Cours sécurité informatique
(option L3)

Introduction

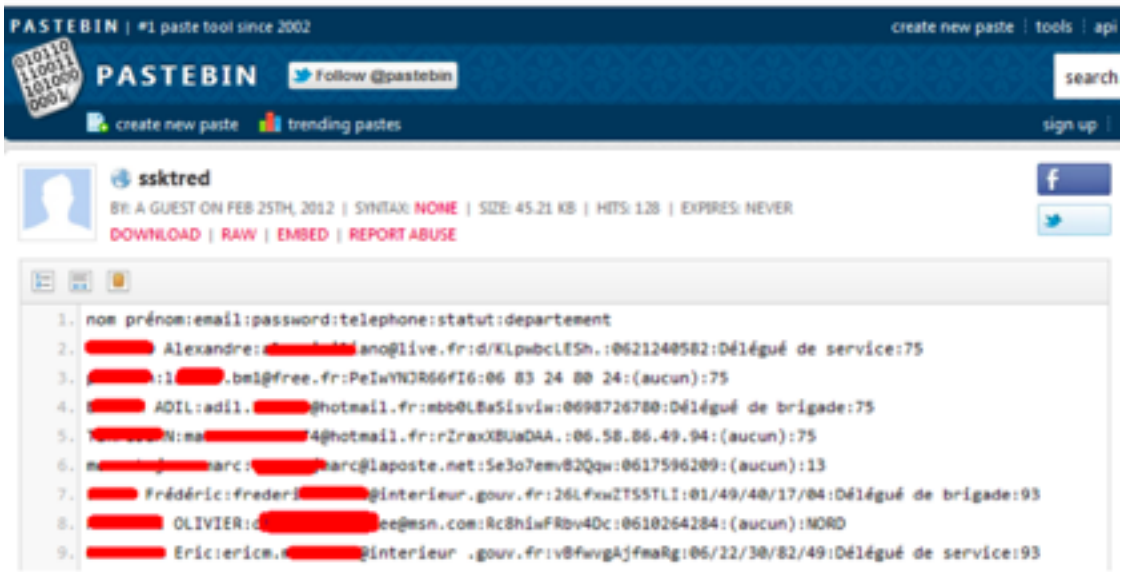
Sécurité (Larousse):
Situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger, à aucun risque, en particulier d'agression physique, d'accidents, de vol, de détérioration

Risque (Larousse):
Possibilité, probabilité d'un fait, d'un événement considéré comme un mal ou un dommage : *Les risques de guerre augmentent.*
Danger, inconvénient plus ou moins probable auquel on est exposé : *Courir le risque d'un échec. Un pilote qui prend trop de risques.*

Cyberattaques: Défiguration de site

Cyberattaques: spam fishing

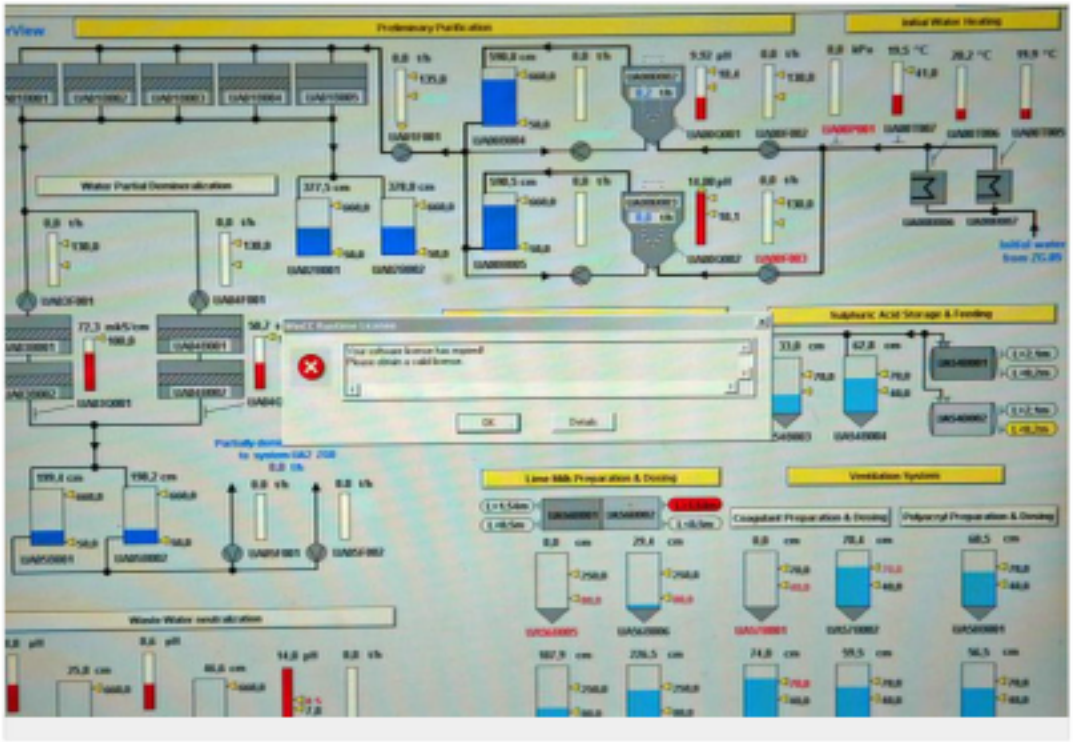
Cyberattaques: fuite de données



Cyberattaques: Déni de service

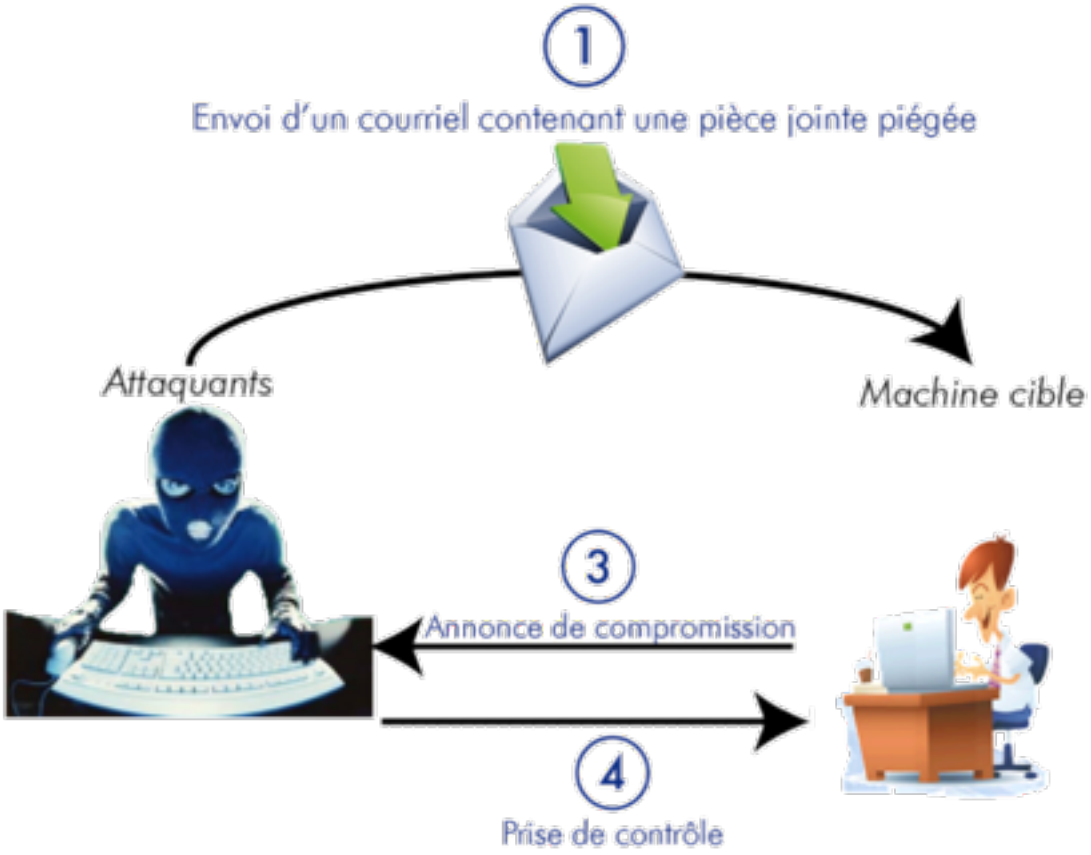
Cyberattaques: Virus

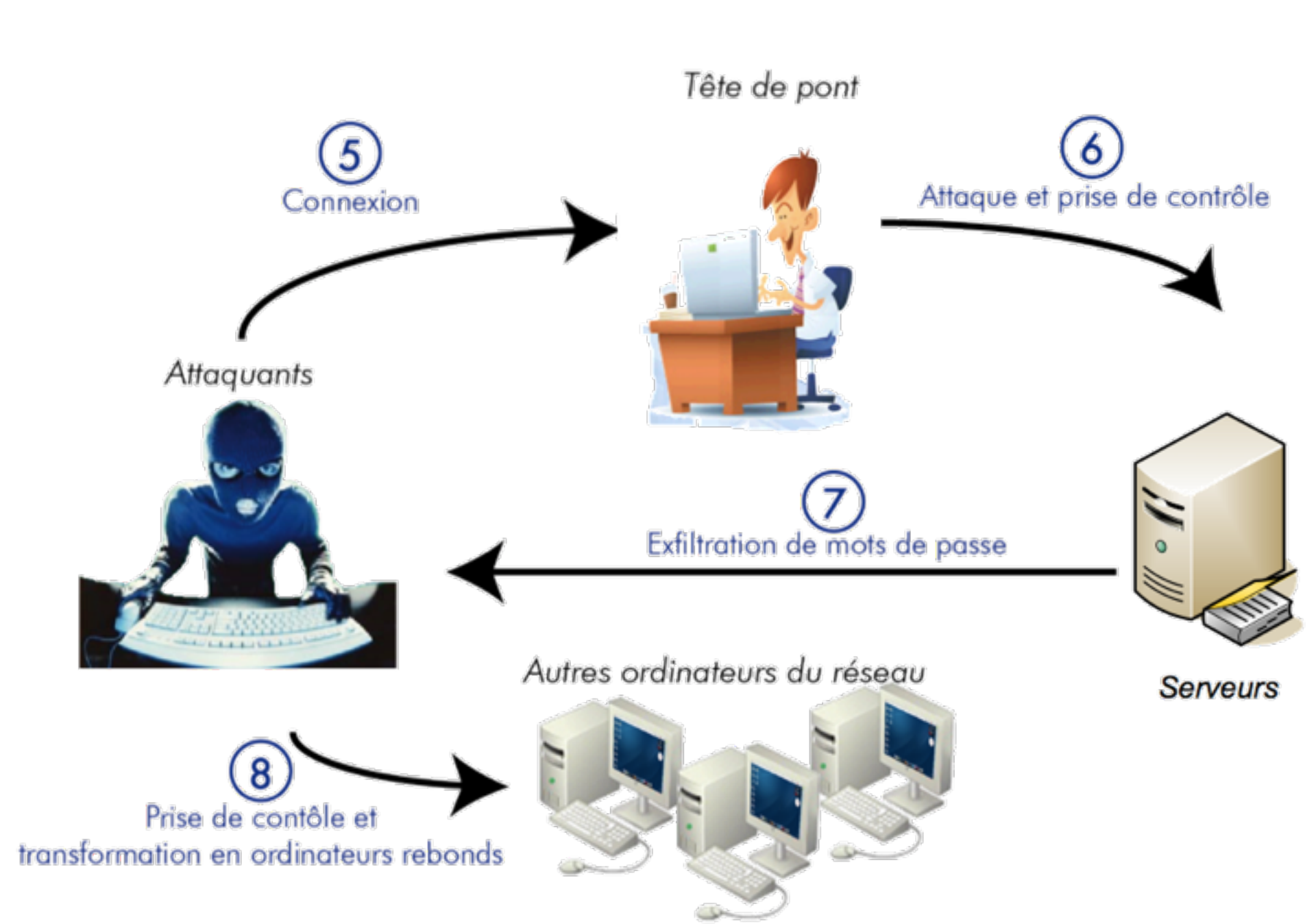
Iran's Bushehr nuclear power plant in Bushehr Port

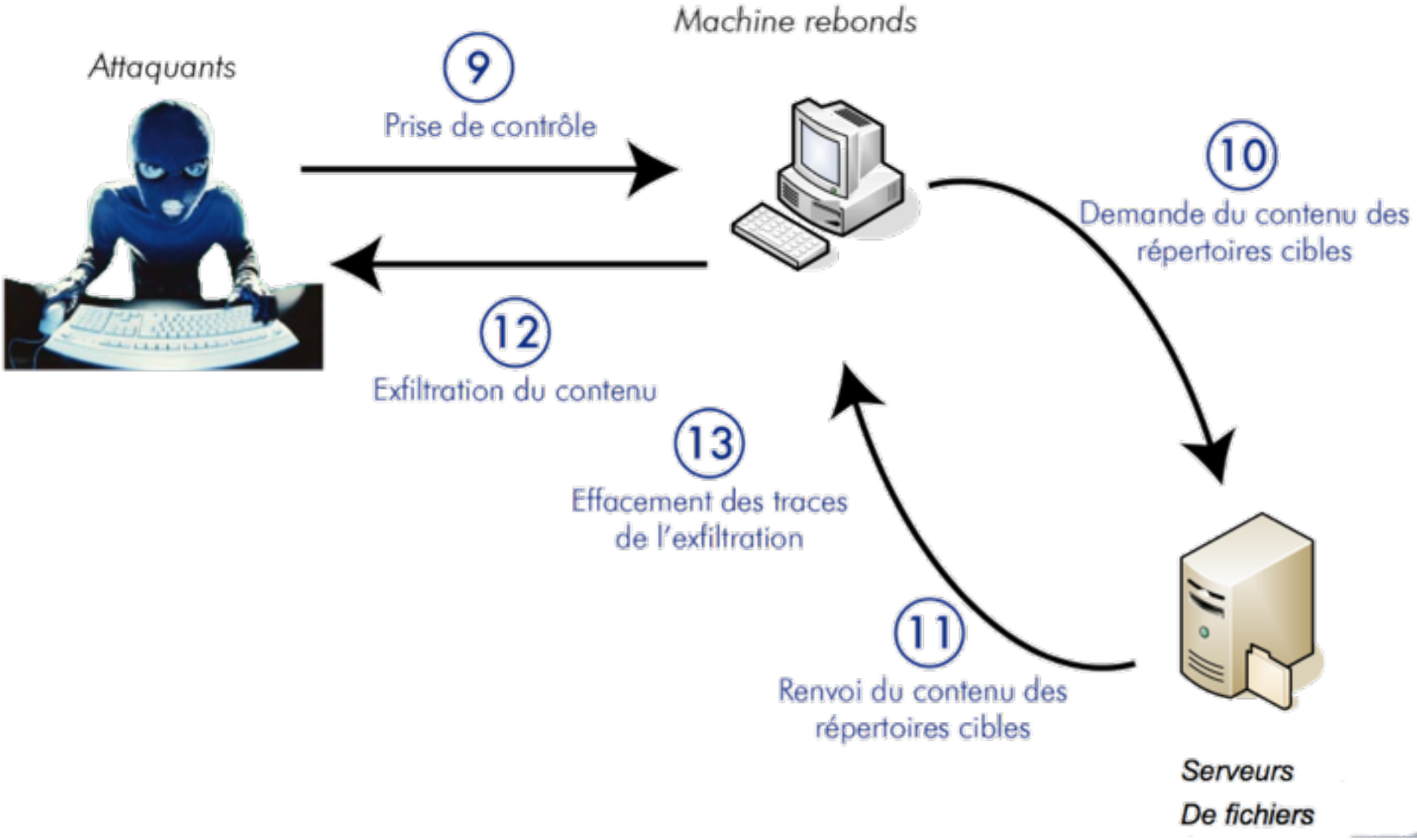


An error is seen on a computer screen of Bushehr nuclear power plant's map in the Bushehr Port on the Persian Gulf, 1,000 kms south of Tehran, Iran on February 25, 2009. Iranian officials said the long-awaited power plant was expected to become operational last fall but its construction was plagued by several setbacks, including difficulties in procuring its remaining equipment and the necessary uranium fuel. (UPI Photo/Mohammad Kheirkhah)

Attaque ciblée (Advanced Persistant Threat)




Tête de pont
5
Connexion
6
Attaque et prise de contrôle
Attaquants
7
Exfiltration de mots de passe
Serveurs
Autres ordinateurs du réseau
8
Prise de contôle et
transformation en ordinateurs rebonds


Attaquants
Machine rebonds
9
Prise de contrôle
10
Demande du contenu des répertoires cibles
12
Exfiltration du contenu
13
Effacement des traces de l'exfiltration
11
Renvoi du contenu des répertoires cibles
Serveurs De fichiers

Et …

- Problème de la protection de la vie privée et des données personnelles…
- Snowden

- En plus:
  - ubiquité
  - fonctions critiques
  - …

Vie privée


EMPLOI

Recalés à l'embauche pour leurs profils Facebook

20% des recruteurs du secteur informatique auraient déjà écarté un candidat à l'embauche sur la base d'informations récoltées sur les réseaux sociaux.

ouest france

Chantage à la webcam. Des victimes dévastées par la honte

Des escrocs, souvent basés en Côte d'Ivoire, poussent des internautes à se livrer à des jeux érotiques devant leur webcam, avant de les faire chanter. L'arnaque, dont les auteurs sont quasi impossibles à identifier, se répand à vitesse grand V. Elle a déjà poussé deux lycéens, dont un Brestois, au suicide.


L'INFORMATICIEN

Le cyberharcèlement, fléau des enfants à l'école

Les parents de Marion, suicidée à 13 ans, portent plainte contre le collège

SOCIÉTÉ | Mis à jour le 28/06/2013 à 16:12

La famille dénonce l'inaction de plusieurs membres de l'équipe du collège face au harcèlement dont aurait été victime la jeune fille.

Que s'est-il passé dans l'enceinte du collège Jean-Monnet à Briis-sous-Forges dans l'Essonne entre Marion et d'autres élèves? Quatre mois après le suicide de cette collégienne de 13 ans qui avait laissé une lettre évoquant des faits de harcèlement, la famille a décidé de réagir. Selon nos informations, elle a déposé plainte le 13 juin dernier pour «violences, menaces de mort, provocation au suicide, homicide involontaire et omission de porter secours». Une action en justice qui, sans donner de noms, vise les auteurs présumés de ces pressions mais aussi des membres de l'équipe du collège.

Selon les parents de Marion, leur fille était devenue la tête de Turc de certains dans ce collège plutôt bien fréquenté, et les responsables de l'établissement ne pouvaient l'ignorer. «Nous avions demandé à plusieurs reprises que notre fille change de classe», explique Nora, la mère de Marion, chef de projet marketing exerçant à la Défense.

Menaces de mort via Facebook

Décrite comme bonne élève, Marion aurait été prise pour cible, raconte sa mère, car elle était différente. Dans sa classe, décrite comme difficile selon la plainte, Marion, elle, réclamait le silence. Audace suprême: la jeune fille ne cédait pas aux codes vestimentaires. Aux sacs dernier

Accusations…

Le Point.fr

NIORT - En garde à vue parce que son voisin utilisait son Wi-Fi

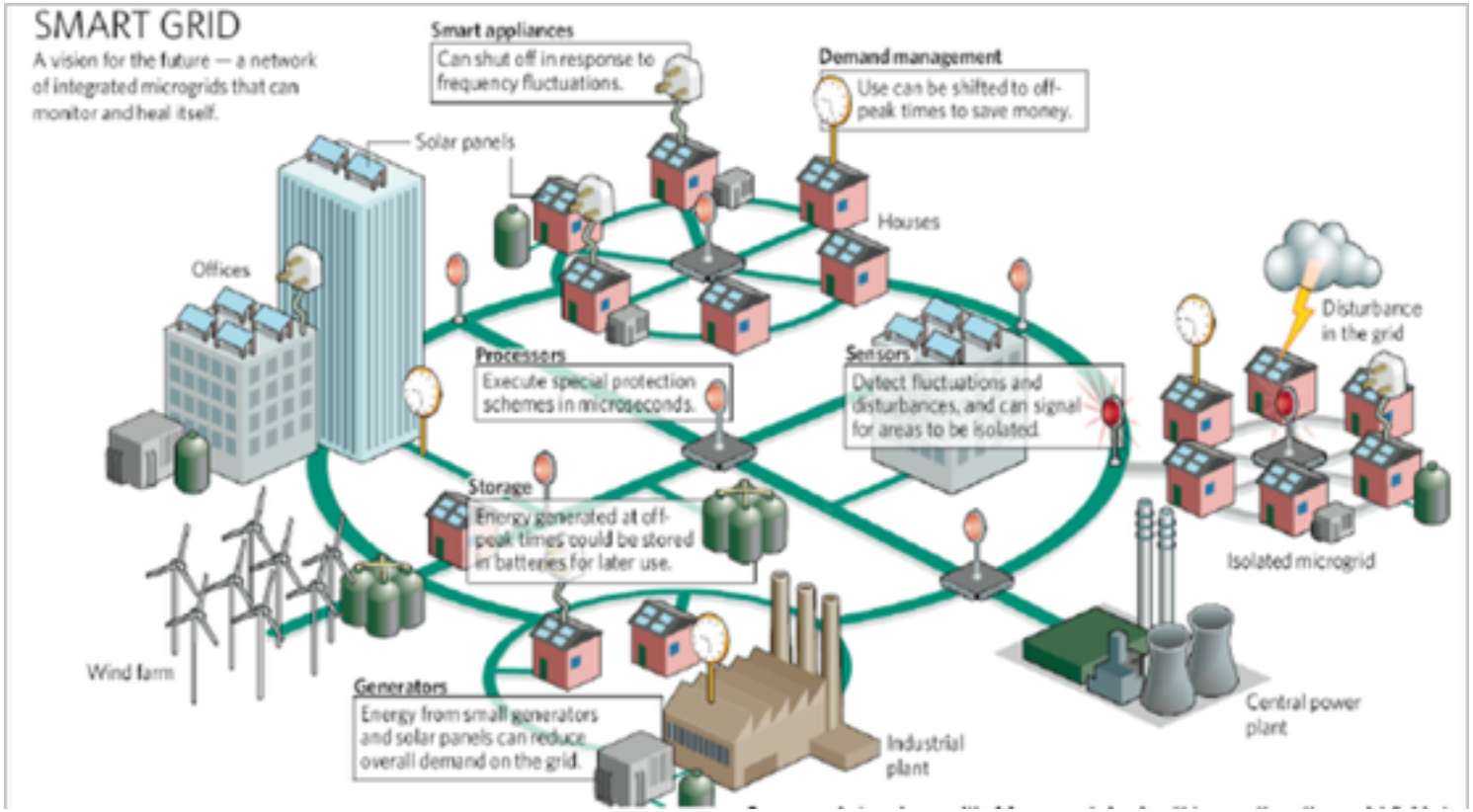
Ce virus qui télécharge des images pédophiles

WEB | Mis à jour le 10/11/2009 à 21:35

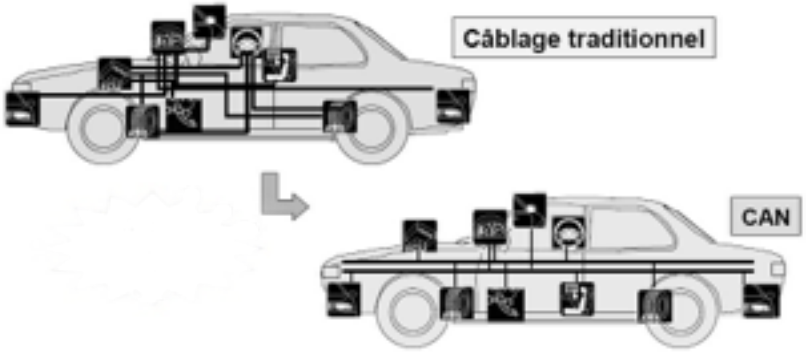
Les pirates utilisent les ordinateurs de leurs victimes pour stocker des images à caractère pédophile. *Crédits photo : AFP*

A cause de ce programme informatique, plusieurs internautes américains sont accusés à tort d'avoir téléchargé des contenus pédophiles. Prouver leur innocence relève du calvaire.

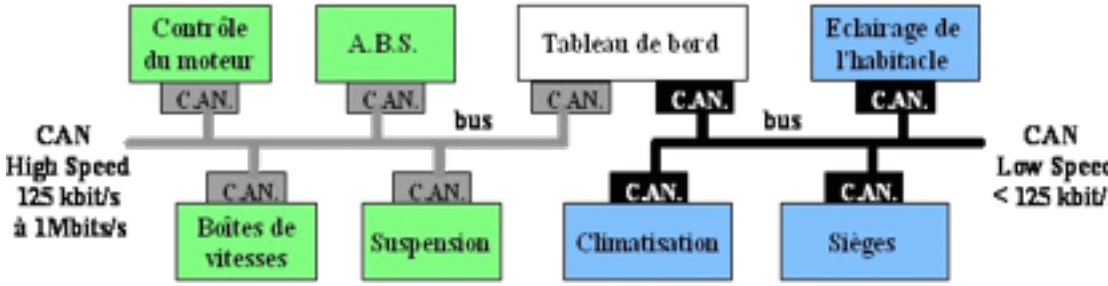
Smart grids


SMART GRID
A vision for the future — a network of integrated microgrids that can monitor and heal itself.
Smart appliances
Can shut off in response to frequency fluctuations.
Demand management
Use can be shifted to off-peak times to save money.
Solar panels
Houses
Offices
Disturbance in the grid
Processors
Execute special protection schemes in microseconds.
Sensors
Detect fluctuations and disturbances, and can signal for areas to be isolated.
Storage
Energy generated at off-peak times could be stored in batteries for later use.
Isolated microgrid
Wind farm
Generators
Energy from small generators and solar panels can reduce overall demand on the grid.
Central power plant
Industrial plant

Partout…



RESEAU C.A.N. AUTOMOBILE



Des agences de sécurité

http://www.ssi.gouv.fr/

cert:-fr: http://www.cert.ssi.gouv.fr/

http://www.cert.org/

Objets connectés

- Il existe un moteur de recherche spécialisé dans les équipements accessibles depuis internet (routeurs, caméra, systèmes industriels,
- Ce moteur propose des « exploits » de hacker

Des objectifs

Confidentialité: seules les entités autorisées peuvent accéder à l'information ou au service.

Pour la communication:

- l'émetteur *chiffre* le message
- le récepteur *déchiffre* le message

Intégrité: l'information ou le service n'est modifiable que par les entités autorisées toute modification non légitime est détectable.

Disponibilité: l'information ou le service doit être disponible (résilience, tolérance aux défaillances aux attaques)

Authenticité: l'information est authentique (ex dvd piraté)

Mais aussi..

Imputabilité: On peut imputer à une entité un fait.

Auditabilité: la conformité de l'information ou du service peut être vérifiée

Non répudiation: l'impossibilité de nier être l'auteur d'un acte ou d'une information

Authenticité: l'information est authentique (ex dvd piraté)

…

Sécurité informatique

- La sécurité n'est pas un service
- On ne peut pas garantir « après coup » la sécurité:
  - La sécurité doit être prise en compte à tous les niveaux
- Dans un système découpé en couches et en modules, les différentes vulnérabilités se cumulent plus qu'elles ne s'annulent les unes les autres

Sécurité

- La sécurité est un état d'esprit
- On peut raisonner suivant 5 grands axes
  - prévenir : éviter l'apparition des vulnérabilités
  - bloquer: empêcher un problème de parvenir jusqu'aux éléments sensibles
  - limiter: réduire les conséquences d'une attaque
  - détecter: repérer une attaque
  - réparer: disposer de moyens permettant de remettre en fonctionnement le système

Sécurité informatique

- vulnérabilités présentes dans tous les domaines…
  - ★ hardware
  - ★ développement du logiciel
  - ★ réseaux
  - ★ …
- elles peuvent provenir
  - ★ de maladresses (bugs, complexité, conception, implémentation, configuration …)
  - ★ actions volontaires (détournements, intrusion, codes tiers sans contrôle)

Sécurité …

- Des mauvaises pratiques sont sources de nombreuses vulnérabilités
  - Exemple

```
#include <stdio.h>
#include <stdlib.h>
void set(int s,int v) { *(&s-s)=v; }
void bad() { printf("Bad things happen!\n"); exit(0); }
int main(void) {
set(1,(int)bad); printf("Hello world\n"); return 0;
}
```

Dans ce cours…

- Côté pratique: java
  - sécurité au niveau langage
    - Architecture de la sécurité: Security provider
    - Cryptographie
    - Infrastructure des clés publiques
    - Authentification
    - Communication sécurisée (SSL)

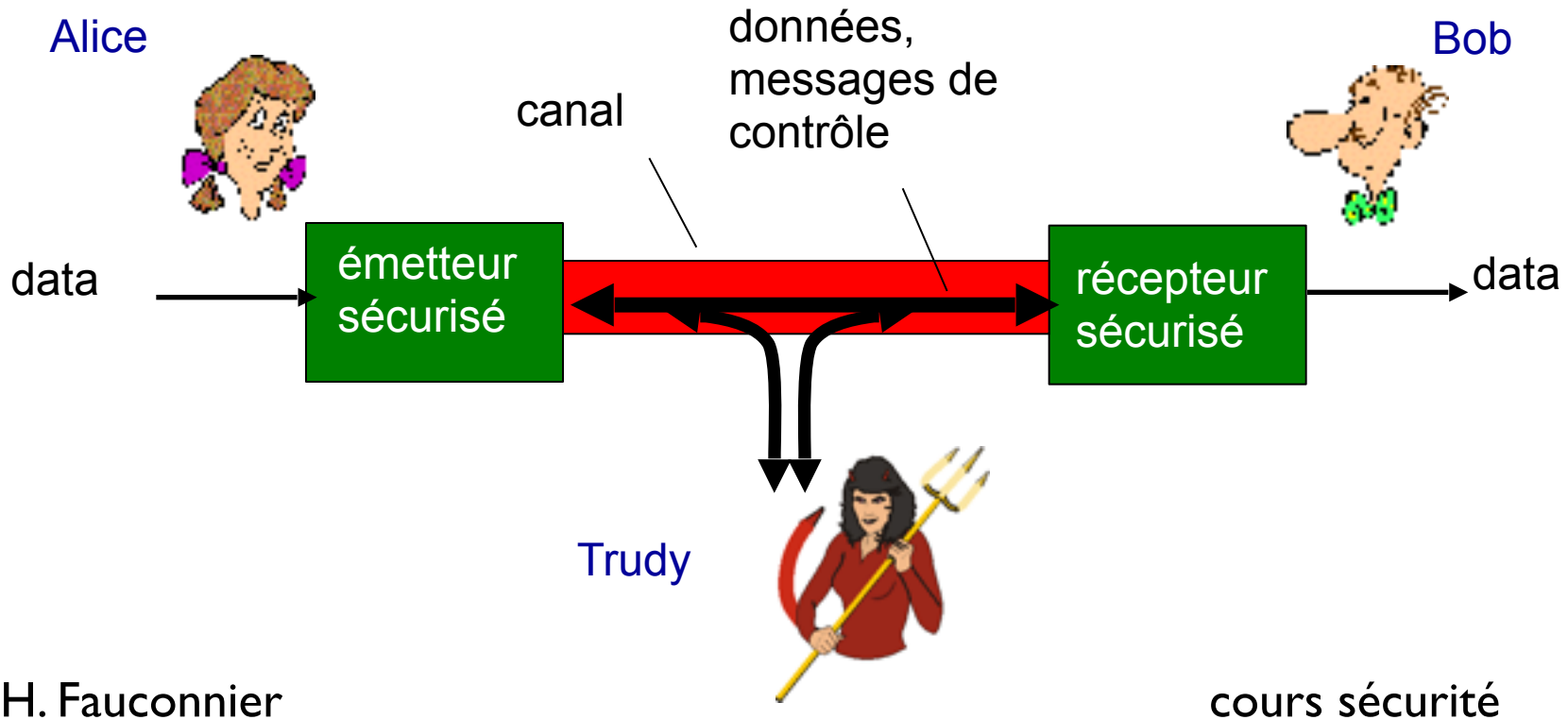
Dans ce cours…

- Codes (intégrité-confidentialité)
  - codes correcteurs
  - Cryptographie
    - code symétriques (DES, AES)
    - codes à clés publiques (RSA …)
- Intégrité et authentification
  - hachage
  - MAC
  - signatures digitales
  - certification de clés
  - end-to-end authentification
- Application PGP email sécurisé
- TCP sécurisé SSL, Wireless
- Nombres pseudo-aléatoires

Cryptographie

Modèle de base pour la communication

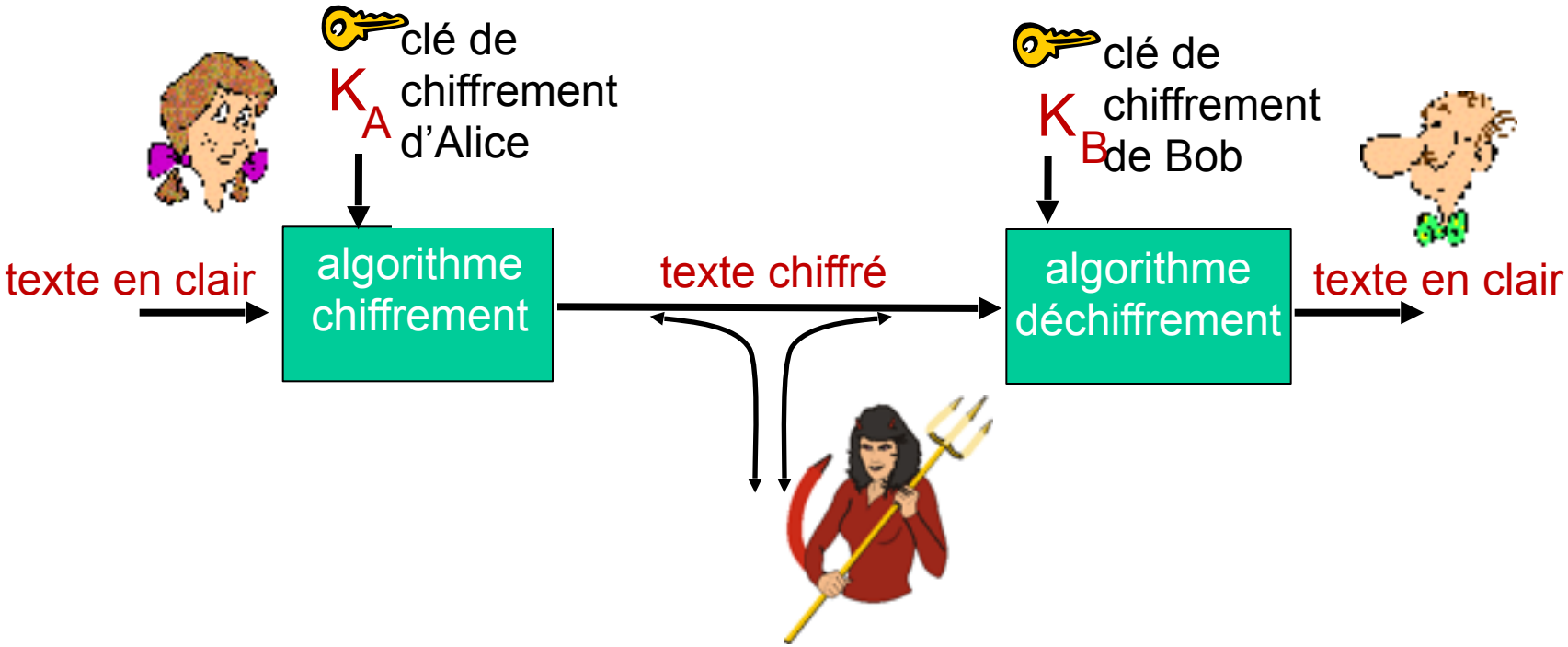
- Bob, Alice veulent communiquer se façon sûre
- Trudy (l'intruse) peut intercepter, supprimer ajouter des messages



Que peut faire un bad guy (réseau)

- *espionner (eavesdrop):* intercepter des messages
- *insérer* des messages
- *imposture (impersonation):* mettre de fausses adresses sources dans les paquets (parodie - spoof)
- *pirater (hijacking) :* prendre la place de l'émetteur ou du récepteur
- *dénis de service:* empêcher le service de fonctionner (surcharge des ressources)

Le langage de la cryptographie



m message en clair

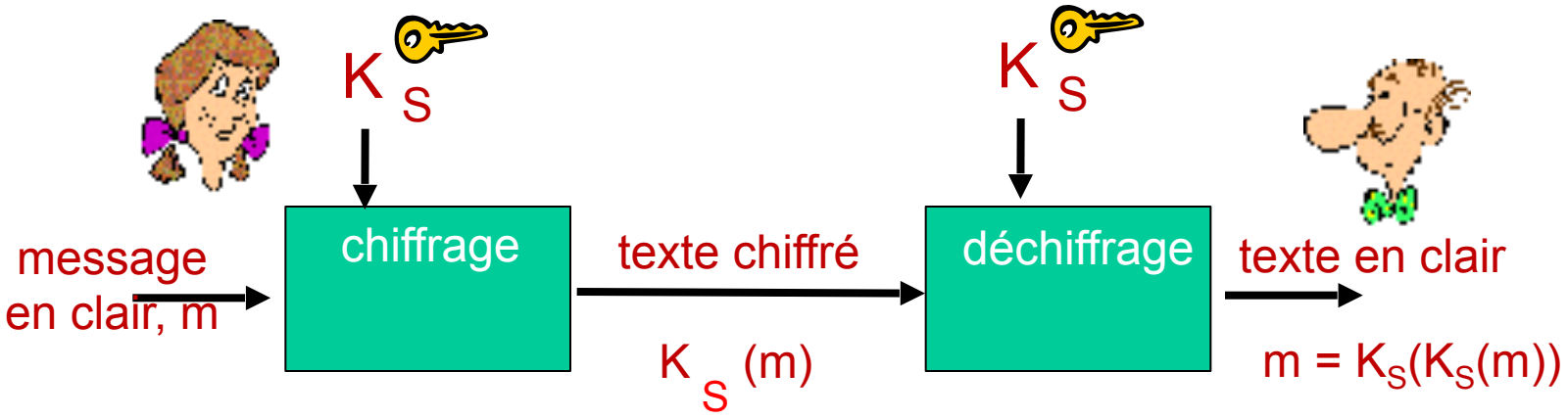
$K_A(m)$ message chiffré avec la clé K_A

$m = K_B(K_A(m))$

Comment casser ce schéma?

- attaque avec le texte chiffré seul: Trudy a le texte chiffré qu'elle peut analyser
- deux approches:
  - force brute: essayer toutes les clés
  - analyse statistique du texte
- attaque avec du texte en clair: Trudy a un texte en clair correspondant a un texte chiffré
- attaque avec du texte en clair choisi: Trudy peut obtenir des textes chiffrés à partir de textes en clair

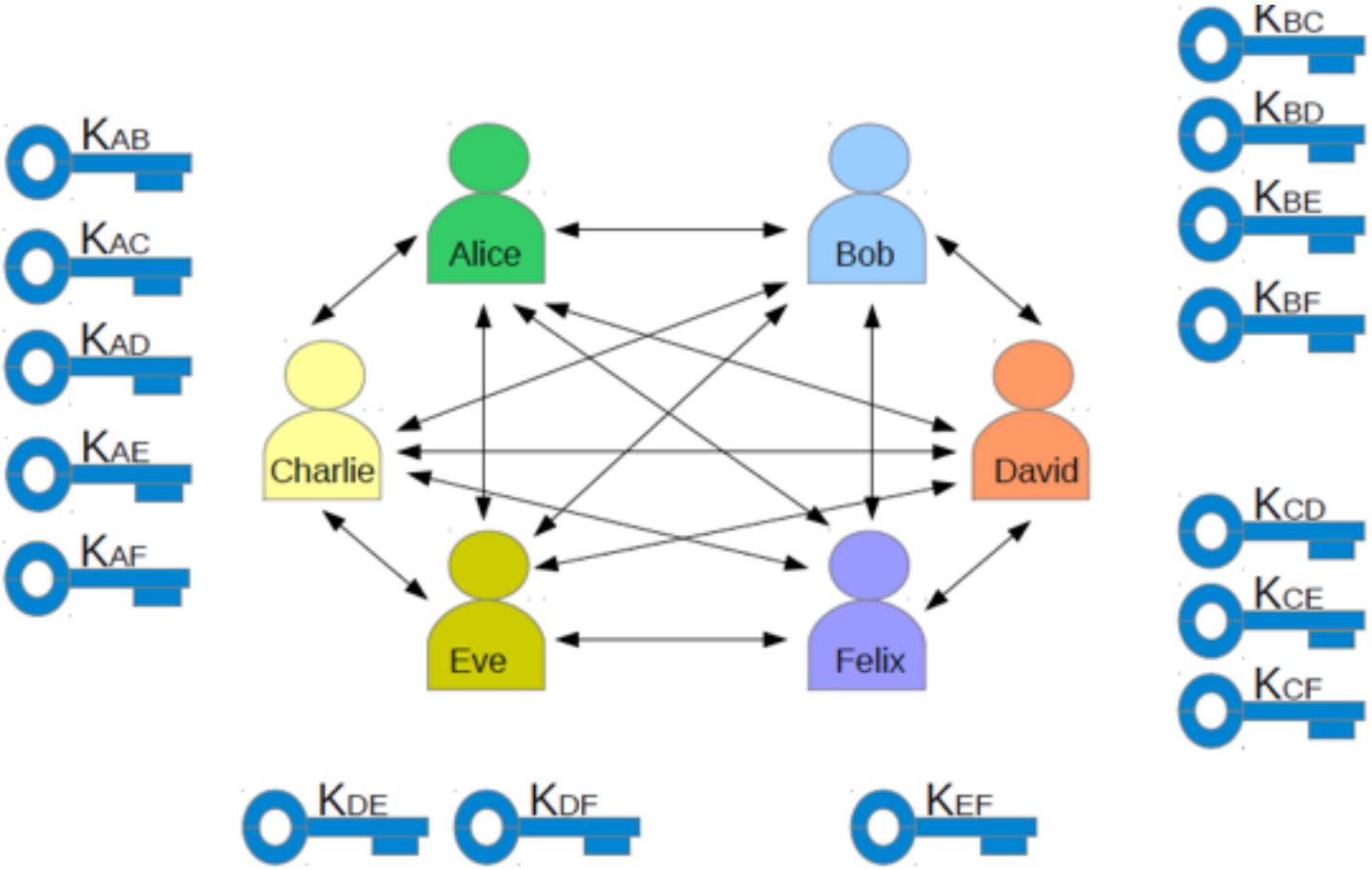
Cryptographie symétrique



cryptographie à clés symétriques: Bob et Alice partagent la même clé (symétrique) K_S

Problème: Comment Bob et Alice obtiennent la clé?

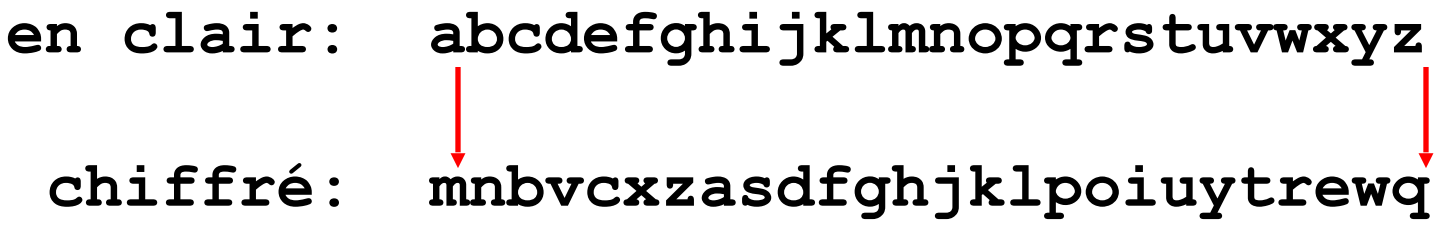
Des clefs:


KAB
KAC
KAD
KAE
KAF
Alice
Bob
Charlie
David
Eve
Felix
KBC
KBD
KBE
KBF
KCD
KCE
KCF
KDE
KDF
KEF

Un chiffrement très simple

chiffrement par substitution:

- chiffrement mono-alphabétique (César): substituer une lettre par une autre



e.g.:

```
en clair: bob. i love you. alice
  chiffré: nkn. s gktc wky. mgsbc
```

Chiffrement clé de codage: application d'un ensemble de 26 lettres dans un ensemble de of 26 lettres

Plus élaboré

- n codes à substitution: $M_1, M_2, \ldots, M_n$
- motifs cycliques:
  - exemple n=4: M_1, M_3, M_4, M_3, M_2; M_1, M_3, M_4, M_3, M_2; ..
- pour chaque nouveau symbole utiliser cycliquement le motif de substitution suivant:
- dog: d de M_1, o de M_3, g de M_4

Clé de chiffrement: n codes à substitution, et un motif de substitution

- la clé n'est pas seulement un motif de n bits

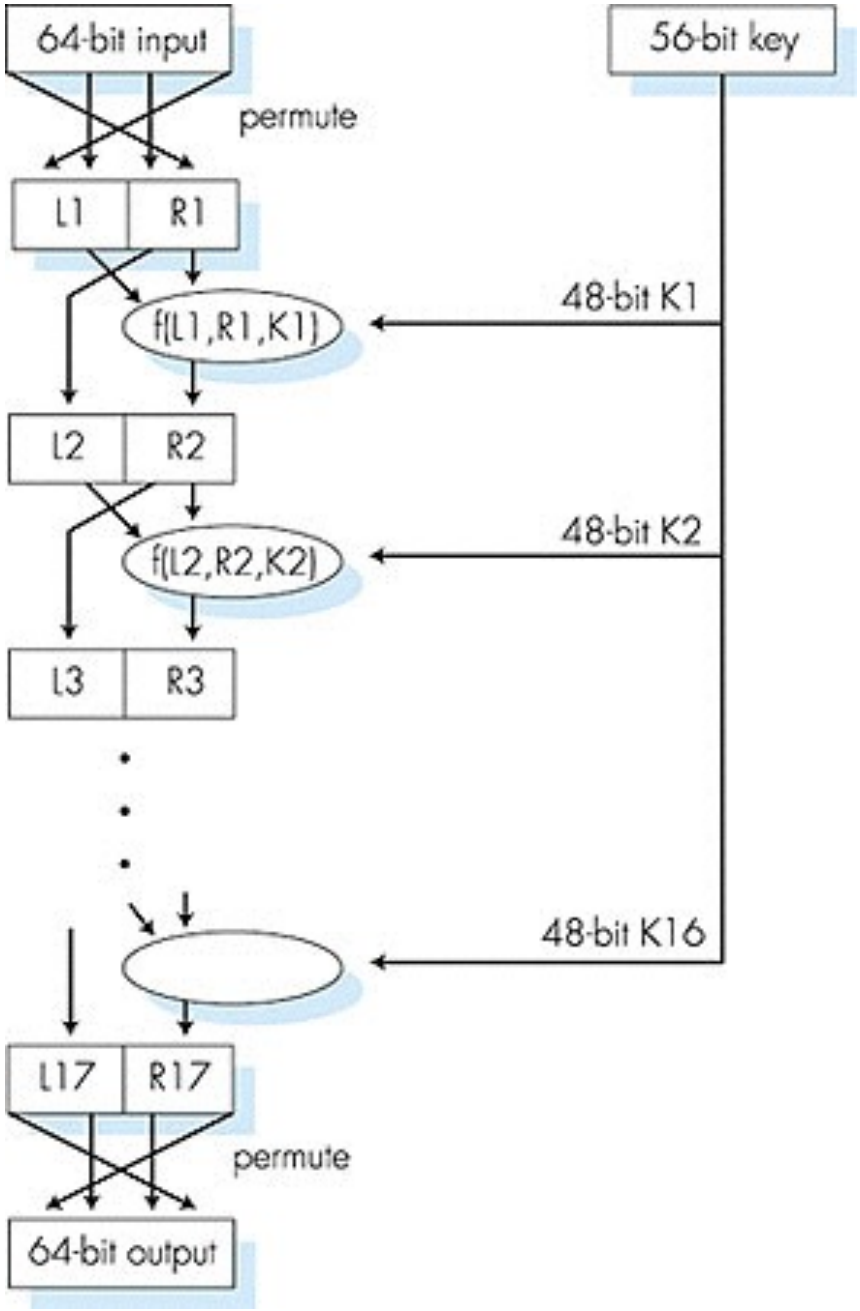
DES: code symétrique

DES:

permutation initiale

16“rondes” identiques d’application de fonctions, chacune utilisant 48 bits différents de la clé

permutation finale



Cryptographie à clés publiques

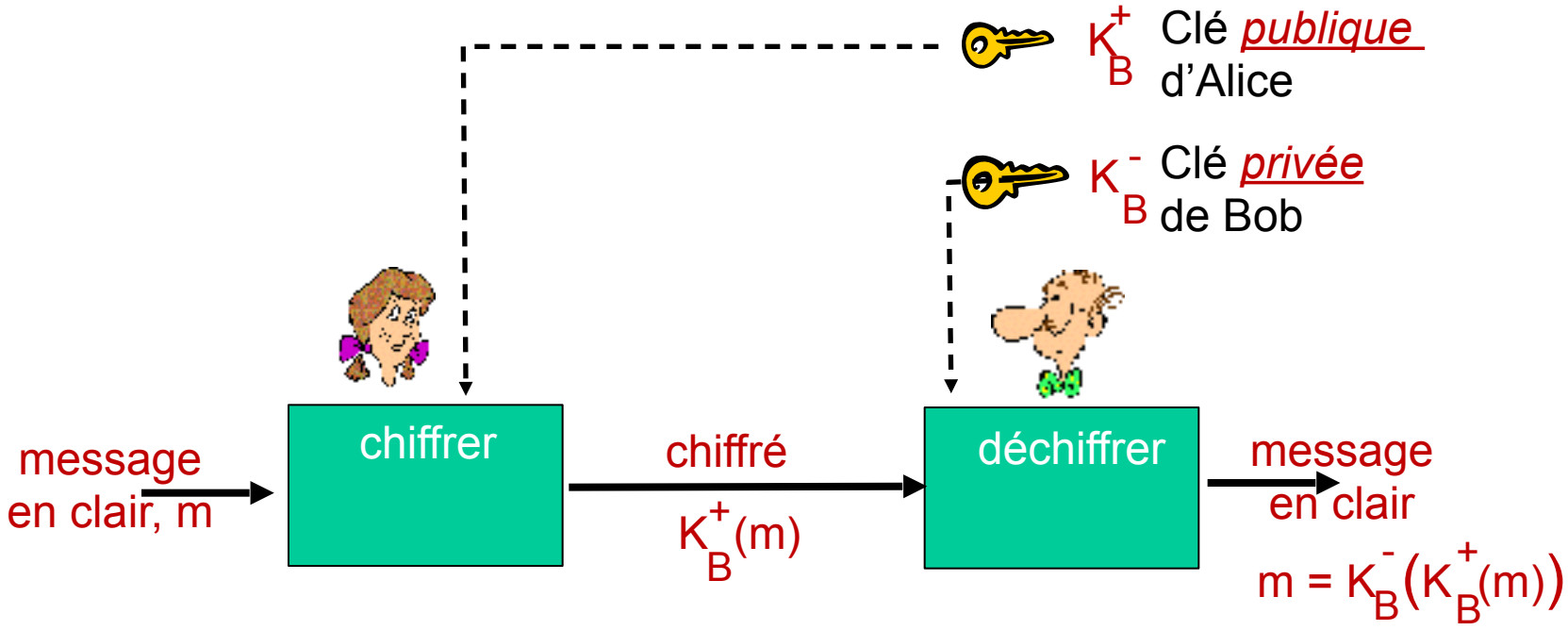
clés symétriques

- Alice et Bob partagent une clé secrète
- Comment obtenir cette clé secrète?

clés publiques

- approche différente [Diffie-Hellman76, RSA78]
- Alice et Bob ne partagent pas de clé secrète
- clé *publique* est connue de tous
- clé *privée* pour déchiffrer n'est connue que de Bob

Cryptographie à clés publiques (Cryptographie asymétrique)



Algorithme de chiffrement

Principe:

1. $K_B^+( )$ et $K_B^-( )$ vérifient

$$K_B^-(K_B^+(m)) = m$$

2. A partir de la clé publique K_B^+, il est « impossible » de calculer la clé privée K_B^-

RSA: Rivest, Shamir, Adelson

RSA: création des clés privée/publique

1. choisir deux grands nombres premiers p et q (par exemple 1024 bits)
2. calculer $n = pq$, $z = (p-1)(q-1)$
3. choisir e $(e<n)$ sans diviseur commun avec z (e, z sont premiers entre eux).
4. choisir d tel que $ed-1$ est divisible par z. (ed mod $z = 1$).
5. *clé publique* $\underbrace{(n,e)}_{K_B^+}$. *clé privée* $\underbrace{(n,d)}_{K_B^-}$.

RSA: chiffrement, déchiffrement,

0. soit (n,e) et (n,d) obtenus précédemment

1. message m ($<n$), c le message chiffré:

   $c = m^e \bmod n$

2. pour déchiffrer c:

   $m = c^d \bmod n$

On a $m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$

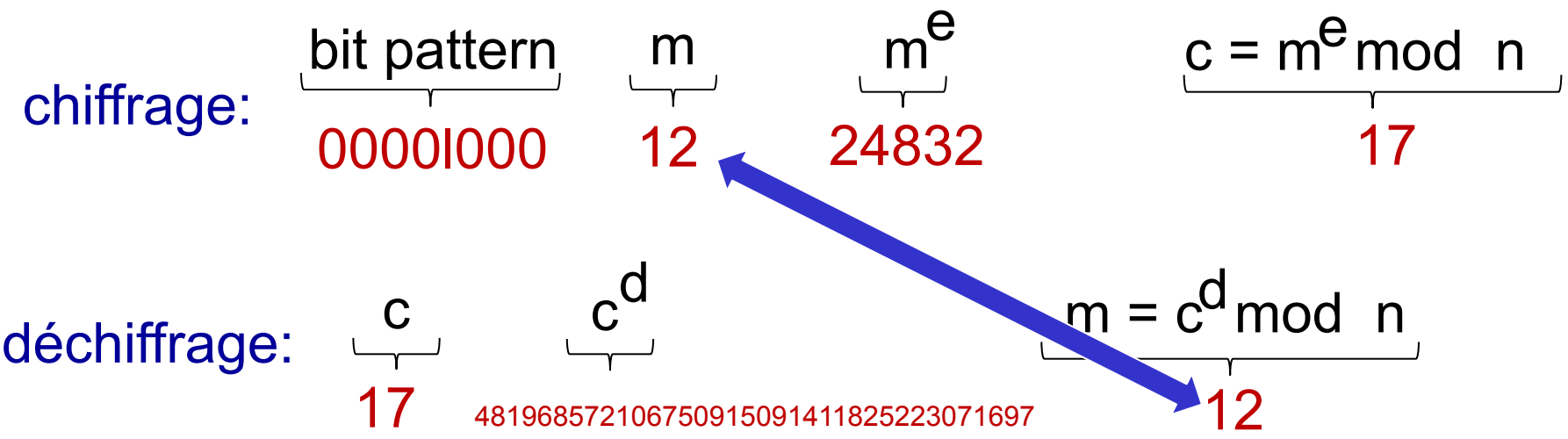
RSA exemple:

Bob choisit *p=5, q=7*. Alors *n=35, z=24*.

e=5 (*e, z* premiers entre eux).

d=29 (*ed-1* divisible par z).

chiffrement message de 8-bits



Chiffrement à clés publiques

RSA vérifie aussi:

$$\underbrace{K_B^-(K_B^+(m))}_{\text{d'abord la clé publique ensuite la clé privée}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{d'abord la clé privée ensuite la clé publique}}$$

Pourquoi RAS est sûr?

- A partir de la clé publique de Bob (n,e). Il est difficile de trouver d
- « nécessite » de factoriser n sans connaître p et q.
  - On considère que factoriser un grand nombre est difficile.

RSA dans la réalité

- l'exponentiation utilisée dans RSA est coûteuse
- DES est 100 fois plus rapide que RSA
- En pratique:
  - utiliser un système à clés publiques pour établir une communication sûre et s'entendre sur une clé symétrique, utiliser cette clé pour chiffrer-déchiffrer les communications.

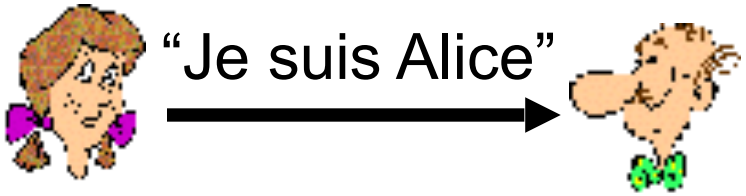
Clé de session, K_S

- Bob et Alice utilisent RSA pour échanger une clé symétrique K_S
- avec K_S, codage symétrique

Authentification

Goal: Bob veut que Alice lui prouve son identité

Protocole ap1.0: Alice dit "Je suis Alice"

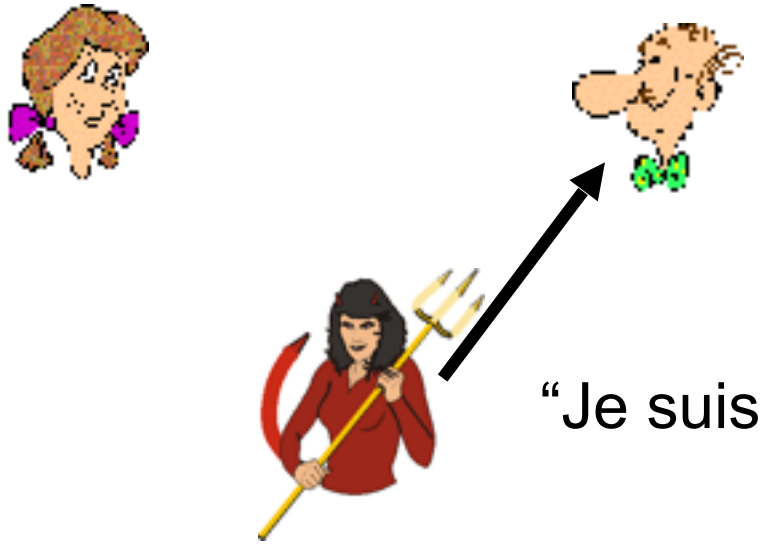


Quelle faille ?

Authentification

Goal: Bob veut que Alice lui prouve son identité

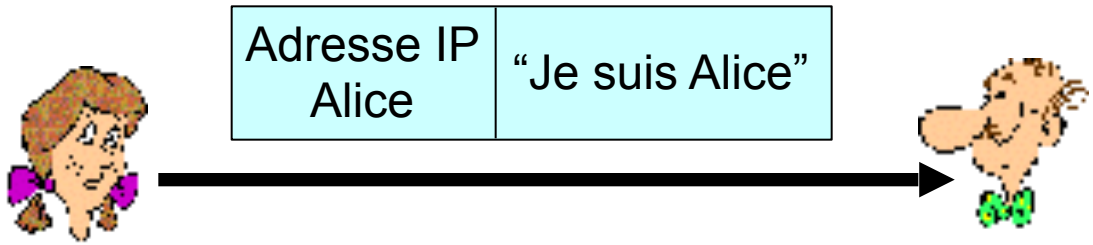
Protocole ap1.0: Alice dit "Je suis Alice"



Bob ne voit pas Alice,
Trudy peut prétendre être
Alice

Authentification: autre essai

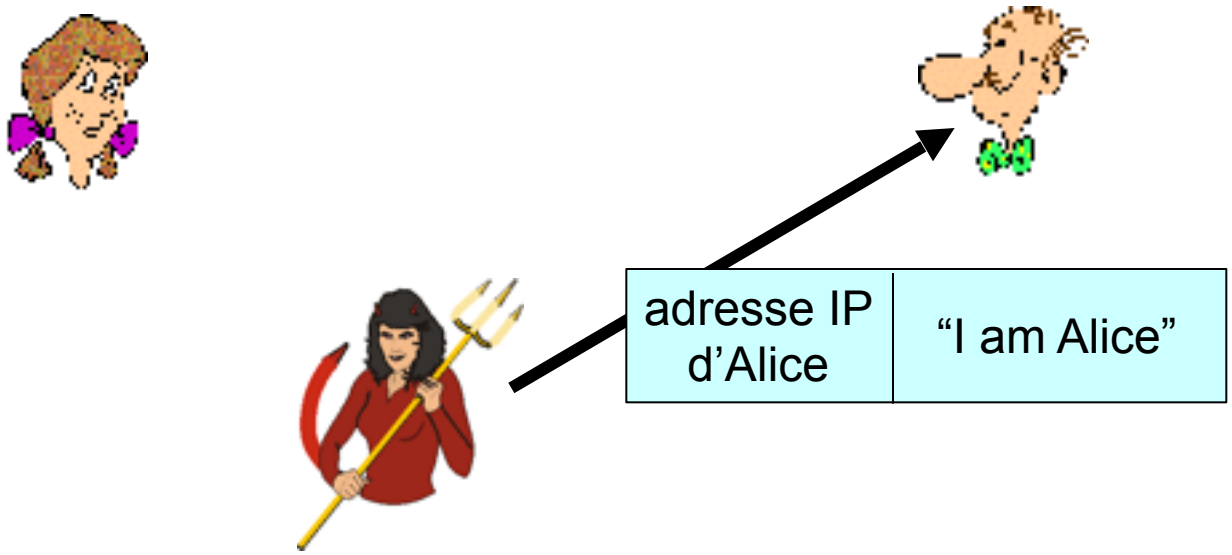
Protocole ap2.0: Alice dit “je suis Alice”
dans un paquet IP avec son adresse IP



La faille??

Authentification: autre essai

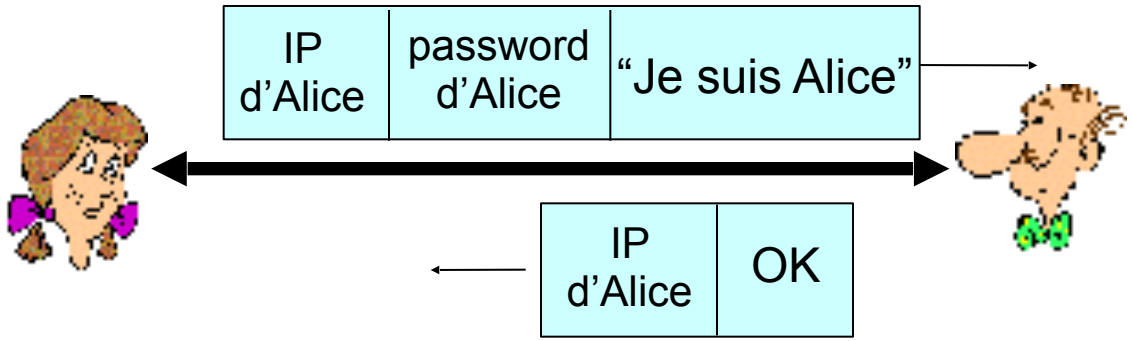
Protocole ap2.0: Alice dit “je suis Alice” dans un paquet IP avec son adresse IP



Trudy peut créer un paquet IP en “spoofant” l’adresse d’Alice

Authentification: autre essai

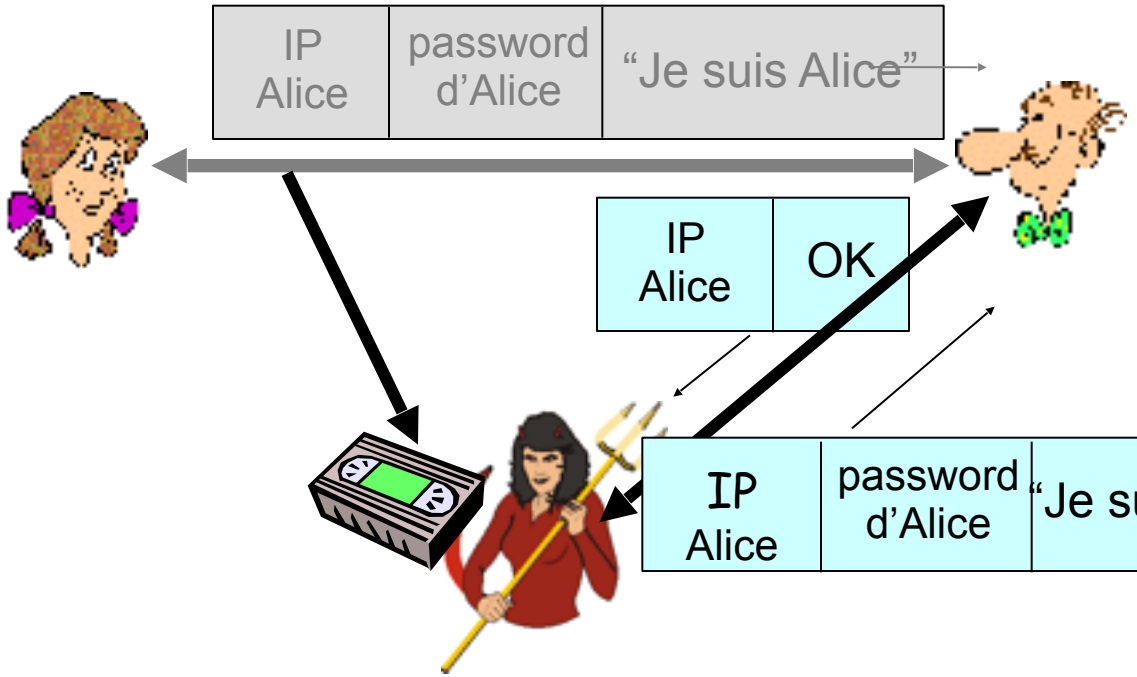
Protocole ap3.0: Alice dit "Je suis Alice" et envoie son password pour le prouver.



Faiblesse ??

Authentification: autre essai

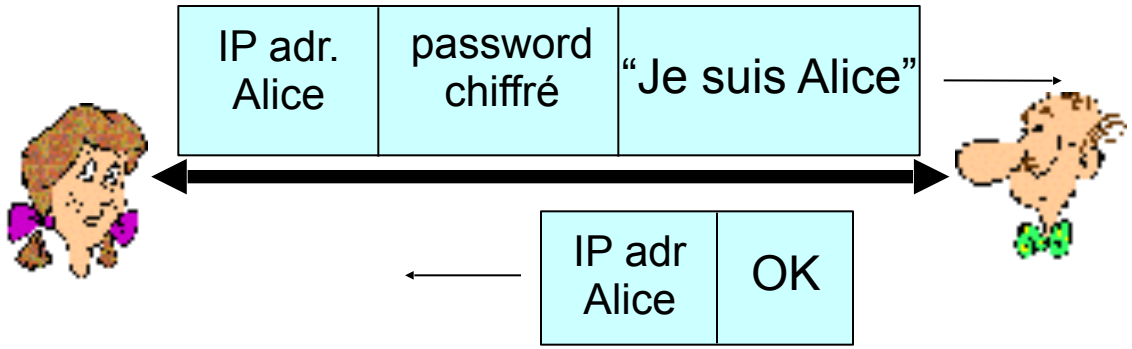
Protocole ap3.0: Alice dit "Je suis Alice" et envoie son password pour le prouver.



attaque par playback: Trudy enregistre le paquet envoyé par Alice et le rejoue vers Bob

Authentification: autre essai

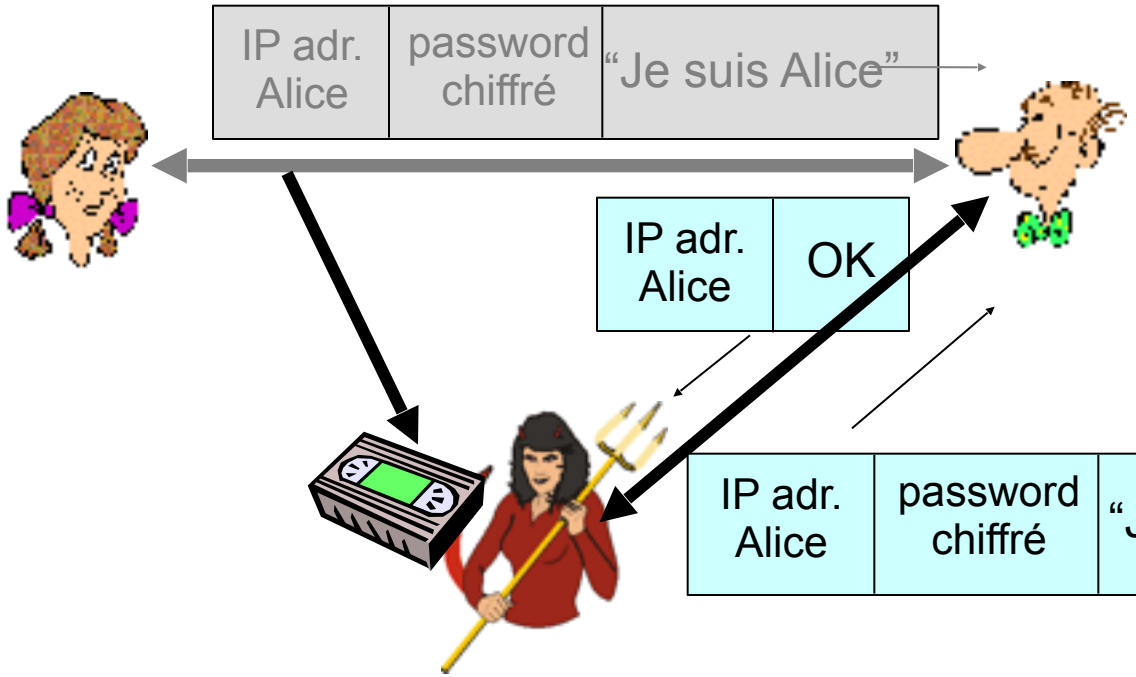
Protocole ap3.01: Alice dit "Je suis Alice" et envoie son password *chiffré* pour le prouver.



La faille??

Authentification: autre essai

Protocole ap3.0: Alice dit "Je suis Alice" et envoie son password pour le prouver.



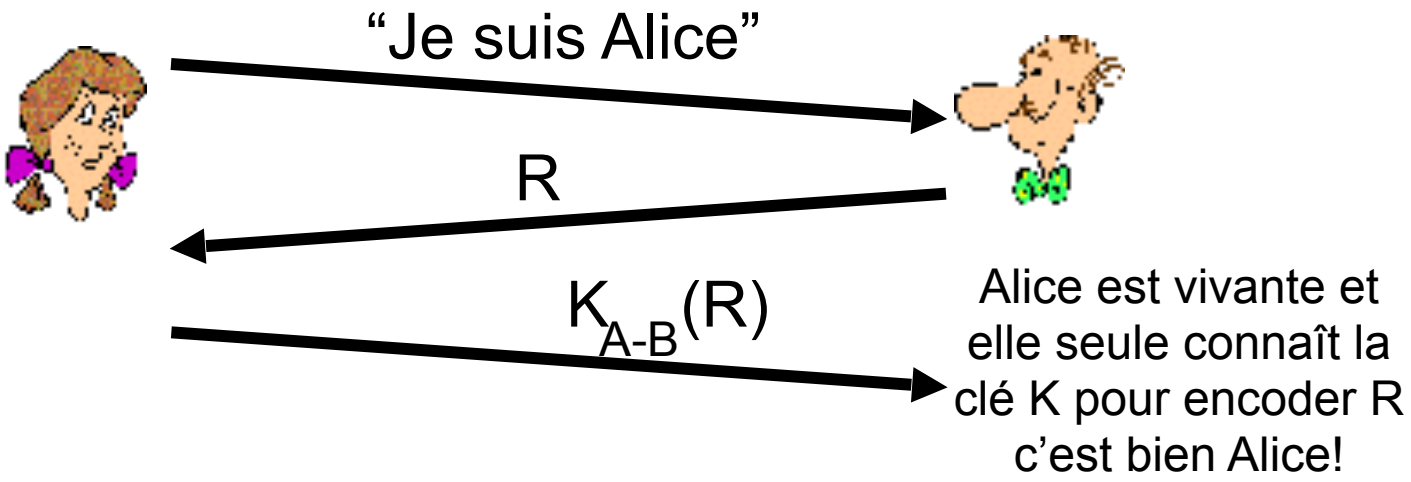
enregistrement et re-jeu (playback) continue à marcher

Authentification: autre essai

But: éviter l'attaque par « playback »

nonce: nombre (R) utilisé *once-in-a-lifetime*

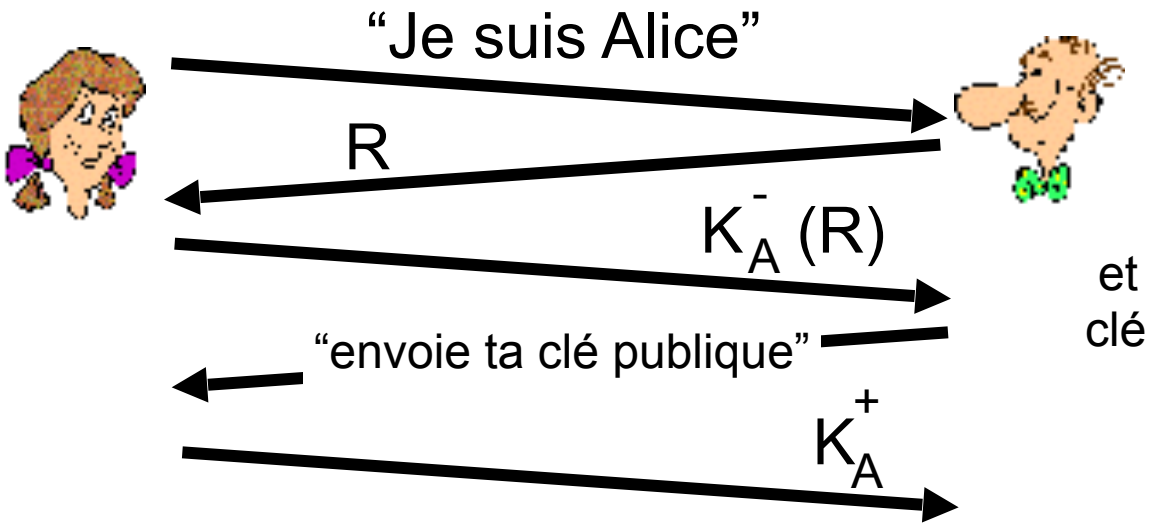
ap4.0: pour prouver que c'est la vraie Alice, Bob envoie à Alice un *nonce* R. Alice renvoie R, chiffré avec la clé secrète partagée



Failles, inconvénients?

Authentification:

dans ap4.0 on a utilisé une clé symétrique partagée
peut-on utiliser un système à clés publiques?
ap5.0: nonce, + cryptographie à clé publique



Bob calcule

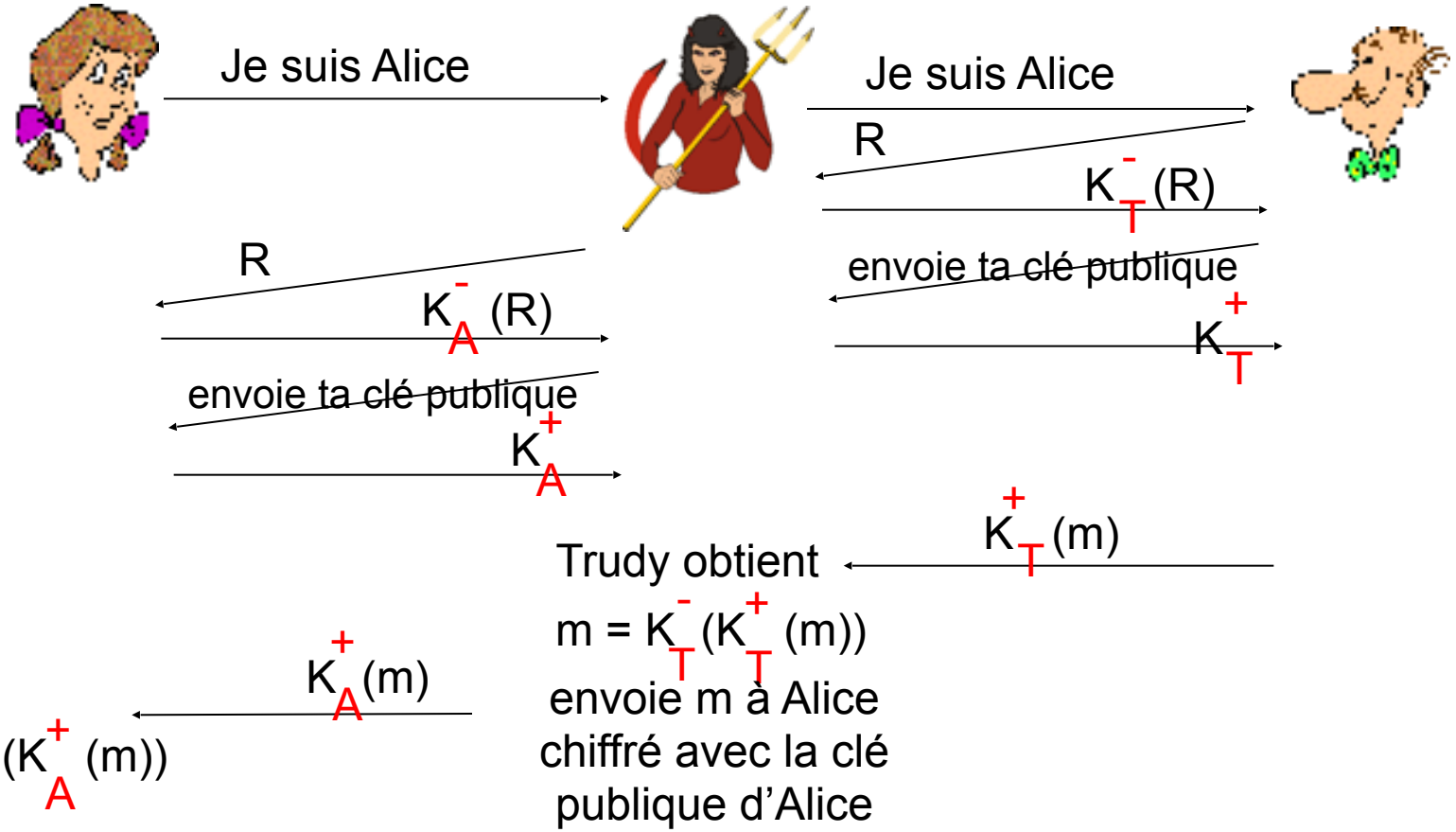
$$K_A^+(K_A^-(R)) = R$$

et sait que seule Alice a la clé privée qui a chiffré R de façon à ce que

$$K_A^+(K_A^-(R)) = R$$

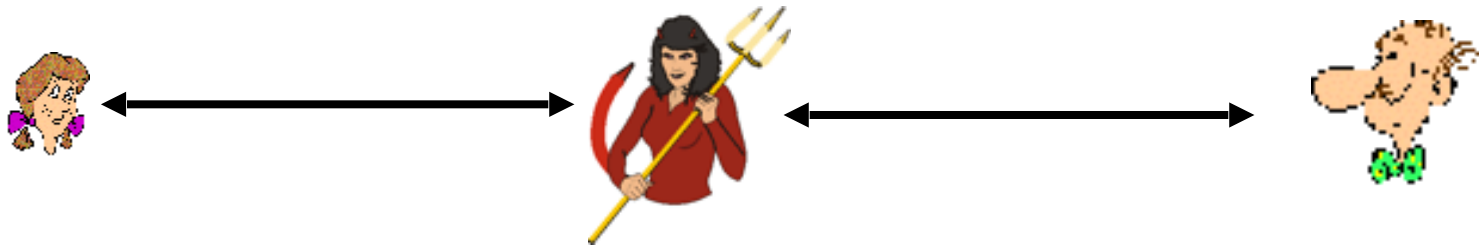
ap5.0: trou de sécurité

man in the middle: Trudy se fait passer pour Alice auprès de Bob et pour Bob auprès d'Alice



ap5.0: trou de sécurité

man in the middle attack: Trudy se fait passer pour Alice auprès de Bob et pour Bob auprès d'Alice



difficile à détecter:

- Bob reçoit tout ce qu'Alice envoie et vice-versa (Bob, Alice peuvent se rencontrer et se rappeler de leur conversation)
- mais Trudy reçoit tous les messages !

Signatures numériques

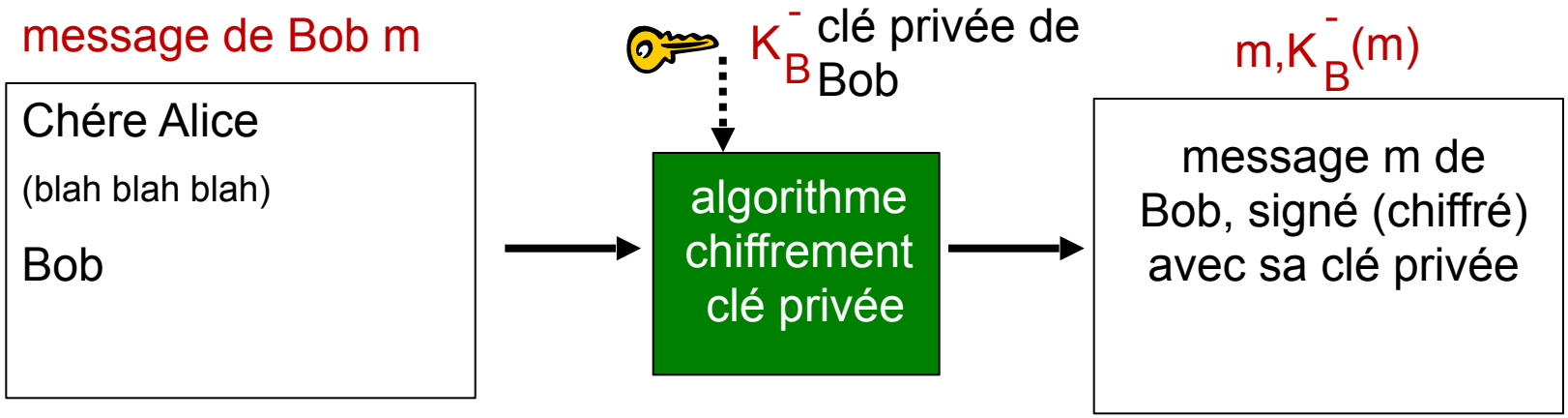
technique analogue à la signature manuelle:

- Bob signe numériquement le document, établissant ainsi qu'il est le créateur/propriétaire du document.
- *vérifiable, infalsifiable (unforgeable):* Alice peut prouver à un tiers que personne d'autres que Bob n'a signé le document

Signatures numériques

simple signature numérique pour le message m:

- Bob signe m en le codant avec sa clé privée K_B^-, créant le message signé , $K_B^-(m)$



Signatures numériques

- si Alice reçoit m, avec la signature: m, $K_B^-(m)$
- Alice vérifie m signé par Bob avec la clé publique de Bob K_B^+ que $K_B^+(K_B^-(m)) = m$.
- Si $K_B^+(K_B^-(m)) = m$, celui qui a signé avait la clé privée de Bob

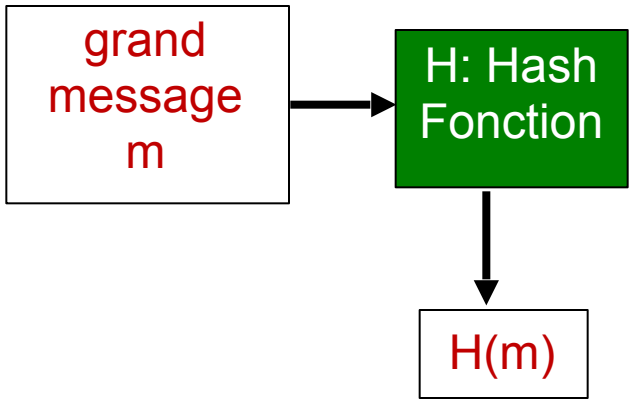
Alice vérifie:

- Bob a signé m
- personne d'autre n'a signé m
- Bob a signé m et pas m'

non-répudiation:

- ✓ Alice peut aller en justice prendre m, et la signature $K_B^-(m)$ et prouver que Bob a signé m

« Message digest »



le chiffrement de longs messages avec clés publique est très coûteux

Mais: mais on peut facilement chiffrer des empreintes (digest) de taille fixe ("fingerprint")

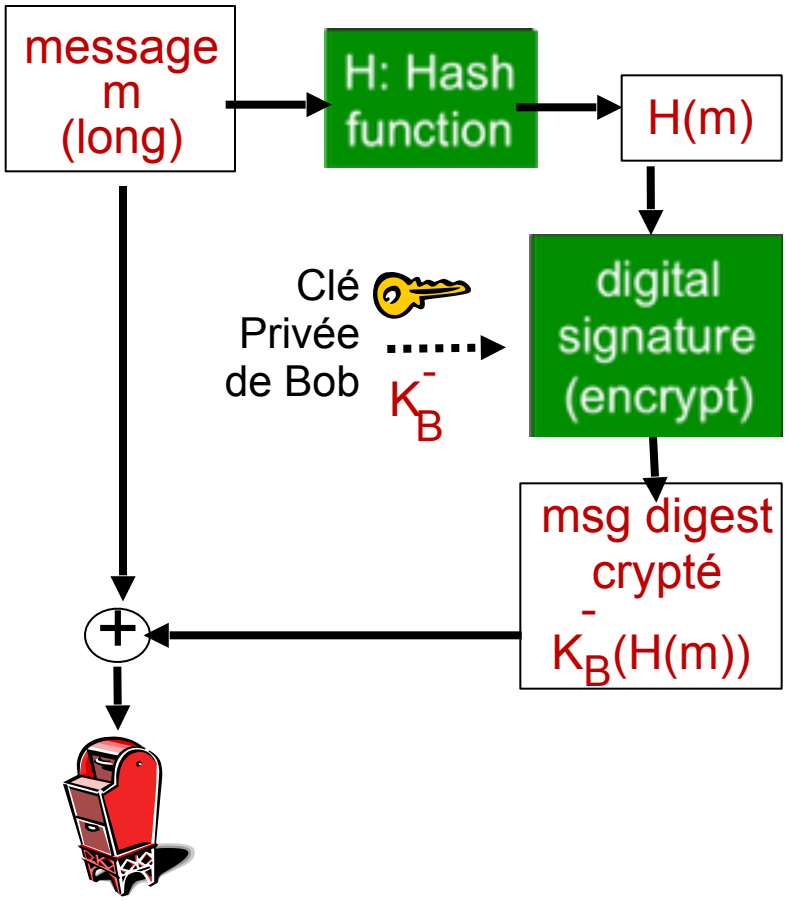
- en appliquent H fonction de hachage à m, on obtient un digest *H(m)*.

Propriétés des fonctions de hachage:

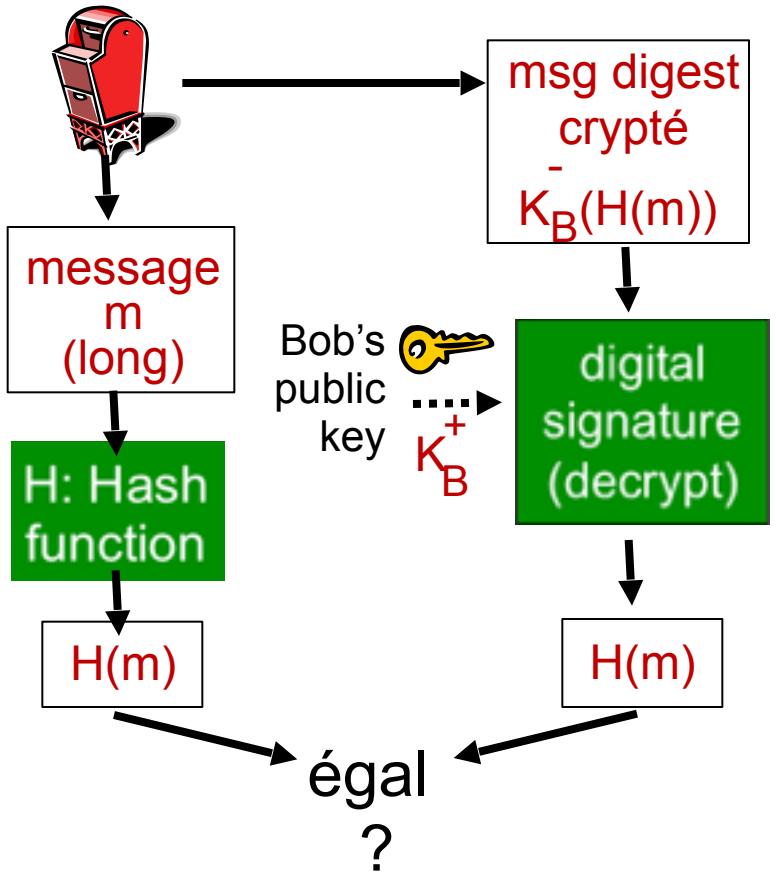
- E=H(M): « impossible »de trouver M connaissant E
- connaissant M et E « impossible »de trouver M' tel que H(M')=H(M)=E
- « impossible » de trouver M et M' tels que H(M)=H(M')

Digest signé comme signature numérique

Bob envoie le message signé :



Alice vérifie la signature,
l'intégrité du message signé:

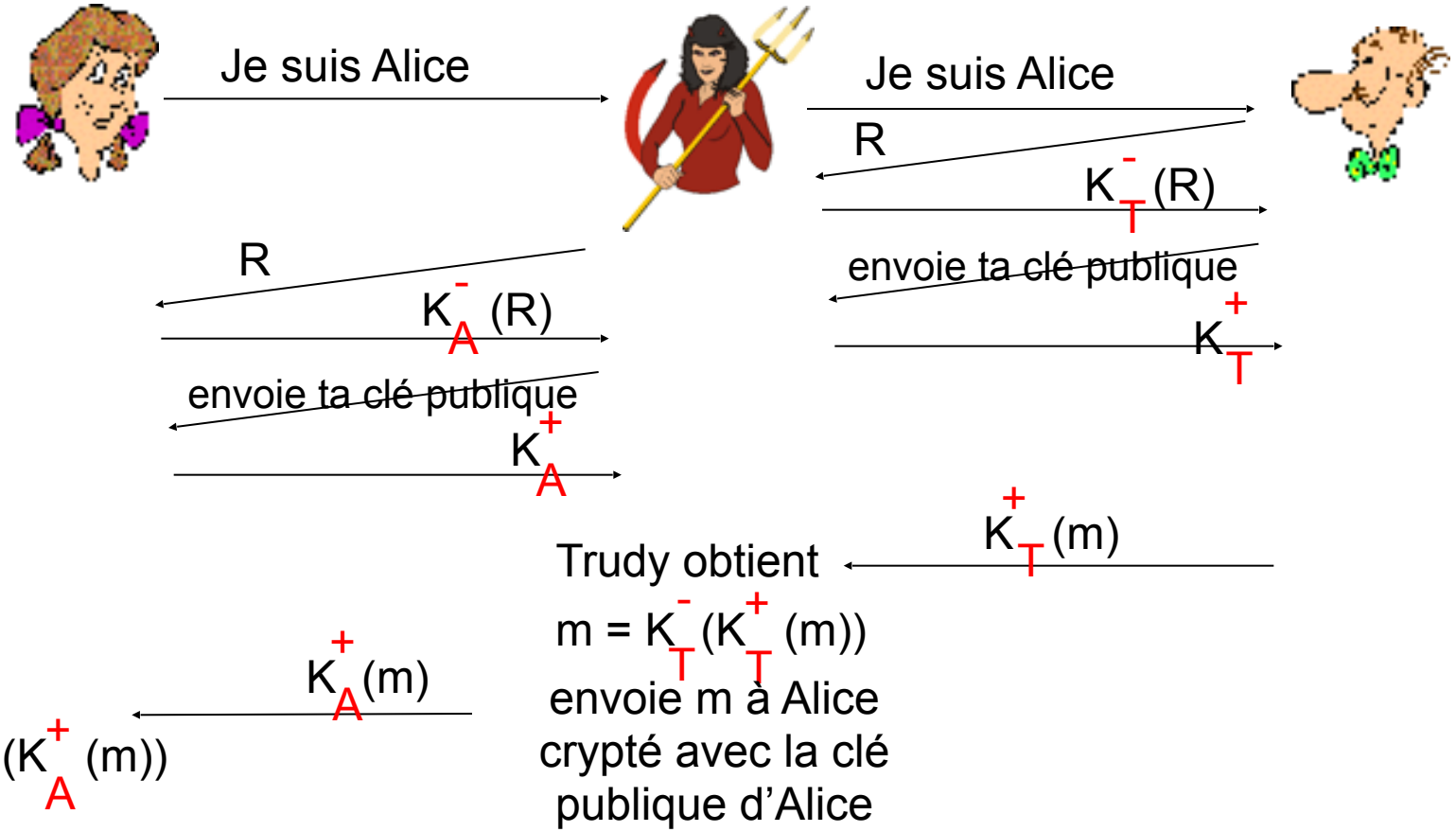


algorithmes de Hash

- MD5 (RFC 1321)
  - calcule un « digest » de128-bit
  - à partir d'une chaîne x de128-bits, il est difficile de construire un msg m pour lequel le hachage par MD5 est égal à x
  - cassé!
- SHA-256 SHA-512

ap5.0: trou de sécurité

man in the middle: Trudy se fait passer pour Alice auprès de Bob et pour Bob auprès d'Alice

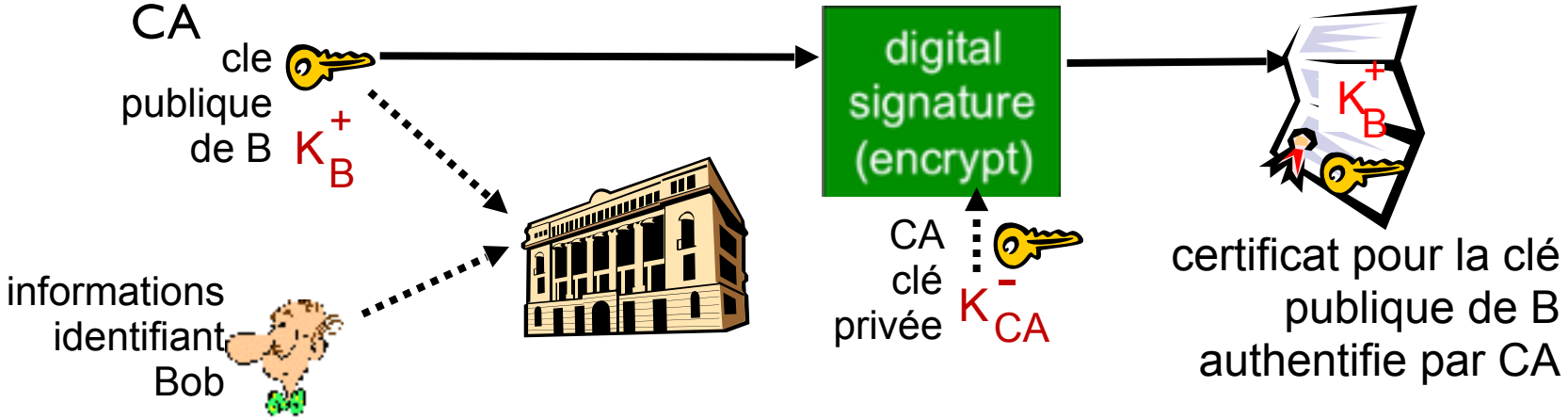


Certification des clés publiques

- motivation:
  - Trudy envoie une commande par e-mail:
    acheter 4 pizzas
  - Trudy signe la commande avec sa clé privée
  - Trudy envoie au magasin sa clé publique mais prétend que c'est celle de Bob
  - le magasin vérifie la signature elle envoie les 4 pizzas à Bob
  - Bob n'a rien demandé!

Autorités de certification

- *certification authority (CA):* associe une clé publique à une entité E.
- E (personne, site) enregistre sa clé publique auprès de l'autorité de certification
- E fournit la preuve de l'identité par la CA.
  - CA crée un certificat associant E à sa clé publique.
  - ce certificat contient la clé publique de E signée numériquement par CA



Autorités de certification

- quand Alice veut obtenir la clé publique de Bob:
  - elle obtient le certificat de Bob (de n'importe qui).
  - applique la clé publique de CA au certificat de Bob, et obtient la clé publique de Bob.