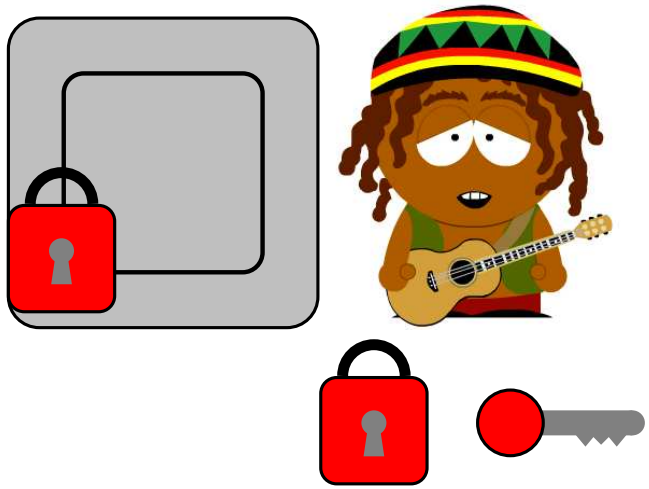


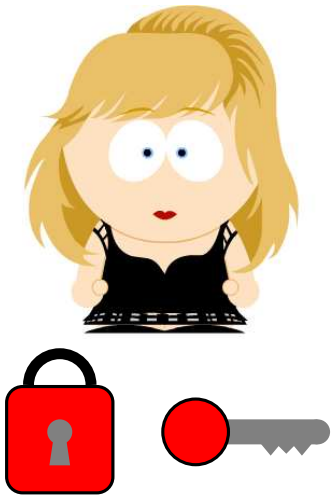


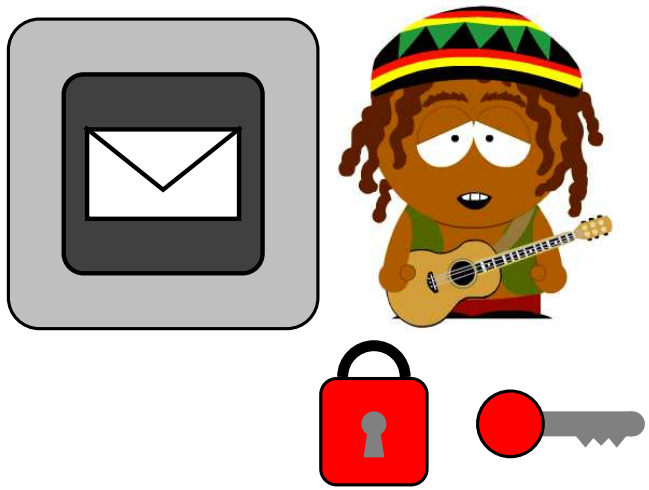


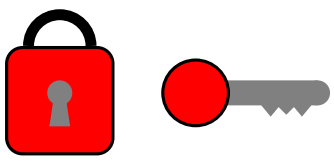


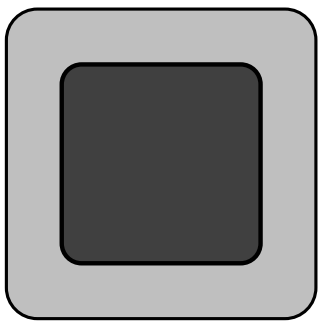


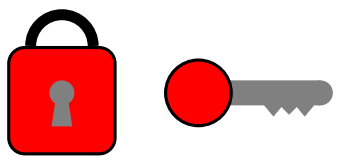












L'histoire a montré que chaque fois qu'une fonction de chiffrement f est destinée a être utilisée un nombre important de fois, il devient de plus en plus difficile de la maintenir complètement secrète.

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

$\rightsquigarrow$ Il faut changer régulièrement la fonction de chiffrement.

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

$\rightsquigarrow$ 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 a être utilisée un nombre important de fois, il devient de plus en plus difficile de la maintenir complètement secrète.

$\rightsquigarrow$ 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.

$\rightsquigarrow$ K est la Kouleur de la clé et du cadena.

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

$\rightsquigarrow$ 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.

$\rightsquigarrow$ K est la Kouleur de la clé et du cadena.

$\rightsquigarrow$ Oscar a un gros problème de vue : il ne voit pas les couleurs

$\rightsquigarrow$ surtout celle des cadenas.

- Exemple :

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

- Exemple :

$$f_k(\texttt{Au mon dieu ! Ils ont tues Kenny}) = \begin{cases} \texttt{Bv npo ejfv ! Jmt pou uvft Lfooz} & k = 1 \\ & \end{cases}$$

- Exemple :

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

- Exemple :

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

- Exemple :

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

- Exemple :

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

- Exemple :

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

- Exemple :

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

Systéme de Vernam

- Soit Σ un alphabet de cardinalité m.

Systéme de Vernam

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

Systéme 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 $\mathbb{Z}/m\mathbb{Z}$.

Systéme 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 $(\mathbb{Z}/m\mathbb{Z})^n$.

Systéme 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 $(k_1, ..., k_n)$ tiré aléatoirement dans $(\mathbb{Z}/m\mathbb{Z})^n$

Systéme 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 $(k_1, ..., k_n)$ tiré aléatoirement dans $(\mathbb{Z}/m\mathbb{Z})^n$

- La fonction de chiffrement est :

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

Systéme 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 $(k_1, ..., k_n)$ tiré aléatoirement dans $(\mathbb{Z}/m\mathbb{Z})^n$

- La fonction de chiffrement est :

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

où $\ell'_i = \ell_i + k_i \mod m$.

Systéme 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 $(k_1, ..., k_n)$ tiré aléatoirement dans $(\mathbb{Z}/m\mathbb{Z})^n$

- La fonction de chiffrement est :

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

où $\ell'_i = \ell_i + k_i \mod m$.

- C'est un système *parfait*.

Systéme 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 $(k_1, ..., k_n)$ tiré aléatoirement dans $(\mathbb{Z}/m\mathbb{Z})^n$

- La fonction de chiffrement est :

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

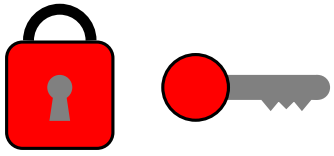
où $\ell'_i = \ell_i + k_i \mod m$.

- C'est un système *parfait*.

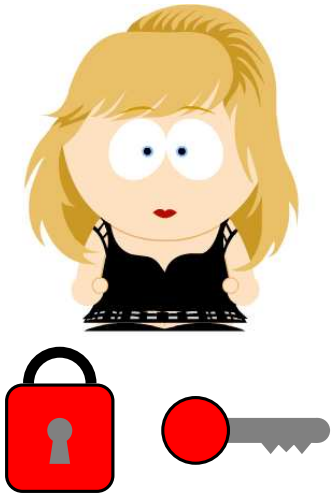
- Une clé K ne doit jamais être réutilisée : très lourd.

Comment faire sans partager une clé ?

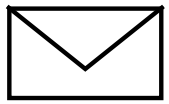
Comment faire sans partager une clé ?

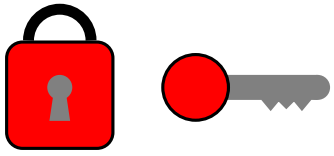


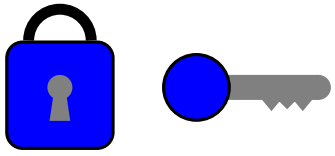
Comment faire sans partager une clé ?



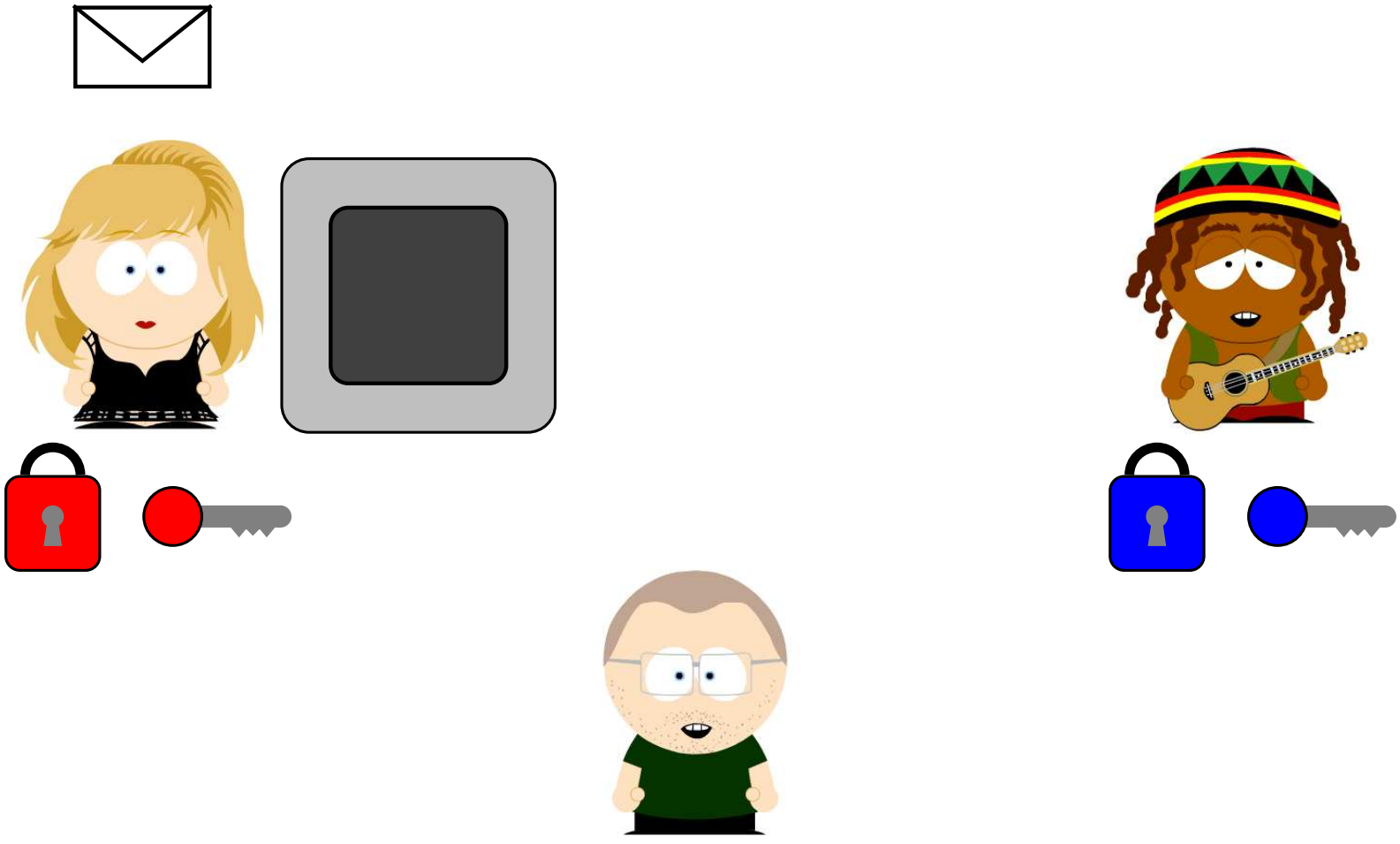
Comment faire sans partager une clé ?



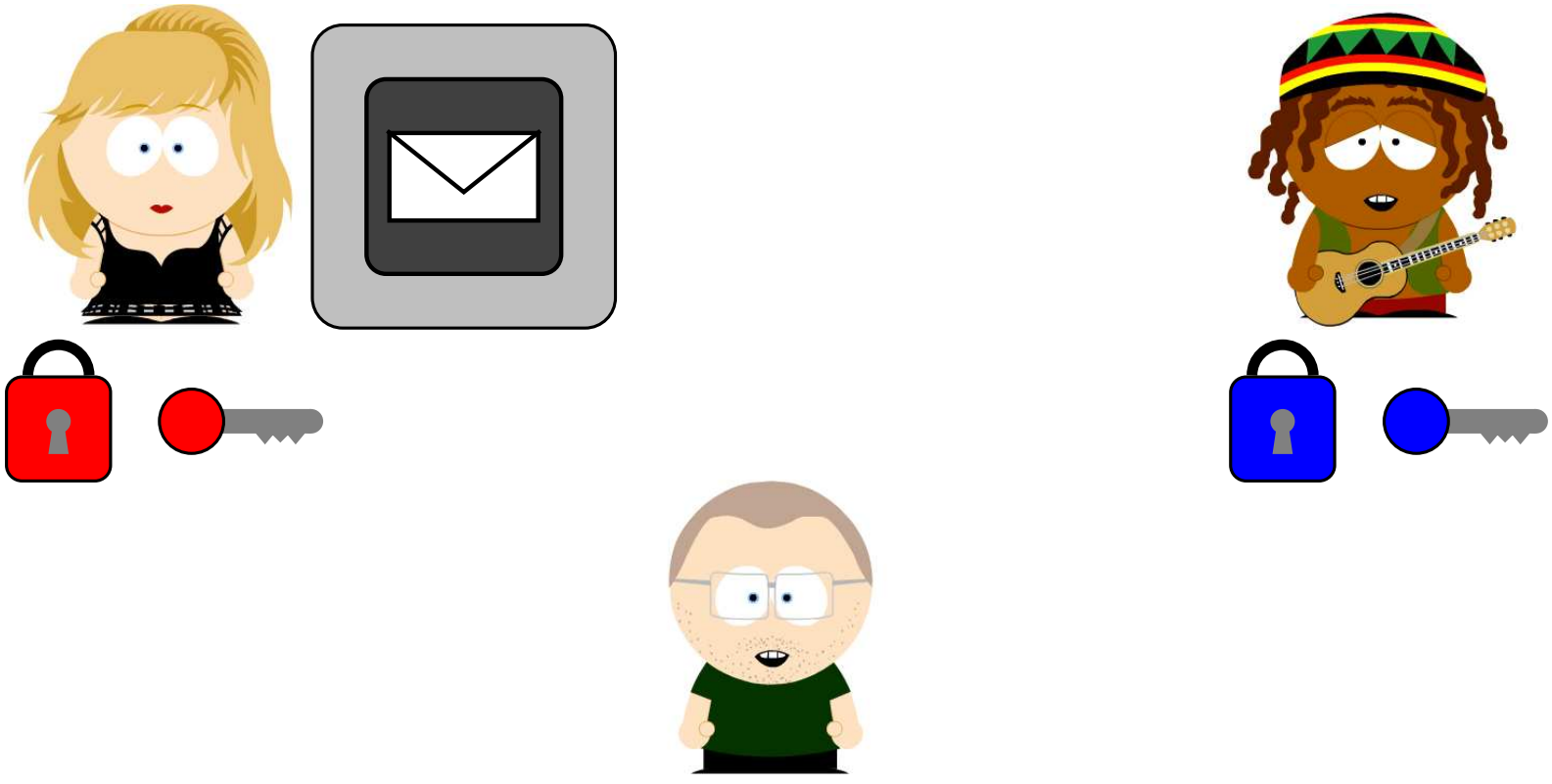




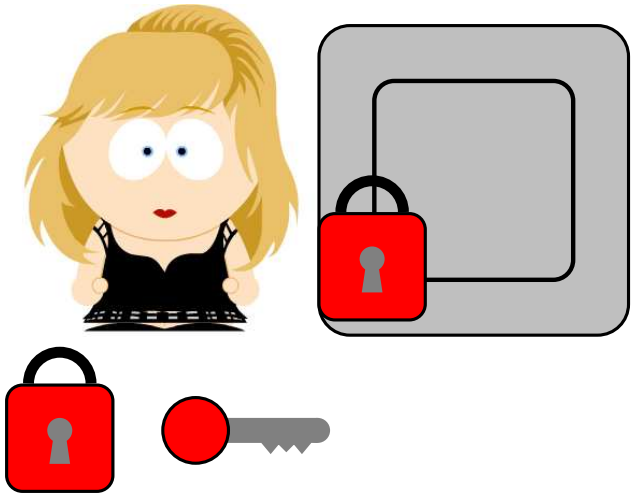
Comment faire sans partager une clé ?



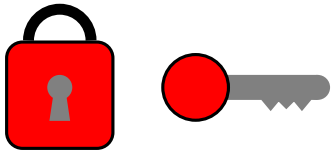
Comment faire sans partager une clé ?

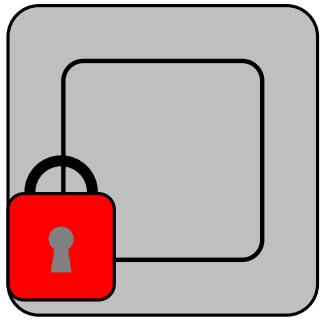


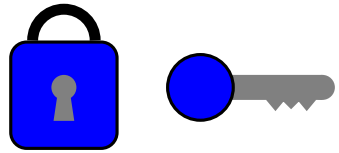
Comment faire sans partager une clé ?



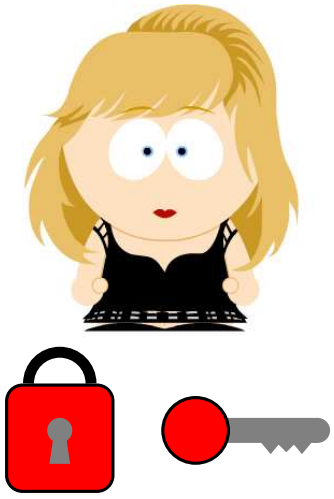
Comment faire sans partager une clé ?

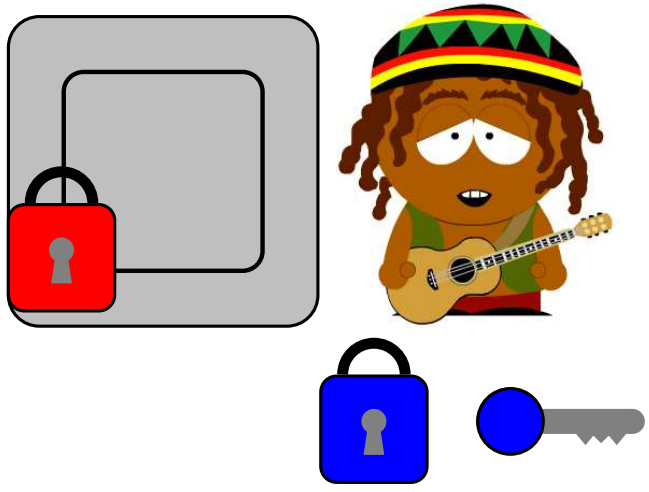




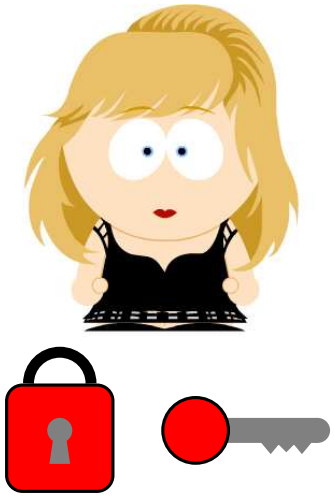


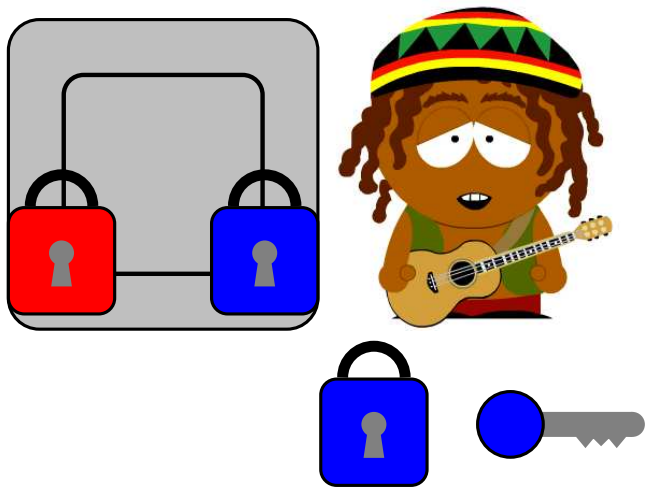
Comment faire sans partager une clé ?



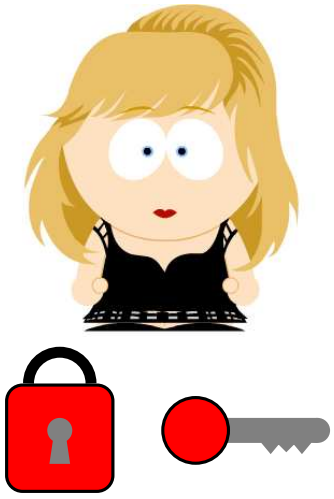


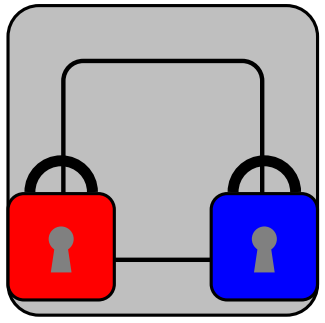
Comment faire sans partager une clé ?



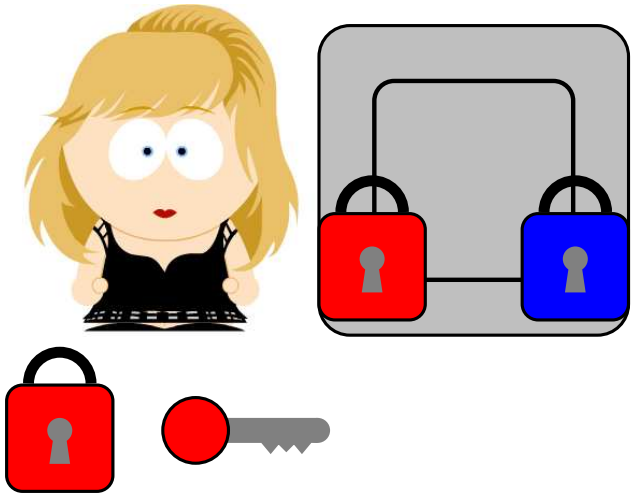


Comment faire sans partager une clé ?

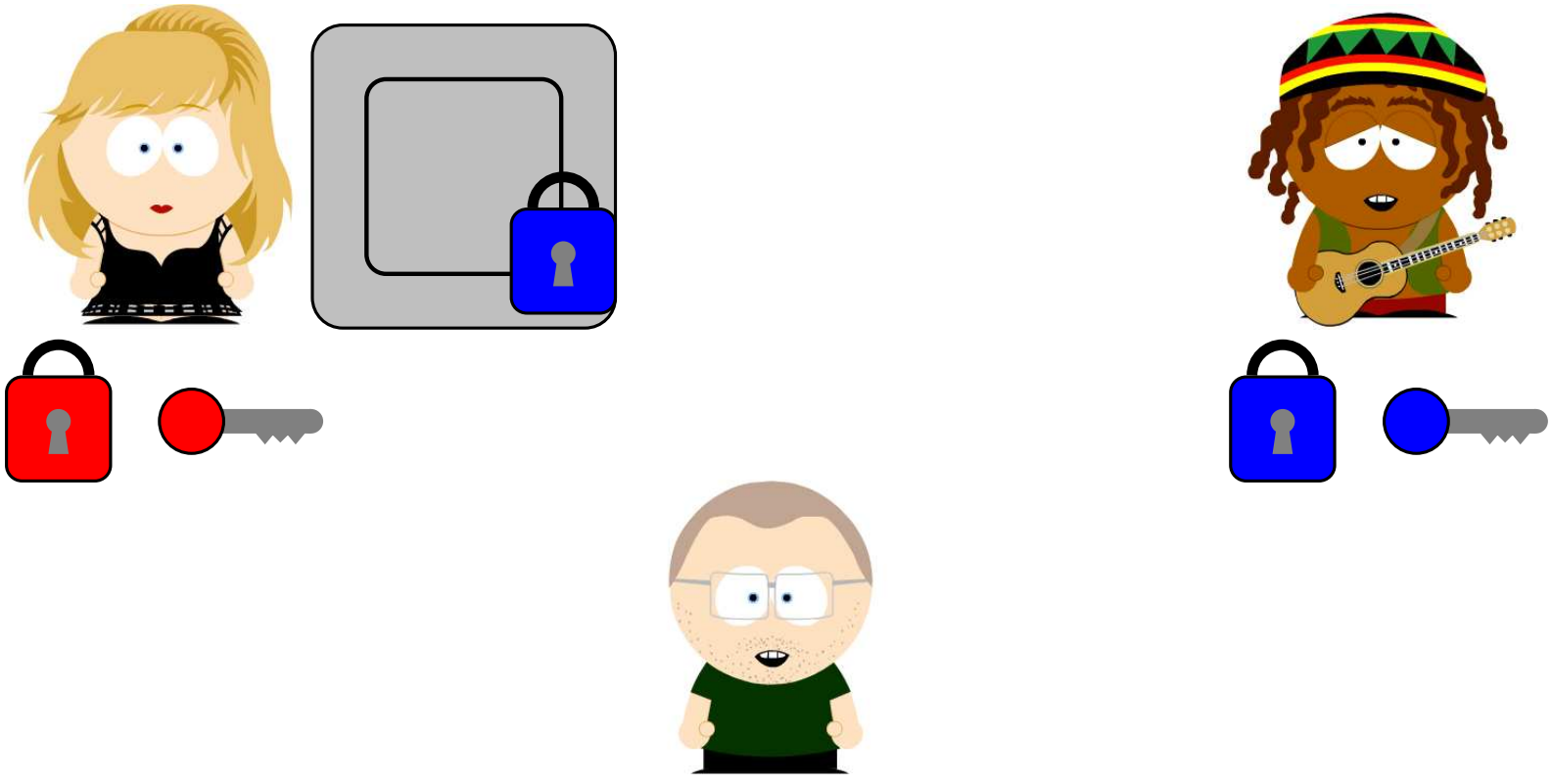




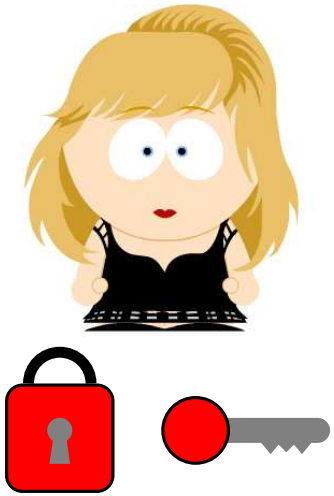
Comment faire sans partager une clé ?

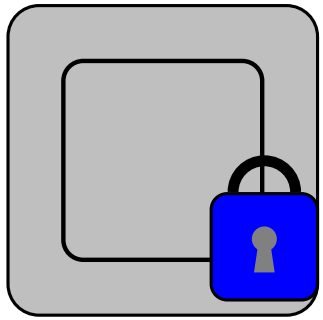


Comment faire sans partager une clé ?

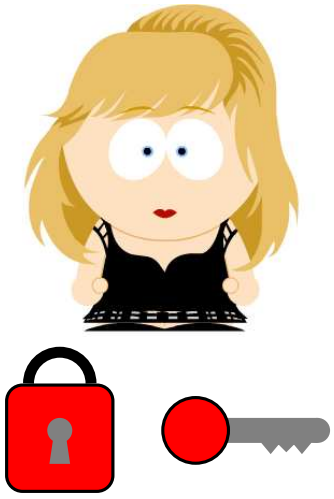


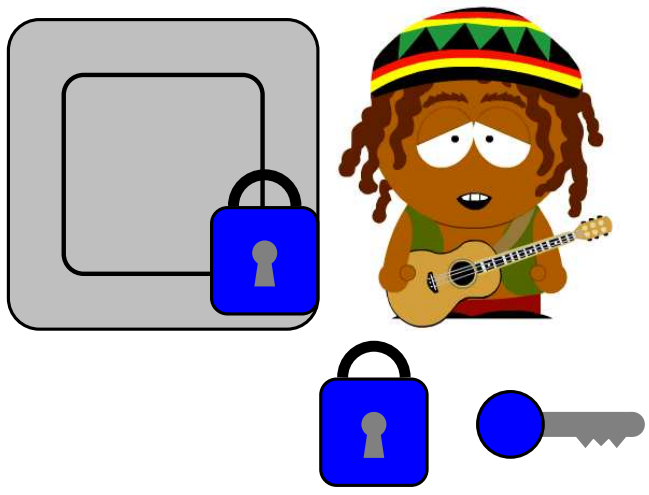
Comment faire sans partager une clé ?



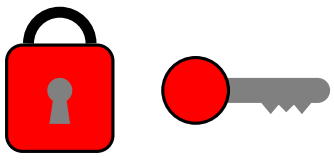


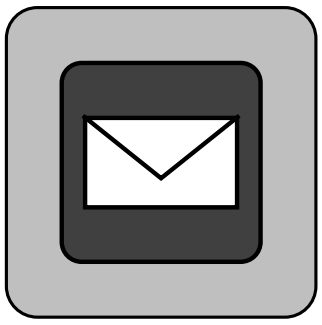
Comment faire sans partager une clé ?

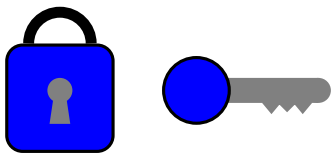




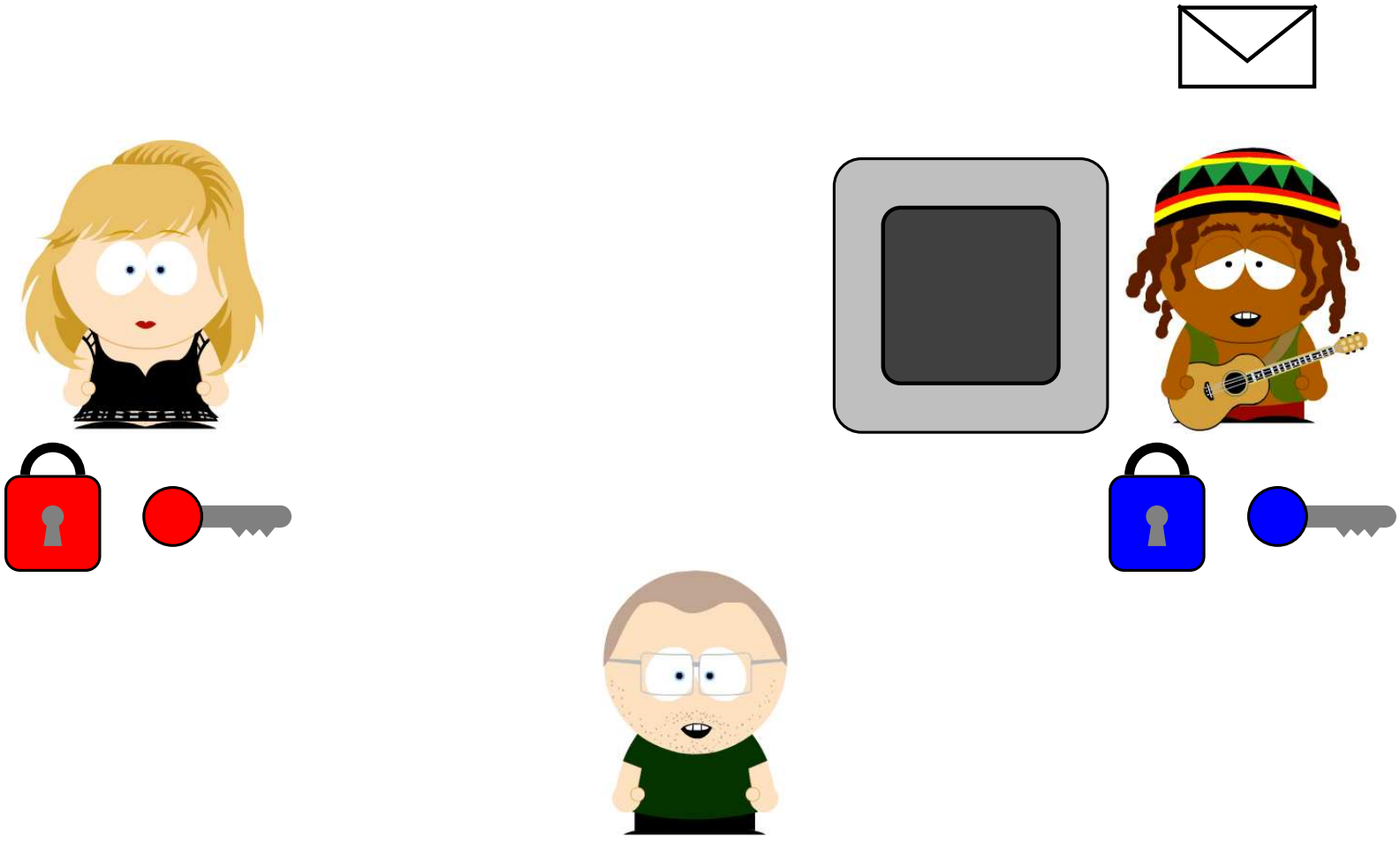
Comment faire sans partager une clé ?







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.

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).

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

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

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

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

• 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.

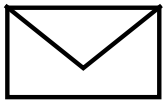
• Principe: N'importe qui peut chiffrer le message (grâce à la clé publique), mais une seule personne peut le déchiffrer (grâce à la clé secrète).

ou l'inverse

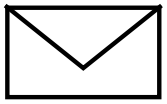
• Utilisation :
  – Partage de clé secrète
  – Paiement sécurisé
  – Authentification
  – ...

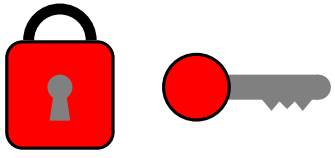
Cryptographique à clé publique : 1er schéma

Cryptographique à clé publique : 1er schéma

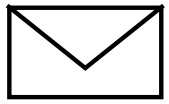


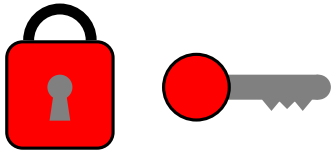
Cryptographique à clé publique : 1er schéma



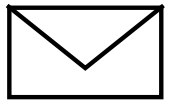


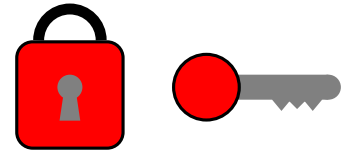
Cryptographique à clé publique : 1er schéma



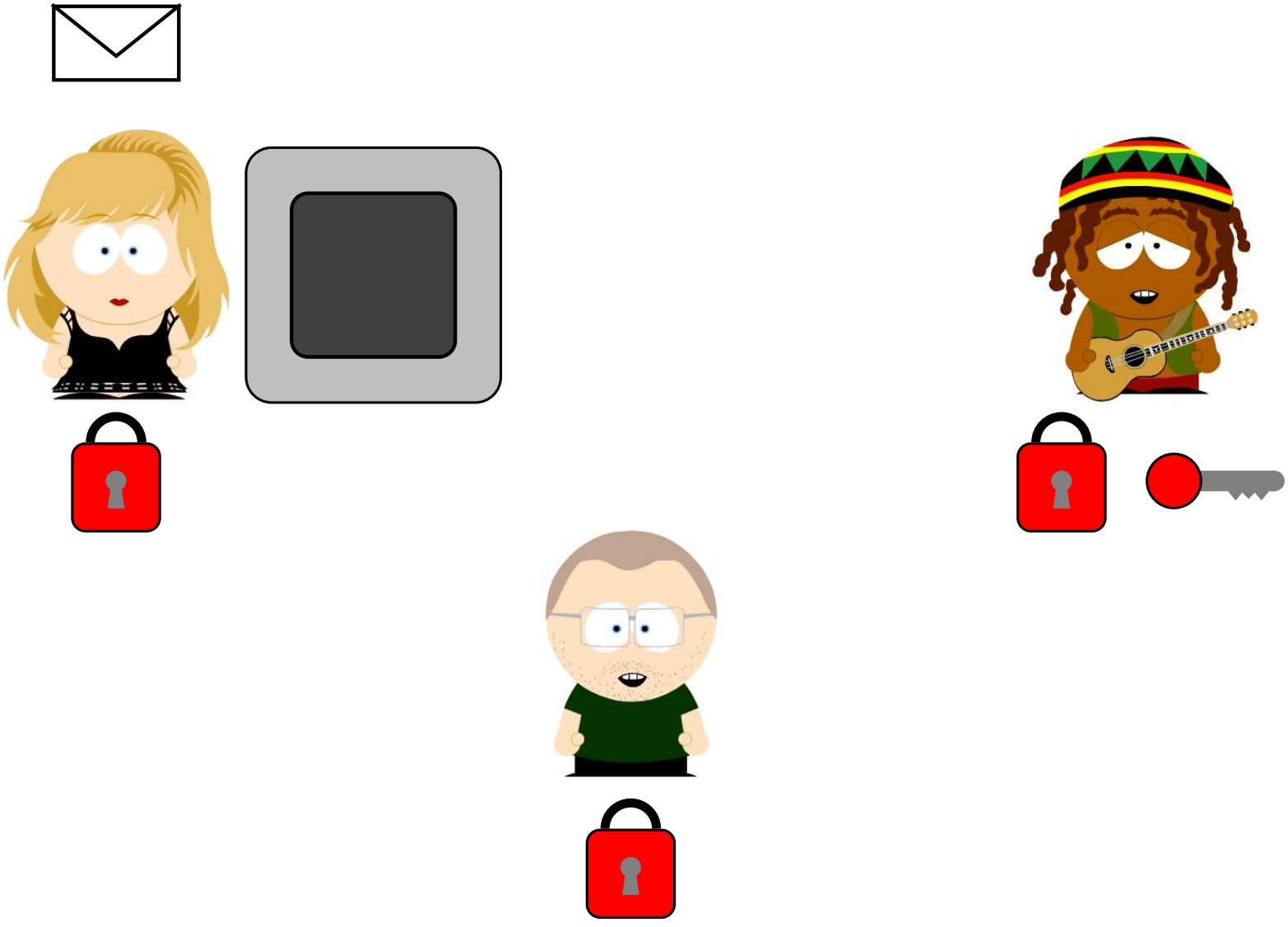


Cryptographique à clé publique : 1er schéma

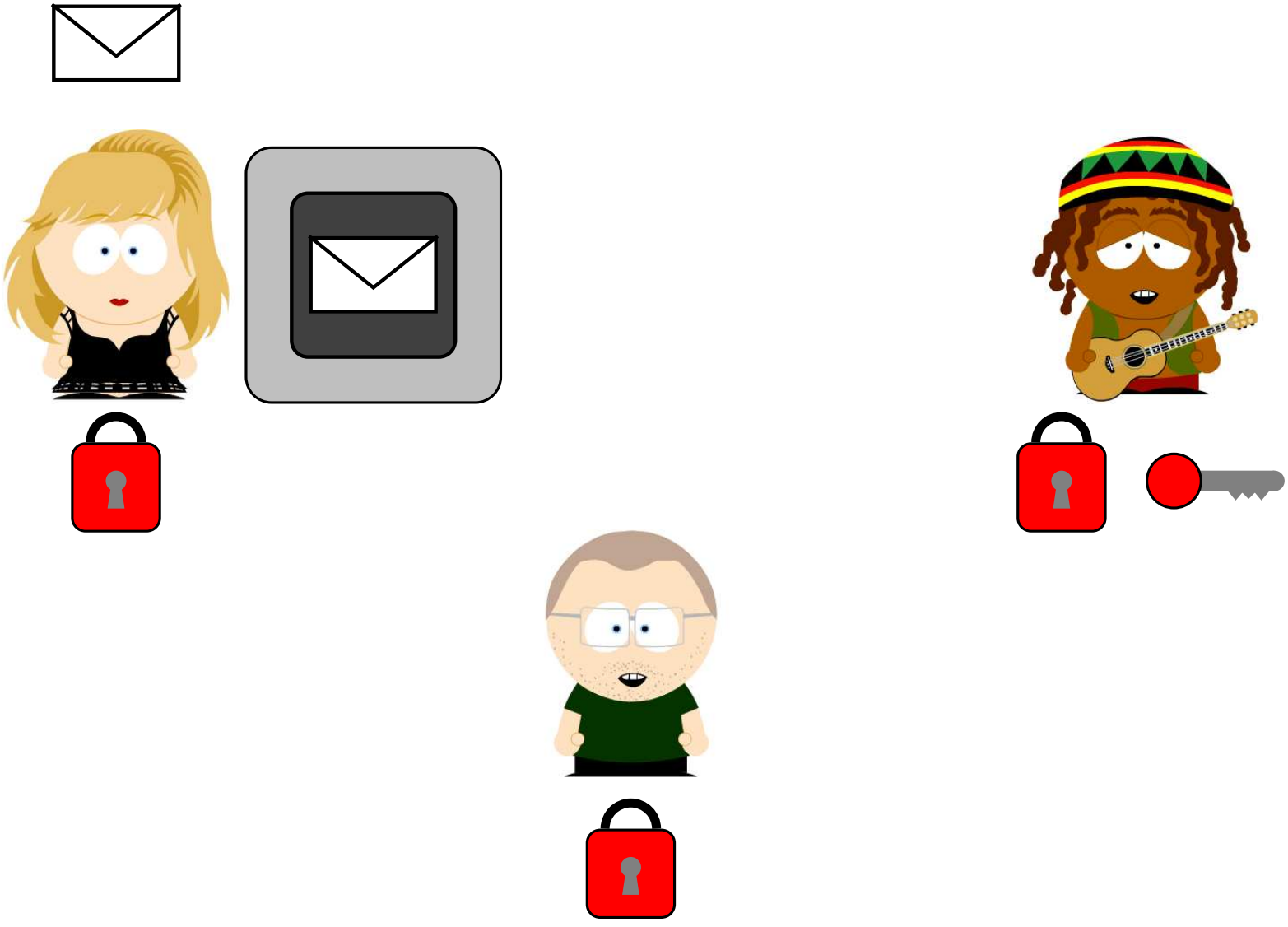




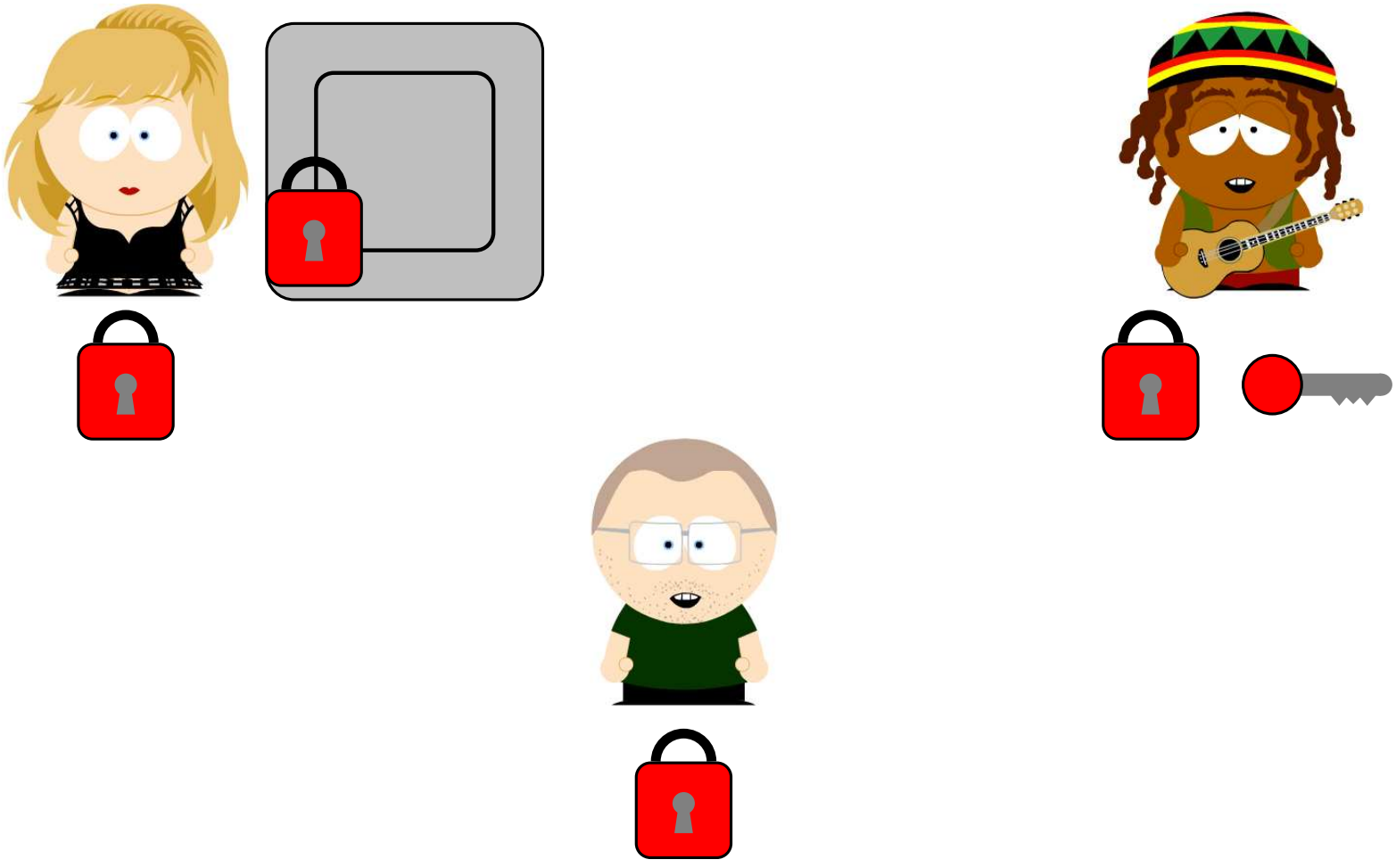
Cryptographique à clé publique : 1er schéma



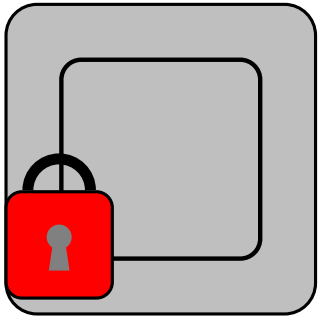
Cryptographique à clé publique : 1er schéma



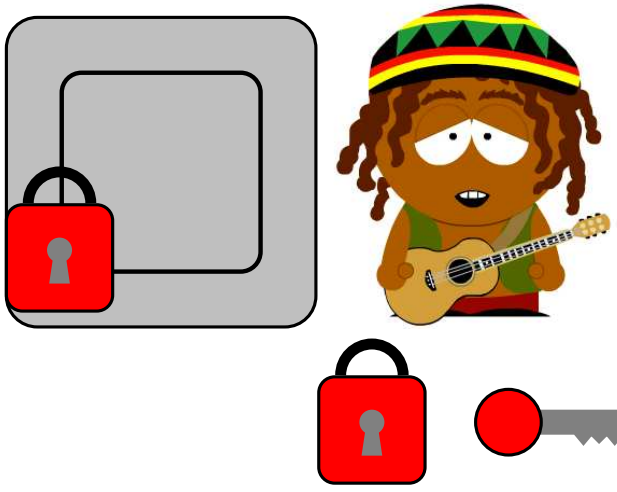
Cryptographique à clé publique : 1er schéma



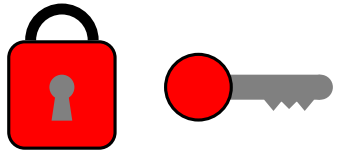
Cryptographique à clé publique : 1er schéma



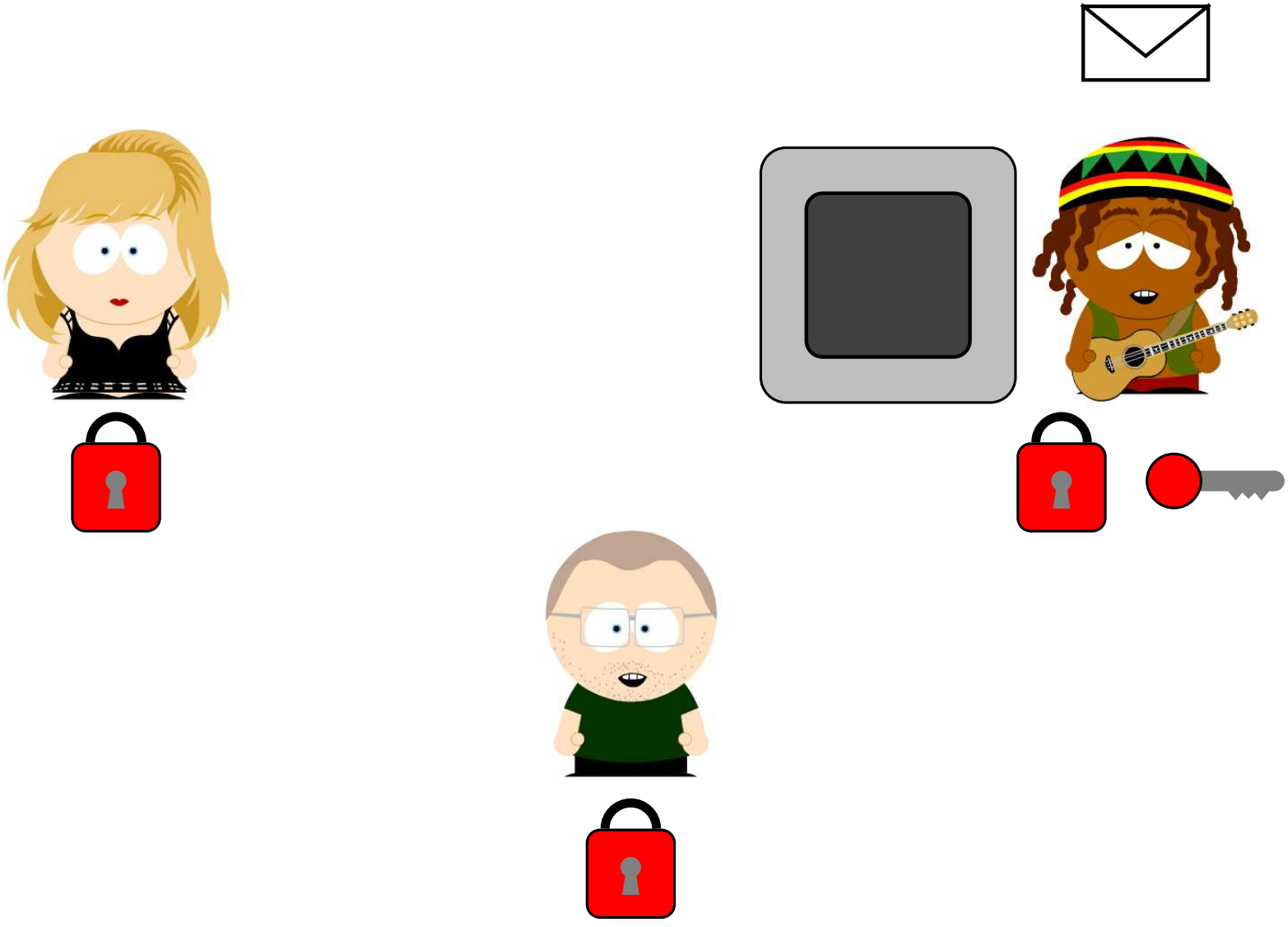
Cryptographique à clé publique : 1er schéma



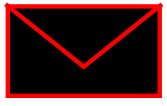
Cryptographique à clé publique : 1er schéma



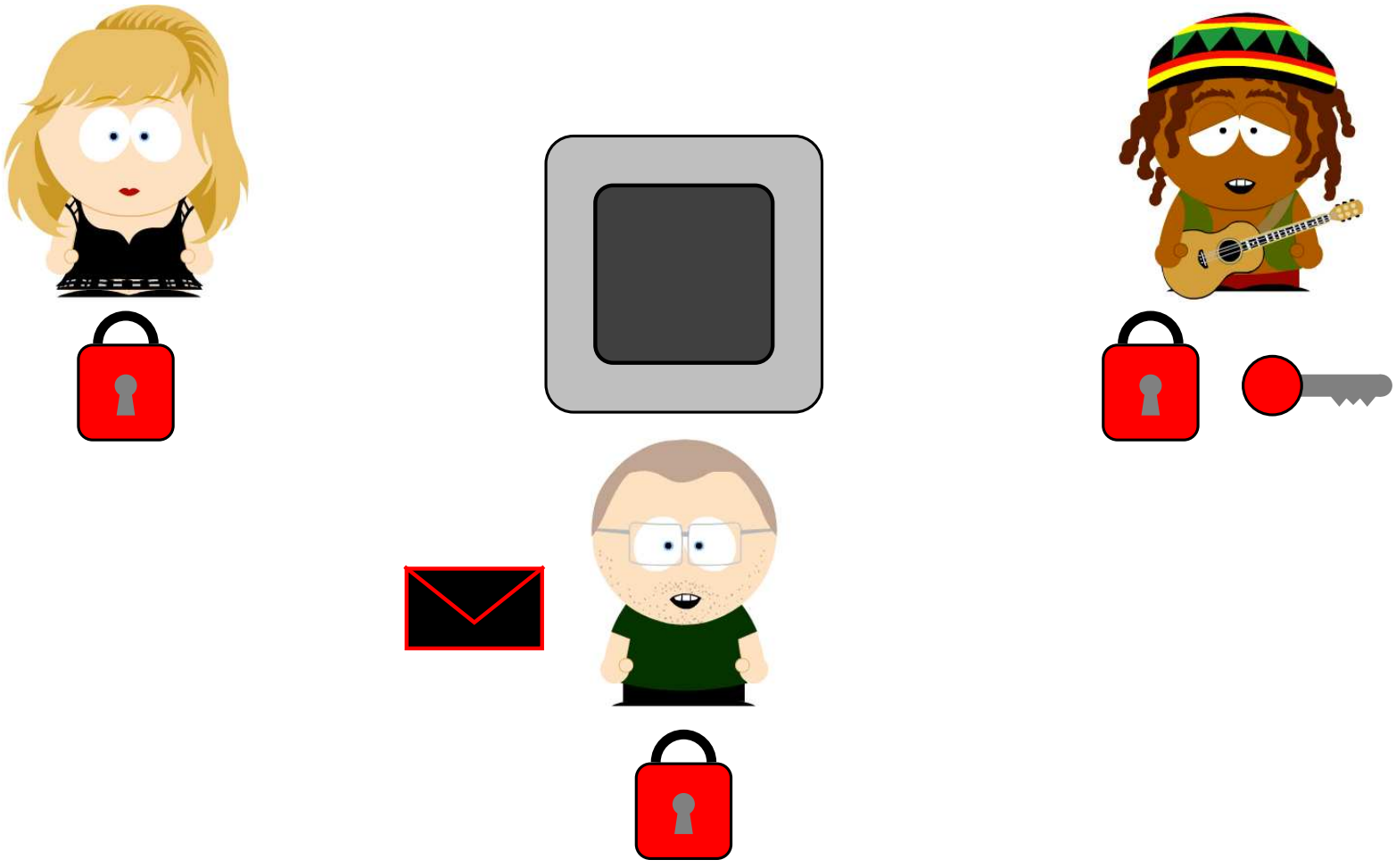
Cryptographique à clé publique : 1er schéma



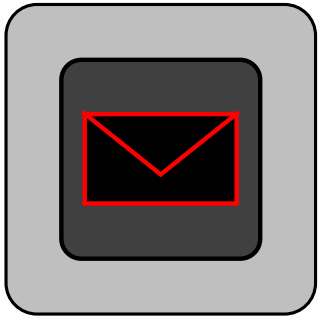
Cryptographique à clé publique : 1er schéma

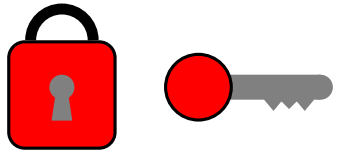


Cryptographique à clé publique : 1er schéma

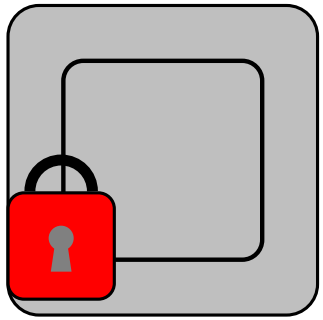


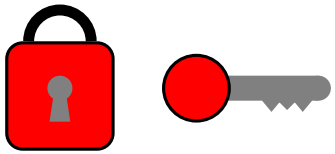
Cryptographique à clé publique : 1er schéma



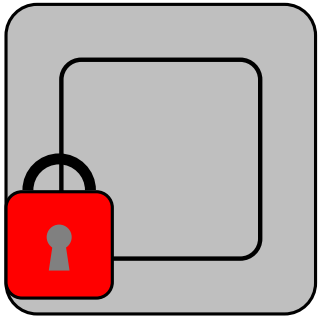


Cryptographique à clé publique : 1er schéma

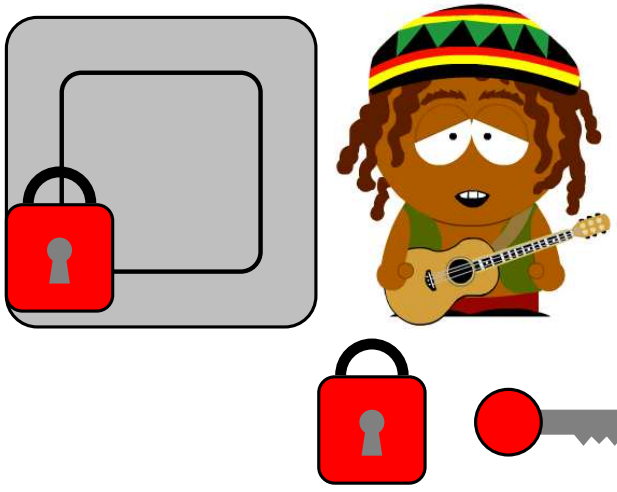




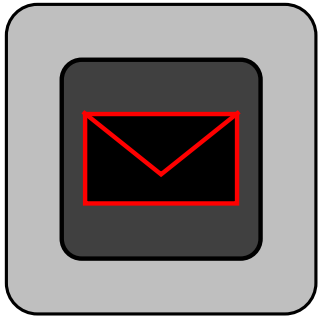
Cryptographique à clé publique : 1er schéma



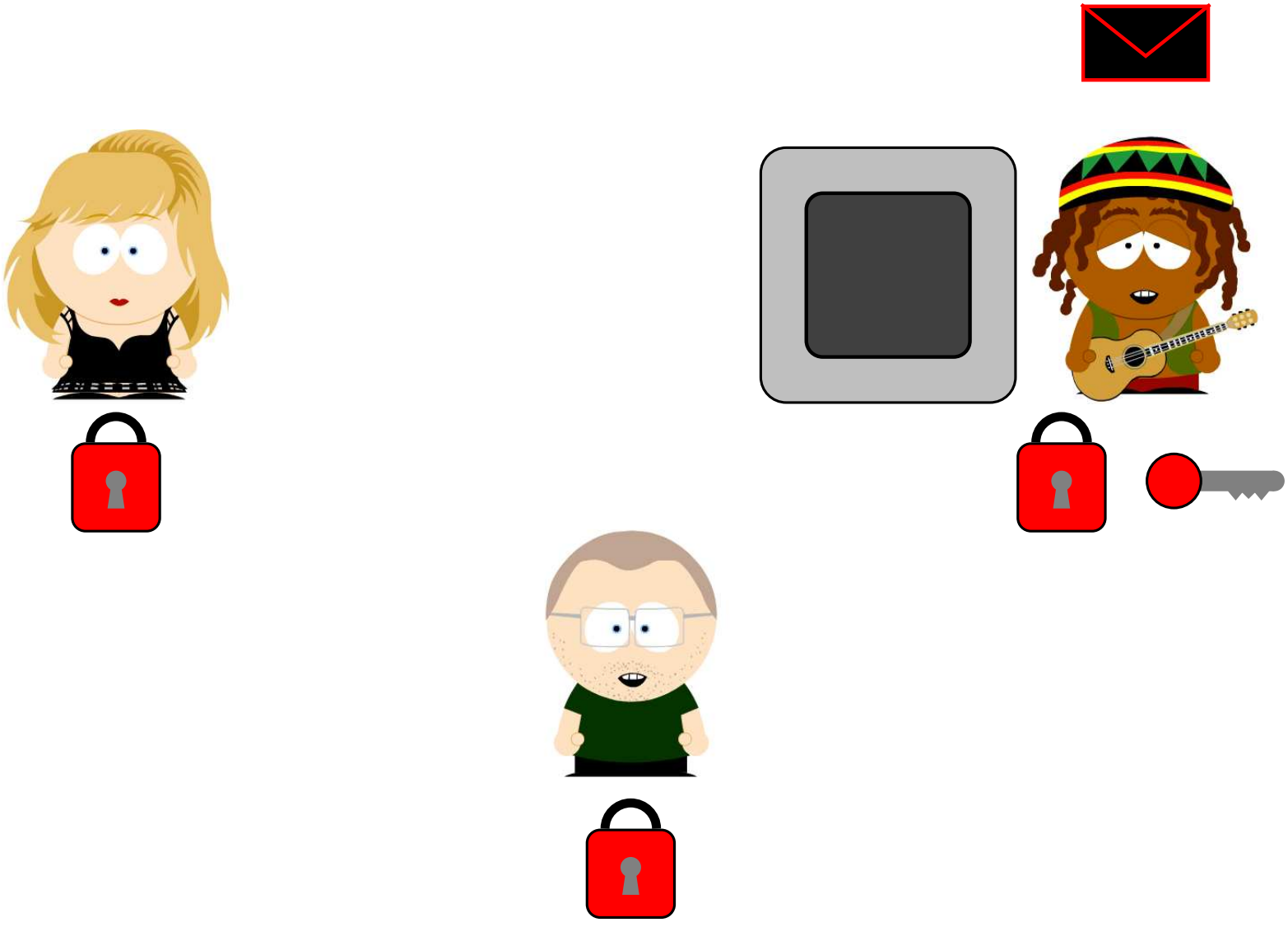
Cryptographique à clé publique : 1er schéma



Cryptographique à clé publique : 1er schéma

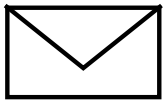


Cryptographique à clé publique : 1er schéma

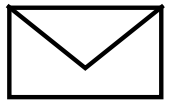


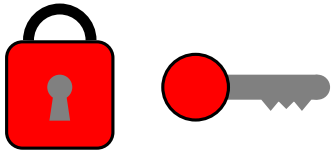
Cryptographique à clé publique : 2^{e} schéma

Cryptographique à clé publique : 2^{e} schéma

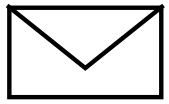


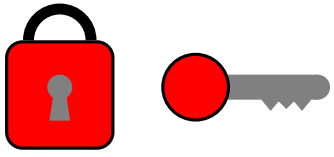
Cryptographique à clé publique : 2e schéma



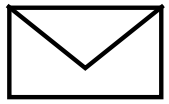


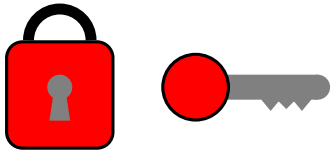
Cryptographique à clé publique : 2e schéma



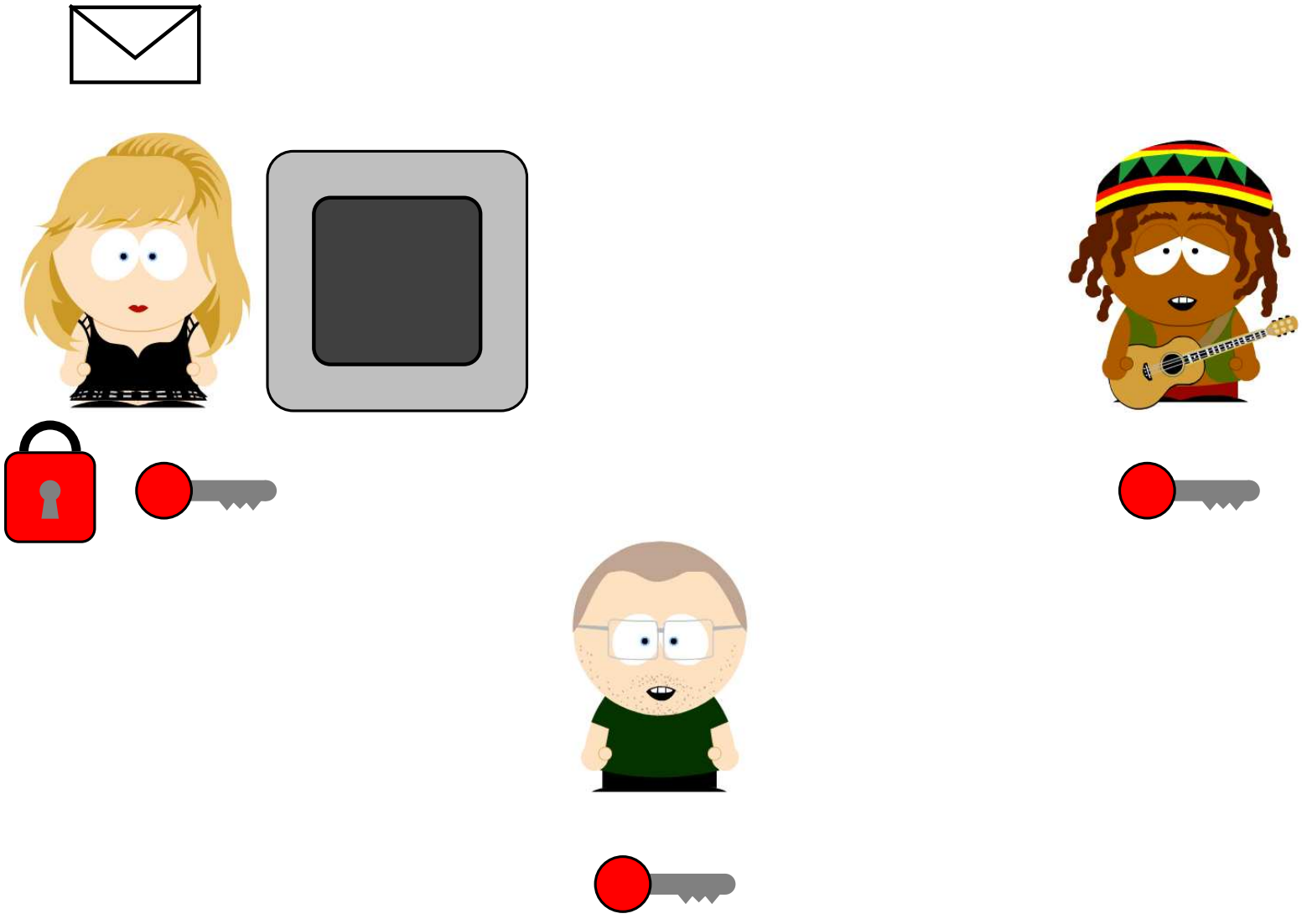


Cryptographique à clé publique : 2e schéma

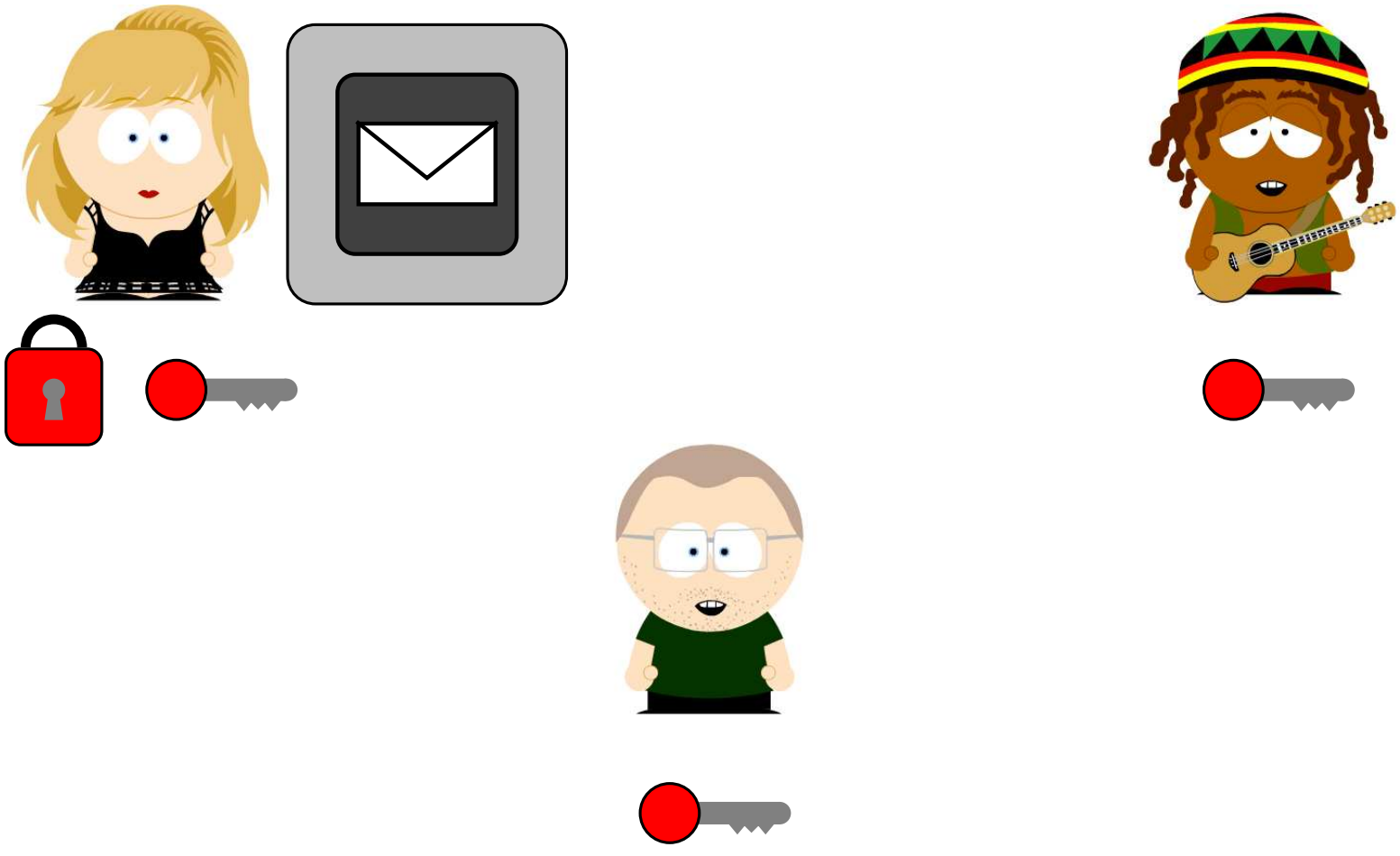




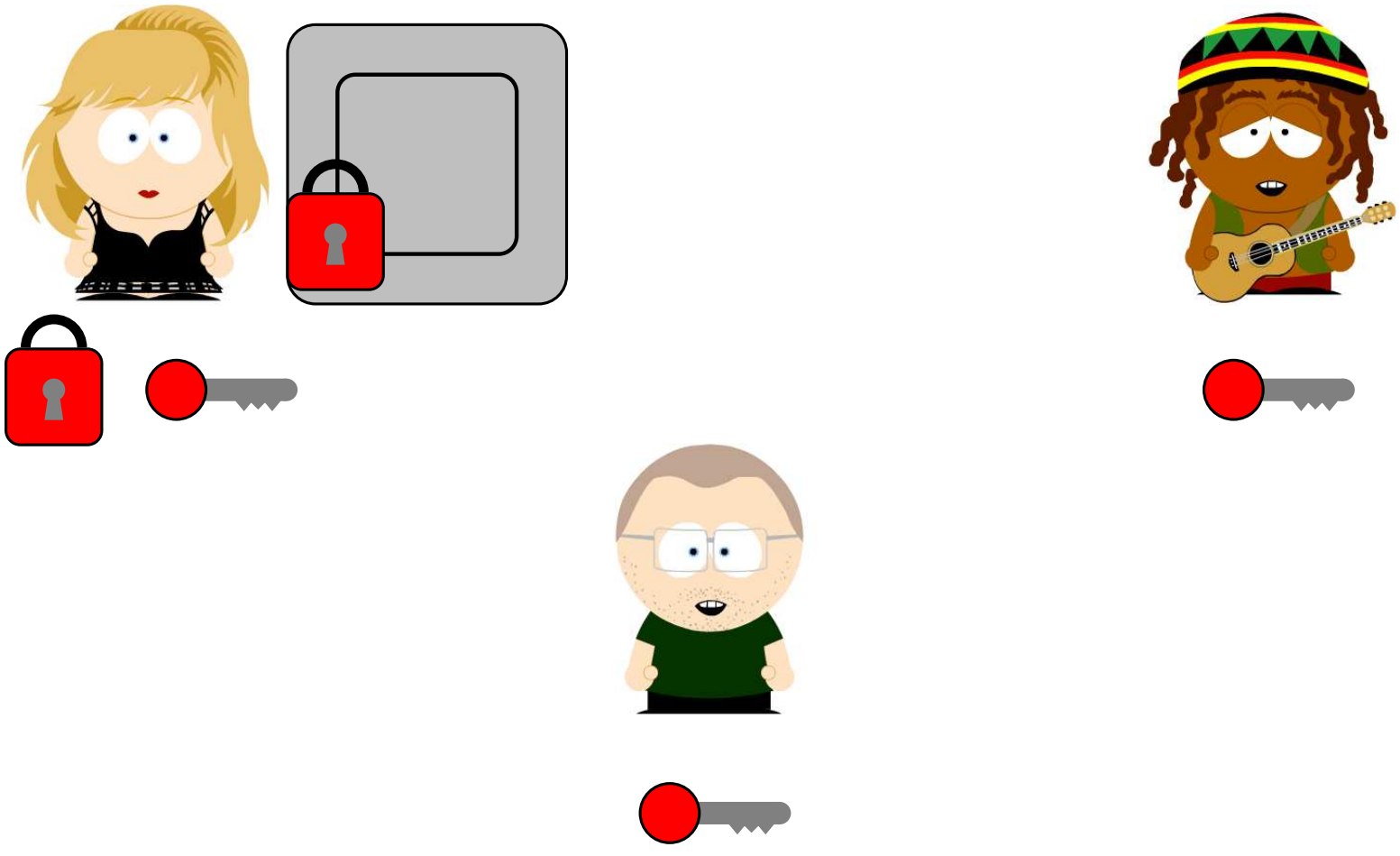
Cryptographique à clé publique : 2e schéma



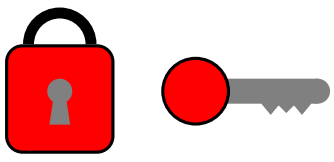
Cryptographique à clé publique : 2e schéma

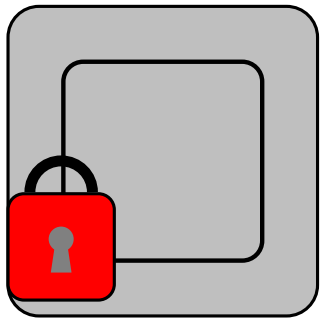


Cryptographique à clé publique : 2e schéma

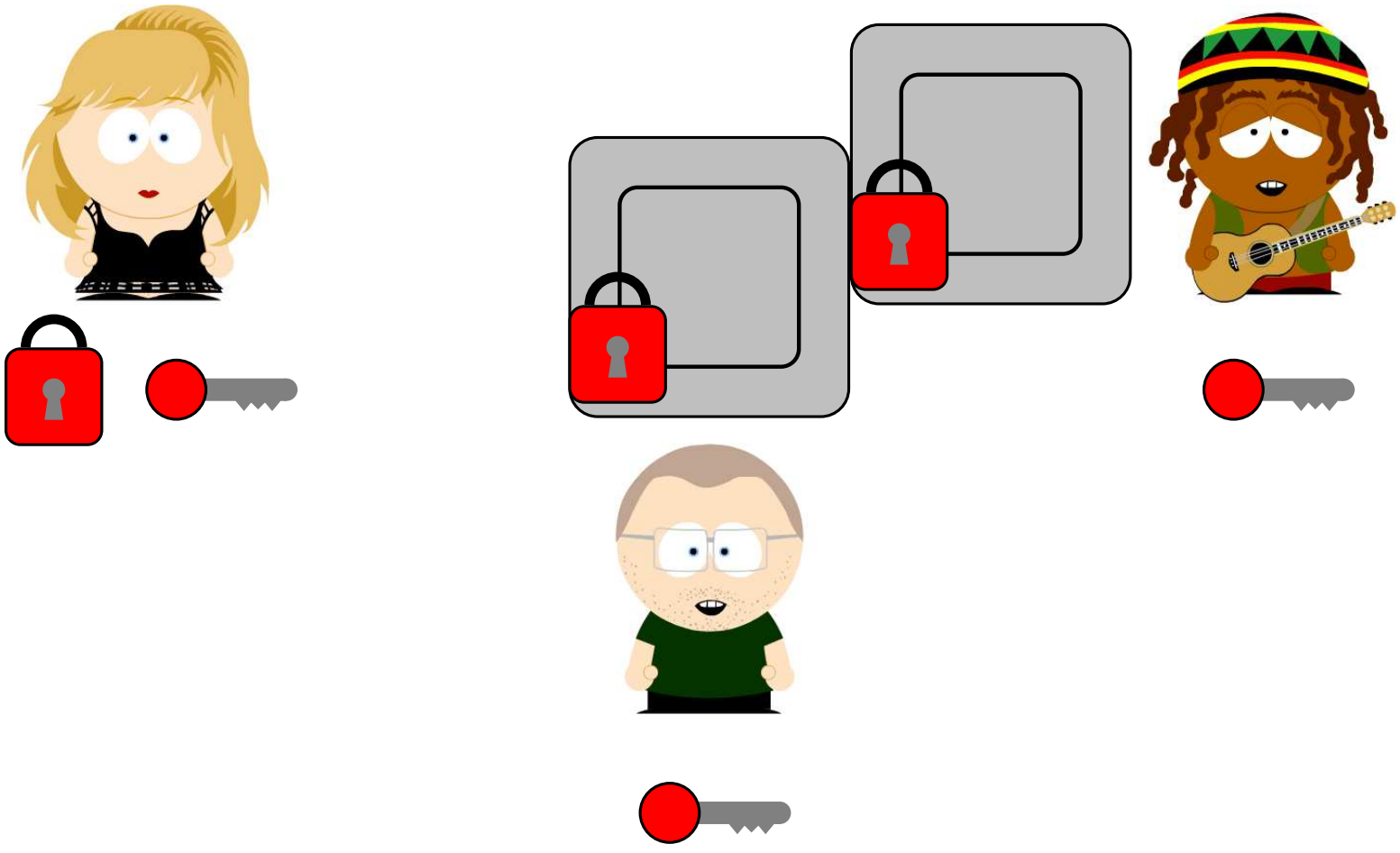


Cryptographique à clé publique : 2e schéma

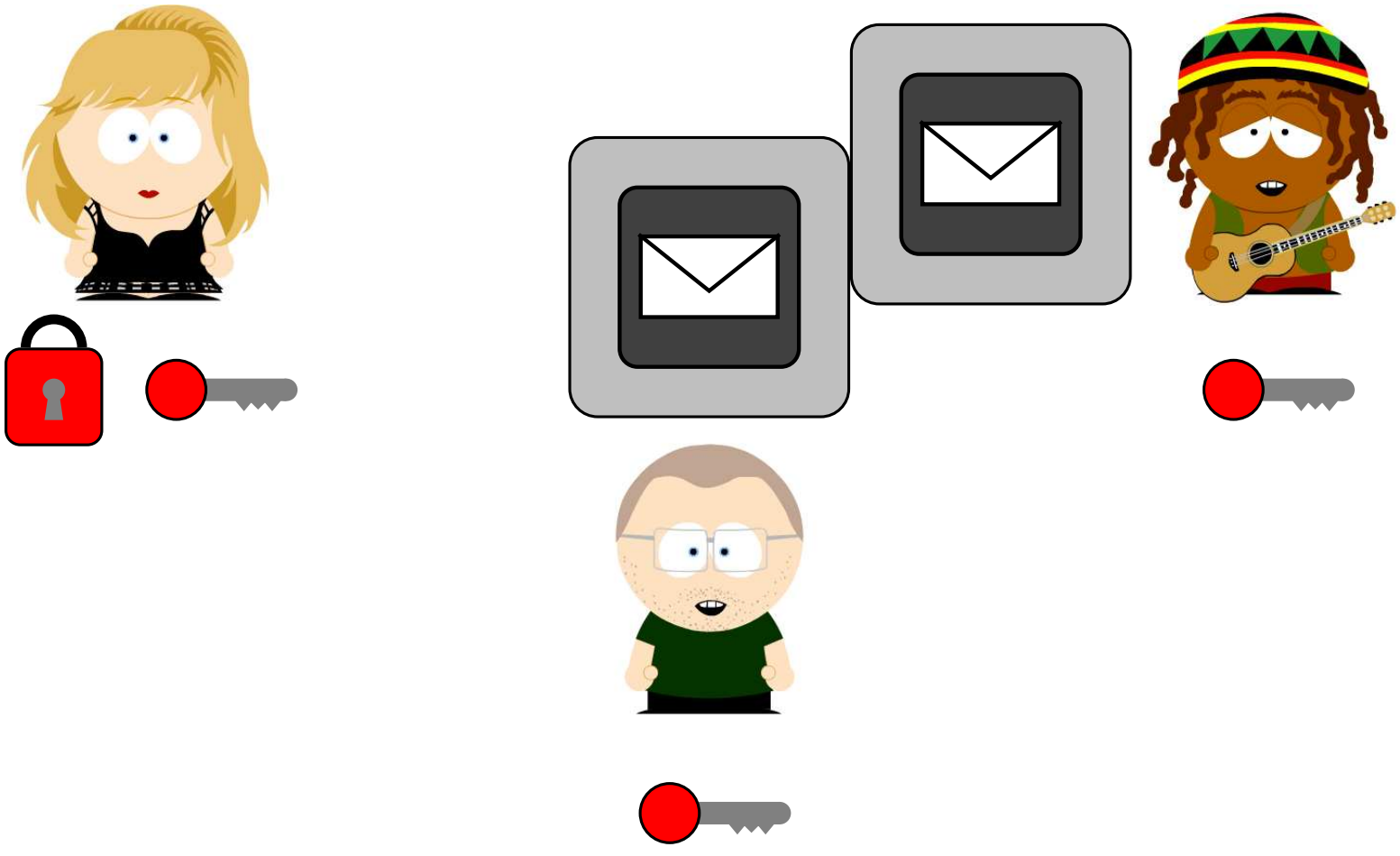




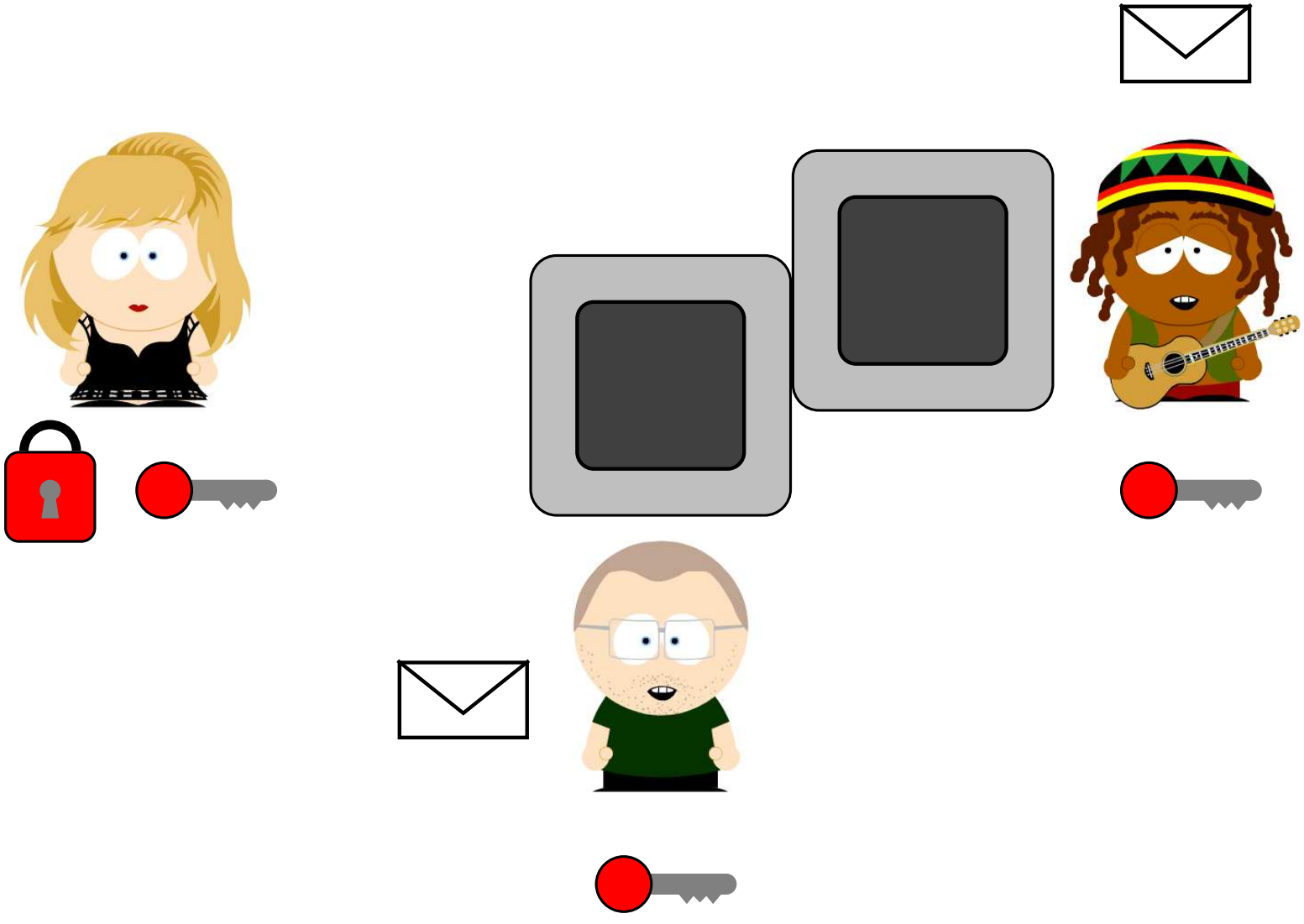
Cryptographique à clé publique : 2e schéma



Cryptographique à clé publique : 2e schéma



Cryptographique à clé publique : 2e 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.

$\rightsquigarrow$ 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.

- $\rightsquigarrow$ facile voulant dire appartenant à la classe P
- $\rightsquigarrow$ 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.

- $\rightsquigarrow$ facile voulant dire appartenant à la classe P
- $\rightsquigarrow$ 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.

$\rightsquigarrow$ facile voulant dire appartenant à la classe P

$\rightsquigarrow$ 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 \$.

$\rightsquigarrow$ 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.

- $\rightsquigarrow$ facile voulant dire appartenant à la classe P
- $\rightsquigarrow$ 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 $.

- $\rightsquigarrow$ on ne sait pas si de telles fonctions existent
- $\rightsquigarrow$ 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 $M^e \mod n$

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 $M^e \mod n$

- 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 $M^e \mod n$

- 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 $M^e \mod n$

- Question : Où est la fonction à sens unique ?

- Réponse : C'est la fonction exponentiation modulaire :

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & M & \mapsto & M^e \end{array}$$

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 $M^e \mod n$

- Question : Où est la fonction à sens unique ?

- Réponse : C'est la fonction exponentiation modulaire :

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & M & \mapsto & M^e \end{array}$$

On *suppose* que inverser f revient a 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 $M^e \mod n$

- Question : Où est la fonction à sens unique ?

- Réponse : C'est la fonction exponentiation modulaire :

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & M & \mapsto & M^e \end{array}$$

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

$\rightsquigarrow$ 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.

$\rightsquigarrow$ 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.

$\rightsquigarrow$ 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.

$\rightsquigarrow$ 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 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 :

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

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

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 $e = 65537$

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & M & \mapsto & C = M^e \end{array}$$

Fonction à sens unique à brèche secrète : retour à RSA

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

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & M & \mapsto & C = M^e \end{array}$$

- Question : Comment inverser f ?

Fonction à sens unique à brèche secrète : retour à RSA

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

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & M & \mapsto & C = M^e \end{array}$$

- 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 $e = 65537$

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & M & \mapsto & C = M^e \end{array}$$

- Question : Comment inverser f ?

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

Fonction à sens unique à brèche secrète : retour à RSA

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

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & M & \mapsto & C = M^e \end{array}$$

- Question : Comment inverser f ?

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

$$C^d =$$

Fonction à sens unique à brèche secrète : retour à RSA

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

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & M & \mapsto & C = M^e \end{array}$$

- Question : Comment inverser f ?

- Réponse :
  - On calcule $\phi(n) = (p-1) \times (q-1)$
  - Par *Bezout*, on calcule d tel que $ed \equiv 1 \mod \phi(n)$
  - 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 $e = 65537$

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & M & \mapsto & C = M^e \end{array}$$

- Question : Comment inverser f ?

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

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

Fonction à sens unique à brèche secrète : retour à RSA

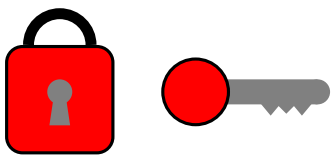
- On a $n = p \times q$ et $e = 3$ ou $e = 65537$

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & M & \mapsto & C = M^e \end{array}$$

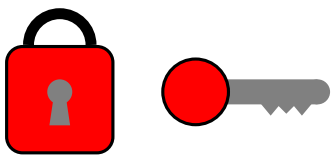
- Question : Comment inverser f ?

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

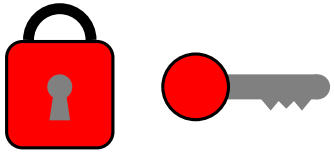
$$C^d = (M^e)^d = M^{ed+k\phi(n)} = M \mod n$$



(p, q)

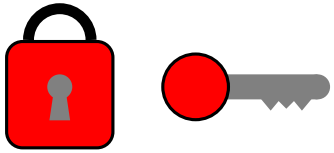


(p, q) ; $n = p \times q$



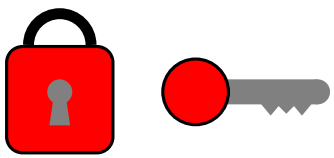
n

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



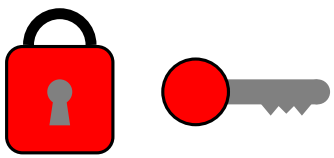
n

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



n
e

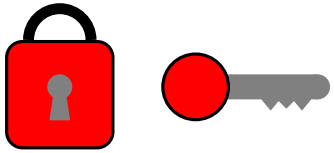
(p, q) ; $n = p \times q$; $\phi(n) = (p-1) \times (q-1)$; e ; $ed \equiv 1 \mod n$



n
e

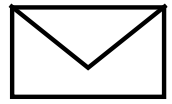
d

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

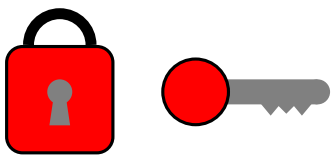


n
e

d

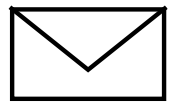


(p, q) ; $n = p \times q$; $\phi(n) = (p-1) \times (q-1)$; e ; $ed \equiv 1 \mod n$

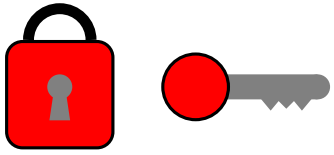


n
e

d



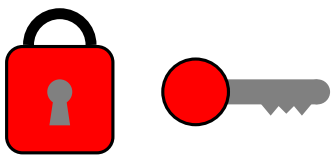
(p, q) ; $n = p \times q$; $\phi(n) = (p-1) \times (q-1)$; e ; $ed \equiv 1 \mod n$



n
e

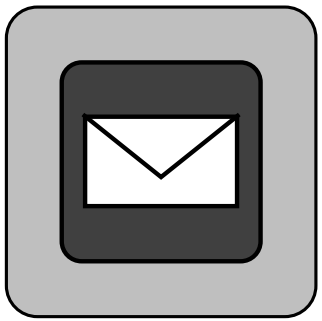
d

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

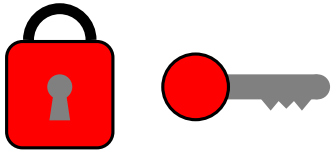


n
e

d

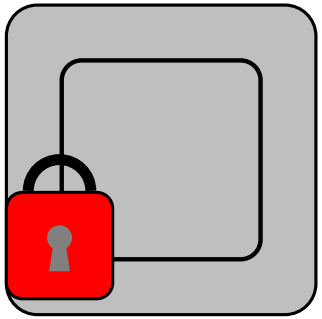


(p, q) ; $n = p \times q$; $\phi(n) = (p-1) \times (q-1)$; e ; $ed \equiv 1 \mod n$

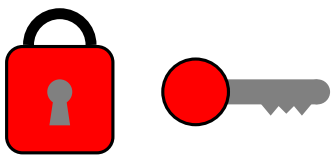


n
e

d

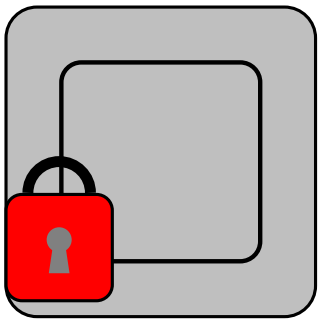


(p, q) ; $n = p \times q$; $\phi(n) = (p-1) \times (q-1)$; e ; $ed \equiv 1 \mod n$

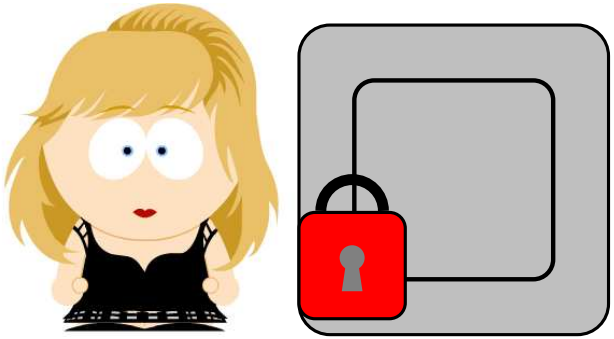


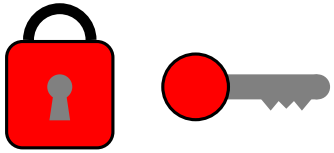
n
e

d



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

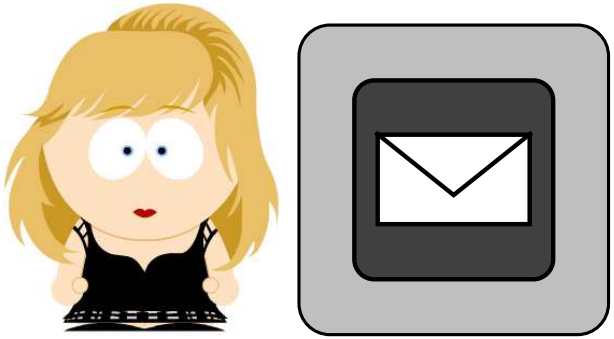


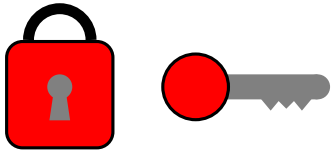


n
e

d

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

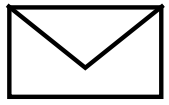


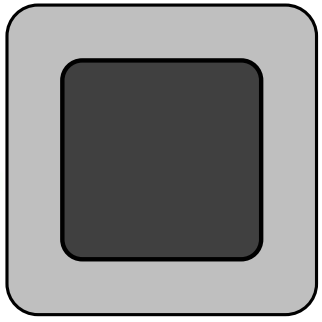


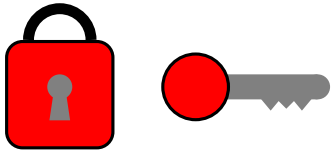
n
e

d

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







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.

$\rightsquigarrow$ 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.

$\rightsquigarrow$ L'image d'une fonction à sens unique ou de hachage est souvent appelée condensat.

- Fait : Le condensat *caractérise* la donnée mais ne peux la reconstuire.

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

$\rightsquigarrow$ L'image d'une fonction à sens unique ou de hachage est souvent appelée condensat.

- Fait : Le condensat *caractérise* la donnée mais ne peux la reconstuire.

- Utilisation :

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

$\rightsquigarrow$ L'image d'une fonction à sens unique ou de hachage est souvent appelée condensat.

- Fait : Le condensat *caractérise* la donnée mais ne peux la reconstuire.

- Utilisation :
  - somme de contrôle

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

$\rightsquigarrow$ L'image d'une fonction à sens unique ou de hachage est souvent appelée condensat.

- Fait : Le condensat *caractérise* la donnée mais ne peux la reconstuire.

- 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.

$\rightsquigarrow$ L'image d'une fonction à sens unique ou de hachage est souvent appelée condensat.

- Fait : Le condensat *caractérise* la donnée mais ne peux la reconstuire.

- 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.

$\rightsquigarrow$ L'image d'une fonction à sens unique ou de hachage est souvent appelée condensat.

- Fait : Le condensat *caractérise* la donnée mais ne peux la reconstuire.

- 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 pass

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

Le sel peut être un haché obtenu à partir :

Fonction de hachage et mot de pass

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

Le sel peut être un haché obtenu à partir :

- du nom d'utilisateur,

Fonction de hachage et mot de pass

Afin d'augmenter la sécurité, on ne hache pas directement un mot de pass. En effet, on hache le mot de pass augmenter 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 pass

Afin d'augmenter la sécurité, on ne hache pas directement un mot de pass. En effet, on hache le mot de pass augmenter 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 pass

Afin d'augmenter la sécurité, on ne hache pas directement un mot de pass. En effet, on hache le mot de pass augmenter 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.

$\rightsquigarrow$ Grâce au sel, si deux utilisateurs ont le même mot de pass, les hachés seront différents.

Fonction de hachage et mot de pass

Afin d'augmenter la sécurité, on ne hache pas directement un mot de pass. En effet, on hache le mot de pass augmenter 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.

$\rightsquigarrow$ Grâce au sel, si deux utilisateurs ont le même mot de pass, les hachés seront différents.

$\rightsquigarrow$ L'attaque par dictionnaire ou table arc-en-ciel devient pratiquement impossible.