Cryptographie et Cryptanalyse

#BreakTheRules

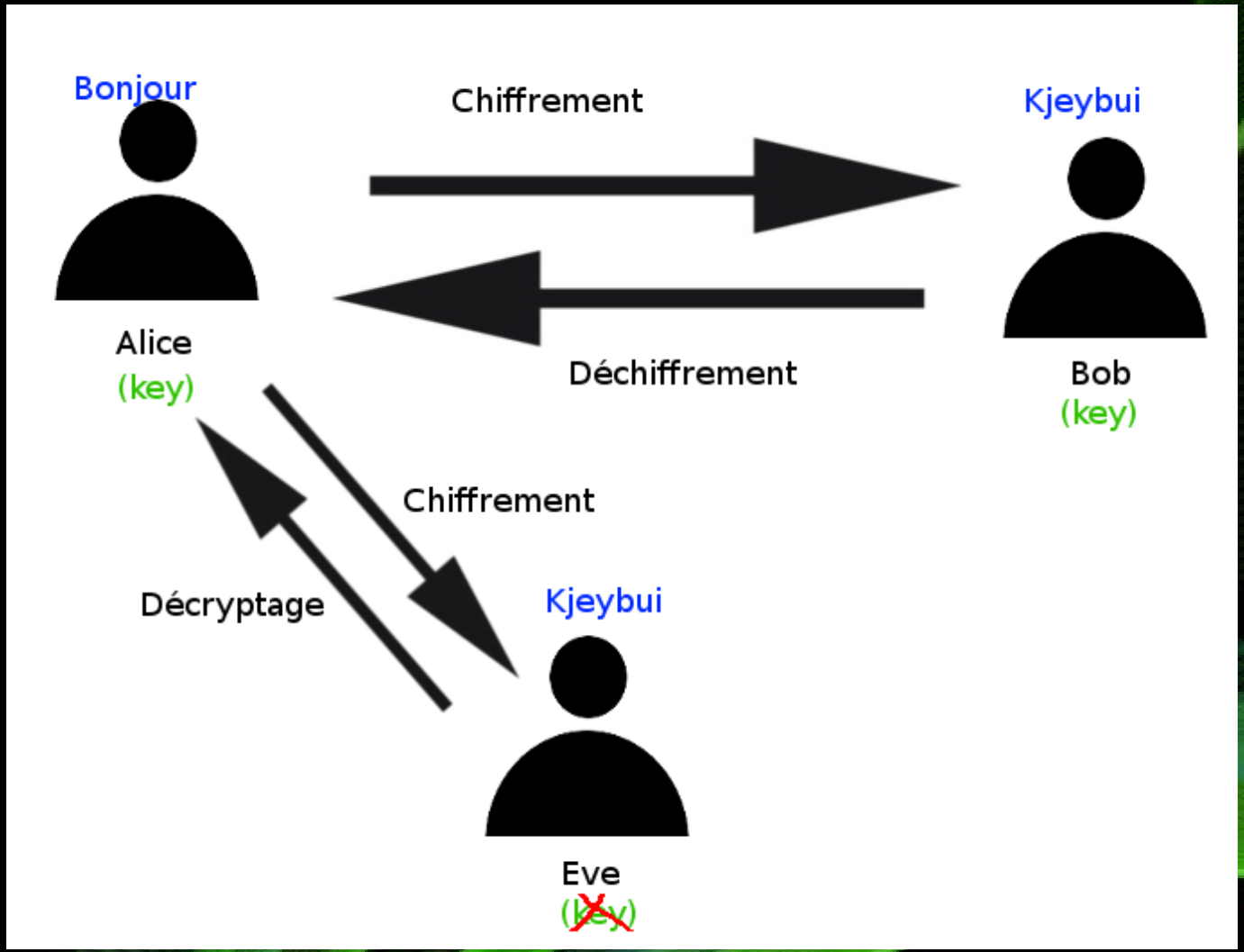
Sommaire

- Définitions
- Cryptographie
- Méthodes de décryptage

Définitions

- Cryptographie : étude et procédés de chiffrement et déchiffrement de l'information
- Cryptanalyse : étude et procédés de décryptage d'une information chiffrée
- Chiffrement/Déchiffrement : avec clé(s)
- Décryptage : Retrouver sans la clé
- "Cryptage" n'existe pas

Définitions



Cryptographie

- But de la cryptographie :
  - Confidentialité : via chiffrement
  - Intégrité : via hachage
  - Authenticité : via signature

Cryptographie

- Chiffrement :

  S’assurer que seuls les personnes autorisées puissent lire les données et personne d’autre

  Se fait obligatoirement grâce à une ou plusieurs clés
- Chiffrement symétrique : même clé pour chiffrement et déchiffrement
- Chiffrement asymétrique : clé pour chiffrement (publique) et pour déchiffrement (privée) différentes mais mathématiquement liées

Cryptographie

- Méthodes de chiffrement symétrique :

- Substitution monoalphabétique :
  - Chaque lettre est remplacée par une autre

- Substitution polyalphabétique :
  - Combinaison message + clé (Vigenère)

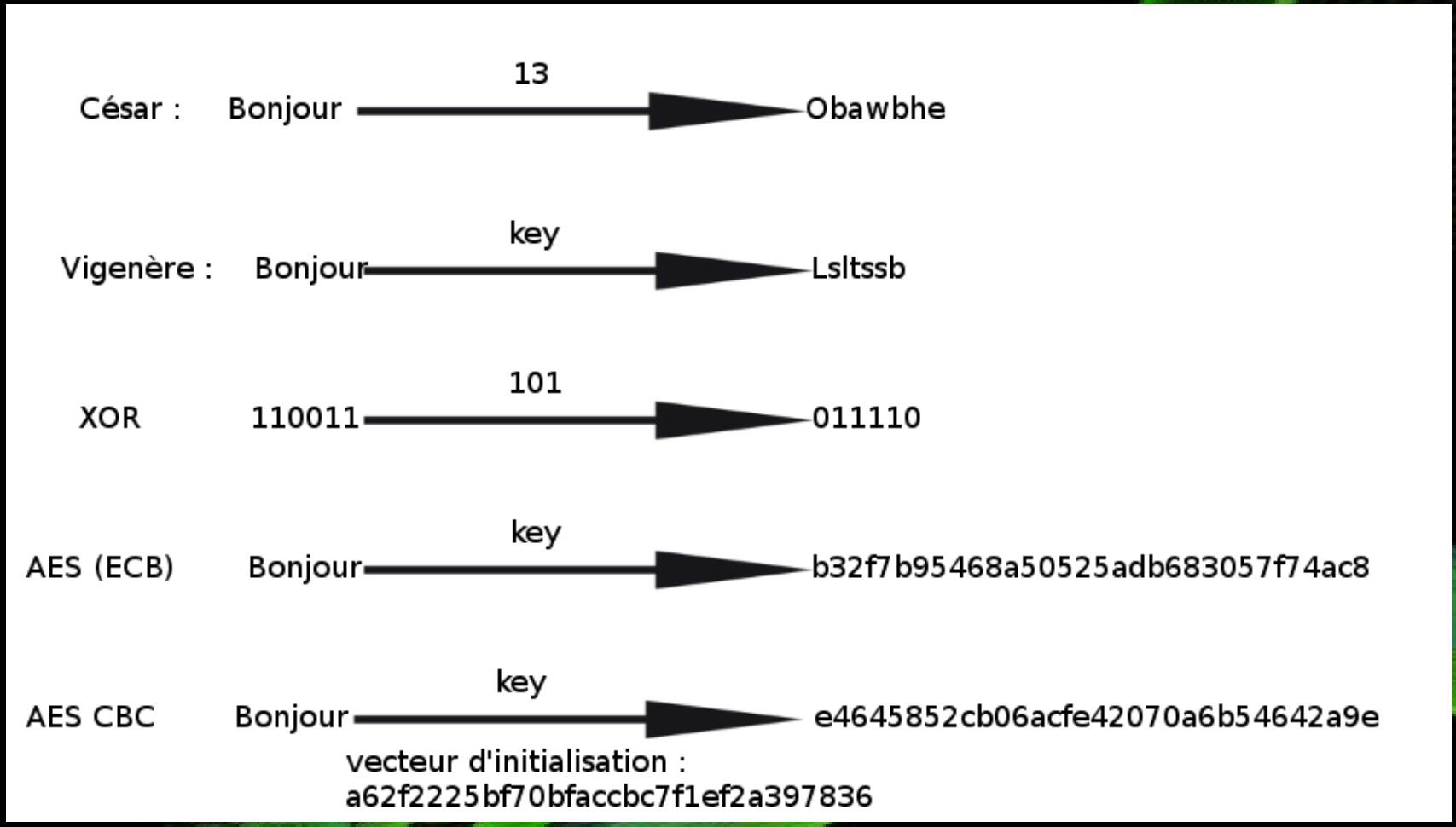
Cryptographie

- Méthodes de chiffrement symétrique :
- Chiffrement de Vernam :
  - Substitution polyalphabétique avec :
    - Clé aléatoire
    - Clé plus longue que le message

- Chiffrement par bloc :
  - Message chiffré bloc par bloc
  - La clé de chaque bloc peut provenir du bloc précédent (mode CBC) ou être la même pour chaque bloc (mode ECB)

Cryptographie

- Chiffrement symétrique : exemples



Cryptographie

- Chiffrement asymétrique : RSA
  - Deux types de clés : publique et privée
  - Clés liées mathématiquement
  - Retrouver la clé publique via la clé privée très difficile (actuellement impossible si très longue)

Cryptographie

- Chiffrement symétrique : RSA

Variables :
p,q nombres premiers
n=pq
phi = (p-1)(q-1)
e premier avec phi
d=inverse de e modulo phi
m =message en clair

Clé publique : (n,e)
Clé privée : (n,d)

On a de plus : $e.d \equiv 1 [n]$

Chiffrement : $y=m^e [n]$

Déchiffrement : $m=c^d [n]$

L'astuce : pour connaitre d, il faut connaitre phi
pour connaitre phi, il faut connaitre p et q
pour connaitre p et q, il faut factoriser n
Si p et q trèèèèèès grands, c'est trèèèèèès difficile

Cryptographie

- Hachage

- Attribuer une chaine de taille fixe à un flot de données
- Fonction de hachage “f(x)” doit être :
  - Irréversible : $f^{-1}(x)$ impossible à trouver
  - Sans collision triviale : x et y tels que f(x)=f(y) difficiles à trouver
  - Chaotique : une petite différence engendre des hashs très différents

Cryptographie

- Hachage : exemples

Cryptographie

- Hachage : utilisation

- Algorithmes rapides : intégrité d’un flot de données
  - MD5, SHA-1, SHA-256,...

- Algorithmes lents : stockage de données d’authentification
  - Bcrypt, couplé avec un sel

Cryptographie

- Hachage : Utilisation d’un sel
- Sel : Données mélangées au mot de passe pour former le hache
- Ajout de complexité : chaque combinaison mot de passe/sel doit être hachée puis comparée au hache stocké.

Cryptographie

- Signature numérique
- Vérifier l’intégrité d’un fichier et l’authenticité de son envoyeur
- Fichier haché
- Hache + certificat chiffrés

Cryptanalyse

- Différentes méthodes de décryptage :
  - Bruteforce
  - Attaque par dictionnaires
  - Analyses statistiques
  - Exploitation de failles
  - Rainbow tables

Cryptanalyse

- Bruteforce
- Tester chaque clé une par une
- Fonctionne pour des petites clés et des algorithmes rapides

Cryptanalyse

- Attaque par dictionnaire
- Liste de mots de passe communs à tester
- Possibilité de combiner avec du bruteforce
- Possibilité d’ajouter des règles (a → @,...)

Cryptanalyse

- Analyses statistiques
- Deviner les substitutions en utilisant la fréquence des caractères

- Efficace pour la substitution monoalphabétique

Cryptanalyse

- Exploitation de failles
- Fonctionne sur les algos “faits main”
- Comprendre le code, trouver une faille
- Ex : Utilisation du PID comme clé → facile à récupérer

Cryptanalyse

- Exploitation de failles
- Fonctionne sur les algos “faits main”
- Comprendre le code, trouver une faille
- Ex : Utilisation du PID comme clé → facile à récupérer

Cryptanalyse

- Rainbow tables
- Vieilles fonctions de hachage (ex : MD5)
- Génération d’une suite de haches “intermédiaires” en fonction du hache de départ

  → Construction d’une table
- Accélération du bruteforce

Conclusion

- Cryptographie représente un enjeu majeur
- Utilisée PARTOUT
- Cryptanalyse destinée à tester la robustesse des algorithmes
- Certaines fonctions communes déjà obsolètes
  - MD5 utilisé encore pour hacher les mots de passe sur certains sites !
- Nécessité de trouver de nouveaux algorithmes en permanence