Introduction à la Cryptographie

1. Généralités et concepts de base

Cécile Pierrot, Chargée de Recherche INRIA Nancy
cecile.pierrot@inria.fr

Supports de E. Thomé

Telecom Nancy, 2A ISS – 2021

Objectifs du cours

- Comprendre
  - le rôle de la cryptographie dans la protection de l'information
  - les fonctionnalités cryptographiques fondamentales
  - les limites de la protection assurée par la cryptographie
- Connaître
  - le langage dans lequel est construite la cryptographie
  - quelques primitives cryptographiques et leurs principes

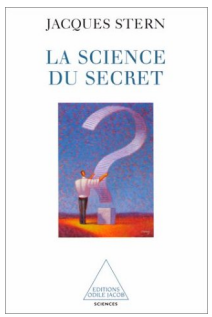
Plan du cours (6 heures)

1. Généralités et concepts de base
2. Chiffrement symétrique
   - chiffrement de Vernam
   - chiffrement par flot
   - chiffrement par bloc (AES)
3. Cryptographie à clé publique
   - chiffrement (RSA)
   - échange de clés (Diffie-Hellman)
   - signature (DSA)

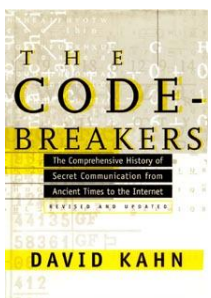
- 3 TD, 1 projet

Bibliographie : histoire / vulgarisation

Singh, *Histoire des Codes Secrets*.
Livre de Poche, 2001.

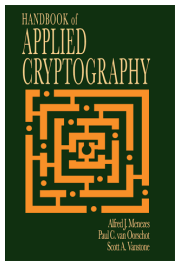


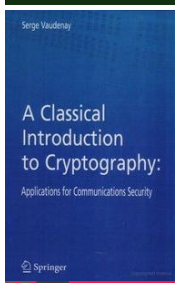
Stern, *La Science du Secret*.
Odile Jacob, 1998.

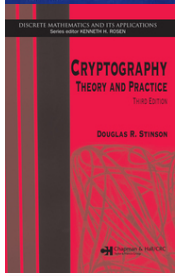


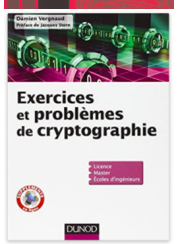
Kahn, *The Codebreakers, revised edition*.
Schribner, 1996.

Bibliographie : ouvrages de référence









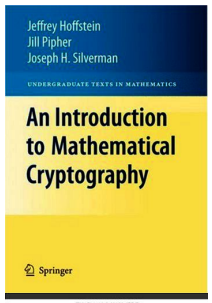
Menezes, van Oorschot, Vanstone,
Handbook of Applied Cryptography.
Chapman & Hall / CRC, 1996.
`http://www.cacr.math.uwaterloo.ca/hac/`

Vaudenay, *A Classical Introduction to Cryptography*.
Springer, 2005.

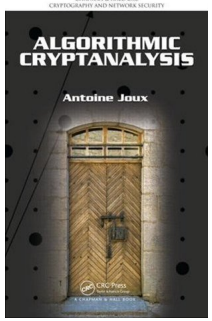
Stinson, *Cryptography: Theory and Practice, 3rd edition*.
Chapman & Hall / CRC, 2005.

Vergnaud, *Exercices et problèmes de cryptographie*.
Dunod, 2017.

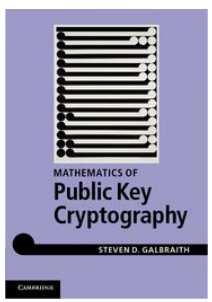
Bibliographie : pour aller plus loin



Hoffstein, Pipher, Silverman,
An Introduction to Mathematical Cryptography.
Undergraduate Texts in Mathematics, Springer, 2008.



Joux, *Algorithmic Cryptanalysis*.
CRC press, 2009.



Galbraith,
Mathematics of Public Key Cryptography.
Undergraduate Texts in Mathematics, Springer, 2012.

Plan

Contexte

Vocabulaire

Repères historiques

Généralités

Cryptographie symétrique / asymétrique

Plan

Position du problème

Caractéristiques des systèmes d'information

- Information numérique
- Communications sur un canal public
- Machines reliées par réseau
- Multi-utilisateurs

Les acteurs

Alice

Les acteurs

Alice

Bob

Mais aussi : Charlie, Eve...

`https://en.wikipedia.org/wiki/Alice_and_Bob`

Tous jouent à un jeu qu'on va d'abord tenter de définir.

Les besoins de sécurité

- Confidentialité
  - Maintien au secret des informations vis-à-vis de tiers
- Intégrité
  - État des informations qui n'ont pas été modifiées
- Authenticité
  - Garantie de l'identité d'une entité ou de l'origine d'une communication
- Et aussi : non répudiation, vote électronique, divulgation nulle de connaissance etc

Situations d'usage (1/2) : le chiffrement

Les propriétés offertes par la cryptographie sont souvent utiles.

- Courrier électronique :
  - Si je ne veux surtout pas que ma petite sœur lise le contenu.
  - Si je ne veux surtout pas que la NSA lise le contenu.
- Disque dur. Je chiffre mon disque dur pour protéger le contenu (informations confidentielles, vie privée) contre :
  - Le vol.
  - L'intrusion (laissez-nous votre PC monsieur, on l'inspecte...)
- Travail à distance (vpn, ssh) : quand il y a 2000km entre le clavier et l'ordinateur.
- Communication sensible : ma carte bancaire avec le terminal de paiement.

Ceci relève de la confidentialité.
Les données chiffrées ne doivent pas être déchiffrables par l'adversaire.

Situations d'usage (2/2) : la signature

D'autres situations :

- Distributions de paquets logiciels : assurer que c'est un vrai, pas une version vérolée.
- Commerce en ligne : assurer qu'on parle bien à Amazon, pas à un pirate.
- Internet des Objets (IoT) : quand ma clef de voiture ouvre ma voiture à distance.
- Signature : créer un courrier électronique capable de faire foi.
- Authentification : Prouver qui on est. Ou qu'un document provient bien de la bonne autorité (ex : passeport).

Tout ceci relève davantage de l'authenticité.
On signe une donner pour lui donner une garantie d'authenticité.

Bien définir le problème

Souvent, il n'y a pas de réponse unique à un besoin de cryptographie.

- Tout dépend des hypothèses faites sur l'espion.
- Tout dépend des garanties qu'on souhaite obtenir.

Il faut être réaliste. Mon mail passe par gmail, donc la NSA l'écoute.

- En général, on suppose que l'attaquant est très fort, et on voit ce qu'on peut garantir.
- Si nécessaire, on raffine (mais si on peut obtenir des garanties maximales pour pas cher, on ne se prive pas).

Moyens de protection

- Il existe plusieurs techniques :
  - Cryptographie
  - Sécurité informatique
  - Tempest
- Chaque technique propose des solutions contre certaines menaces
- Pour se protéger efficacement, il faut combiner les techniques

La science du secret

De nombreuses applications dans la vie courante :

- `ssl`, `ssh`, gpg, *etc.*
- carte bleue, téléphone cellulaire, WiFi, Bluetooth
- *etc.*

En quoi consiste cette science ?

Cryptologie

Définition (Cryptologie)

Étude de la protection de l'information sous forme numérique contre des accès ou manipulations non-autorisés.

$$\text{cryptologie} = \text{cryptographie} + \text{cryptanalyse}$$

- cryptographie : conception des algorithmes cryptographiques
- cryptanalyse : évaluation de la sécurité des algorithmes cryptographiques

Plan

Vocabulaire

- Tous les mots corrects du vocabulaire d'un cryptographe ne se trouvent pas dans tous les dictionnaires communs.
- Internet est régulièrement truffé d'erreurs, en particulier en français et dans les médias.

Anglais	Français	Commentaire
Cipher	Chiffre	Rare (en français)
Cryptosystem	Cryptosystème	
Encrypt	Chiffrer	~~Crypter~~
Encryption	Chiffrement	~~Chiffrage~~ ~~Cryptage~~
Decrypt	Déchiffrer	
Decryption	Déchiffrement	~~Décryptement~~ ~~Décryptage~~
(Ad.) decrypt	Décrypter	L'adversaire décrypte,
(Ad.) decryption	Attaque	le correspondant déchiffre.

Vocabulaire

D'autres termes . . .

Anglais	Français
Cryptanalysis	Cryptanalyse
Block cipher	Chiffrement par blocs
Stream cipher	Chiffrement à flot
Plaintext	Message clair
Ciphertext	Message chiffré
Hash function	Fonction de hachage
Digest	Haché, ou empreinte

Plan

Cryptographie *artisanale*

Antiquité – 19e s.	César (1er s. av. J.C.), Vigenère (1586), *etc.* Transpositions et substitutions alphabétiques

Cryptographie *mécanique*

1883 *La Cryptographie Militaire* [Kerckhoffs]
Formalisation des systèmes de chiffrement

1926 *Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications* [Vernam]
Chiffrement de Vernam (masque jetable)

1939-44 Enigma et les bombes de Bletchley Park

1950-60 Machines Hagelin

Cryptographie *industrielle*

1949 *Communication Theory of Secrecy Systems* [Shannon]
Notion de sécurité inconditionnelle

1973-77 Standardisation de DES (*Data Encryption Standard*)

1976 *New Directions in Cryptography* [Diffie-Hellman]
Invention de la cryptographie à clé publique

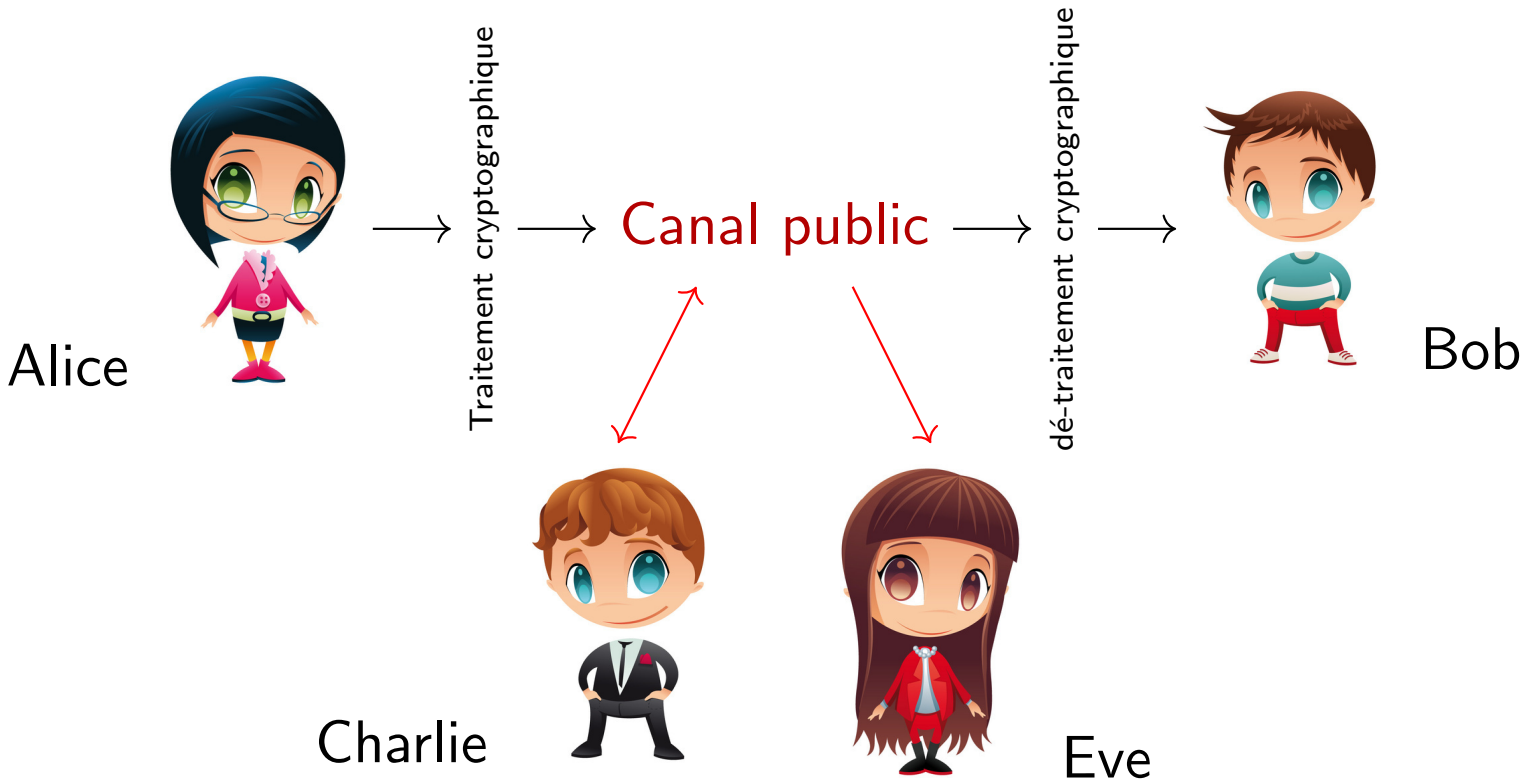
1978 *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* [Rivest-Shamir-Adleman]
Invention de RSA

1997-00 Standardisation d'AES (*Advanced Encryption Standard*)

Plan

Modèle de communication

Modèle simplifié d'un système de communication cryptographique



- Charlie et Eve sont des attaquants (actif/passif).
- Le canal induit du délai, et des intermédiaires.

Différentes menaces

Une attaque peut être

- attaque passive : espionnage
-  : attaque active ;
  - usurpation d'identité (de l'émetteur ou du récepteur)
  - altération des données = modification du contenu du message
  - répudiation du message = l'émetteur nie l'avoir envoyé
  - répétition du message
  - retardement de la transmission
  - destruction du message
- Approximation raisonnable pour les attaques actives : le canal est l'attaquant.

Motivations et cibles

- Des attaques aux motivations très variées
  - Ludique : amusement, curiosité, défi, réputation
  - Idéologie (voire terrorisme) : vandalisme, déni de service
  - Cupidité : vol de données bancaires, extorsion (*ransomware*)
  - Espionnage : industriel (concurrence) ou étatique (surveillance)
- Tout système d'information est une cible potentielle
  - Infrastructures «vitales» : réseaux électrique, de communications, de transports, centrales nucléaires, hôpitaux
  - États : sites gouvernementaux et militaires
  - Entreprises : cyber-espionnage, vengeance
  - Entités académiques : universités, laboratoires de recherche
  - Individus : cibles vulnérables, peu sensibilisées, ne maîtrisent pas toutes les données qu'elles produisent ; leurs machines peuvent aussi servir de relais (*botnet*)

Modèle simplifié de système d'information

- Superposition de plusieurs couches

Modèle simplifié de système d'information

- Superposition de plusieurs couches
  - Matériel (machines, routeurs, câbles, etc.)

Modèle simplifié de système d'information

- Superposition de plusieurs couches
  - Système d'exploitation
  - Matériel (machines, routeurs, câbles, etc.)

Modèle simplifié de système d'information

- Superposition de plusieurs couches
  - Programmes et bibliothèques logicielles
  - Système d'exploitation
  - Matériel (machines, routeurs, câbles, etc.)

Modèle simplifié de système d'information

- Superposition de plusieurs couches
  - Protocoles (IP, TCP, HTTP, etc.)
  - Programmes et bibliothèques logicielles
  - Système d'exploitation
  - Matériel (machines, routeurs, câbles, etc.)

Modèle simplifié de système d'information

- Superposition de plusieurs couches
  - Utilisateurs
  - Protocoles (IP, TCP, HTTP, etc.)

  - Programmes et bibliothèques logicielles
  - Système d'exploitation
  - Matériel (machines, routeurs, câbles, etc.)

Modèle simplifié de système d'information

- Superposition de plusieurs couches
  - Utilisateurs
  - Protocoles (IP, TCP, HTTP, etc.)
  - Primitives cryptographiques (AES, RSA, etc.)
  - Programmes et bibliothèques logicielles
  - Système d'exploitation
  - Matériel (machines, routeurs, câbles, etc.)

Modèle simplifié de système d'information

- Superposition de plusieurs couches
  - Utilisateurs
  - Protocoles (IP, TCP, HTTP, SSL/TLS, etc.)
  - Primitives cryptographiques (AES, RSA, etc.)
  - Programmes et bibliothèques logicielles
  - Système d'exploitation
  - Matériel (machines, routeurs, câbles, etc.)

Modèle simplifié de système d'information

- Superposition de plusieurs couches
  - Utilisateurs
  - Protocoles (IP, TCP, HTTP, SSL/TLS, etc.)
  - Primitives cryptographiques (AES, RSA, etc.)
  - Programmes et bibliothèques logicielles
  - Système d'exploitation
  - Matériel (machines, routeurs, câbles, etc.)
- Chaque couche présente des vulnérabilités et donc autant de risques d'attaque

Modèle simplifié de système d'information

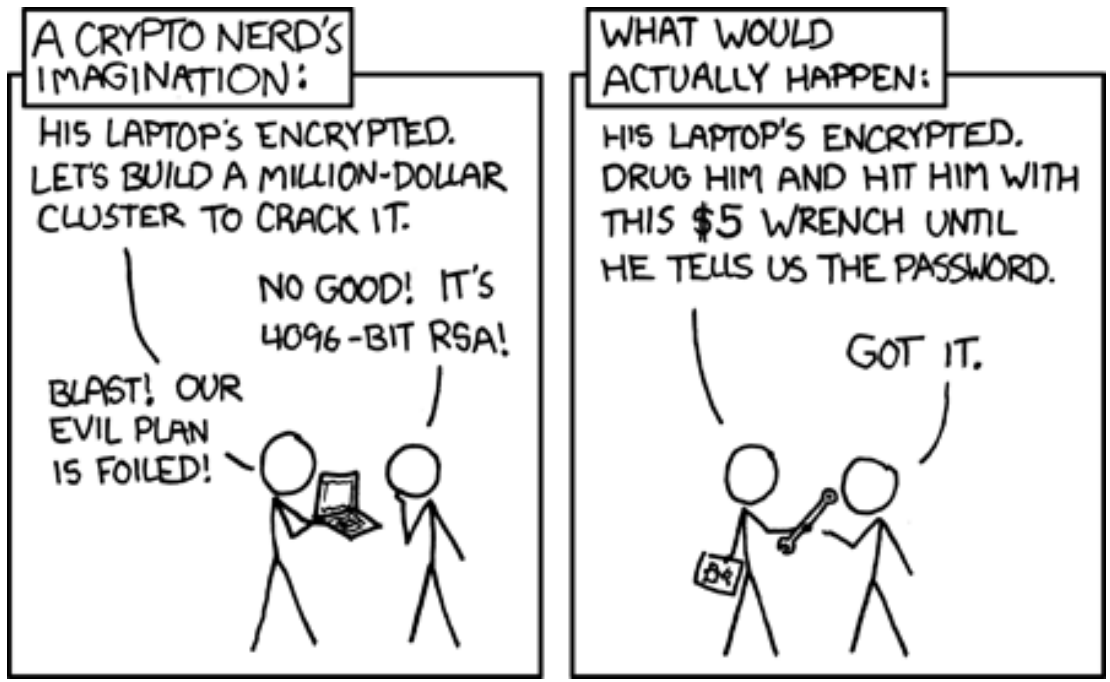
- Superposition de plusieurs couches
  - Utilisateurs
  - Protocoles (IP, TCP, HTTP, SSL/TLS, etc.)
  - Primitives cryptographiques (AES, RSA, etc.)
  - Programmes et bibliothèques logicielles
  - Système d'exploitation
  - Matériel (machines, routeurs, câbles, etc.)
- Chaque couche présente des vulnérabilités et donc autant de risques d'attaque
- Attaque sophistiquée : plusieurs vecteurs d'attaque exploités conjointement

Modèle simplifié de système d'information

- Superposition de plusieurs couches
  - Utilisateurs
  - Protocoles (IP, TCP, HTTP, SSL/TLS, etc.)
  - Primitives cryptographiques (AES, RSA, etc.)
  - Programmes et bibliothèques logicielles
  - Système d'exploitation
  - Matériel (machines, routeurs, câbles, etc.)
- Chaque couche présente des vulnérabilités et donc autant de risques d'attaque
- Attaque sophistiquée : plusieurs vecteurs d'attaque exploités conjointement
- Besoin d'un plan de sécurité globale :
  analogie de la porte blindée et des fenêtres ouvertes

Limites de la cryptographie

La cryptographie n'est pas la réponse à tous les besoins de sécurité :



Elle doit être utilisé avec des mesures complémentaires en fonction des menaces.

Un attaquant attaque toujours le maillon le plus faible (souvent l'utilisateur).

Objectifs versus scénario d'attaque

Si on recherche l'objectif de l'authenticité ou de l'intégrité, alors nécessairement notre hypothèse de raisonnement est celle d'une attaque active.

Si on recherche l'objectif de la confidentialité, on peut réfléchir soit à une attaque passive, soit à une attaque active.

Les primitives cryptographiques

Algorithmes fournissant une fonctionnalité cryptographique élémentaire

- contrôle d'intégrité $\longrightarrow$ fonction de hachage
- génération de clés $\longrightarrow$ générateur d'aléa
- authentification $\longrightarrow$ code d'authentification de message, algorithme de signature
- confidentialité $\longrightarrow$ chiffrement

Plan

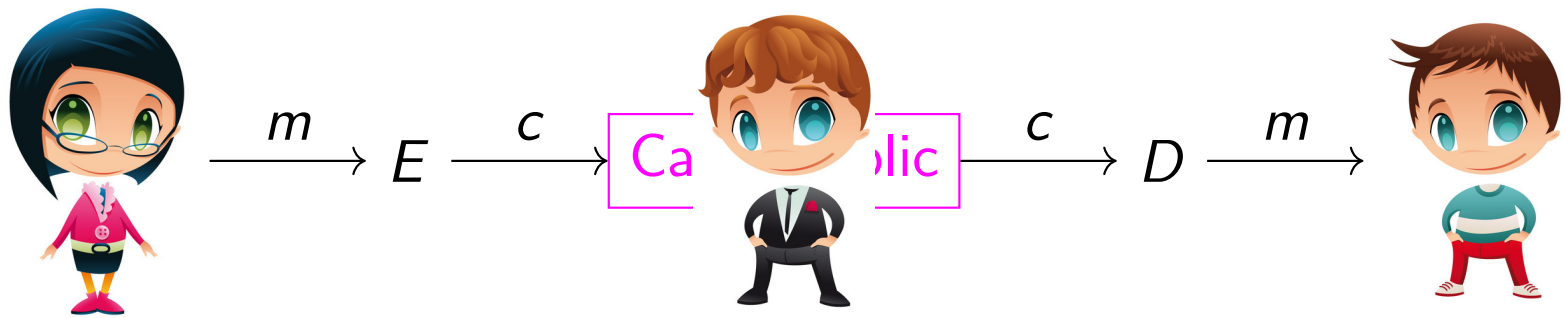
Cryptographie symétrique / asymétrique

Quand on cherche la confidentialité

- D se déduit facilement de $E \Rightarrow$ crypto symétrique
- D **ne** se déduit **pas** facilement de $E \Rightarrow$ crypto asymétrique

Cryptographie symétrique / asymétrique

Quand on cherche la confidentialité



- D se déduit facilement de E $\Rightarrow$ crypto symétrique
- D **ne** se déduit **pas** facilement de E $\Rightarrow$ crypto asymétrique

Cryptographie symétrique / asymétrique

Quand on cherche l'authenticité

- A se déduit facilement de $V \Rightarrow$ crypto symétrique
- A **ne** se déduit **pas** facilement de $V \Rightarrow$ crypto asymétrique

Cryptographie symétrique / asymétrique

Quand on cherche l'authenticité

- A se déduit facilement de $V \Rightarrow$ crypto symétrique
- A **ne** se déduit **pas** facilement de $V \Rightarrow$ crypto asymétrique

Les algorithmes cryptographiques

- Un algorithme :
  - est long à concevoir
  - doit être implanté sur du matériel
  - doit être transmis aux utilisateurs
  - doit être maintenu
- Confidentialité $\Rightarrow$ déchiffrement possible **seulement** par le récepteur
- Authentification $\Rightarrow$ authentifiant calculable **seulement** par l'émetteur
- Les algorithmes doivent-ils être secrets ?

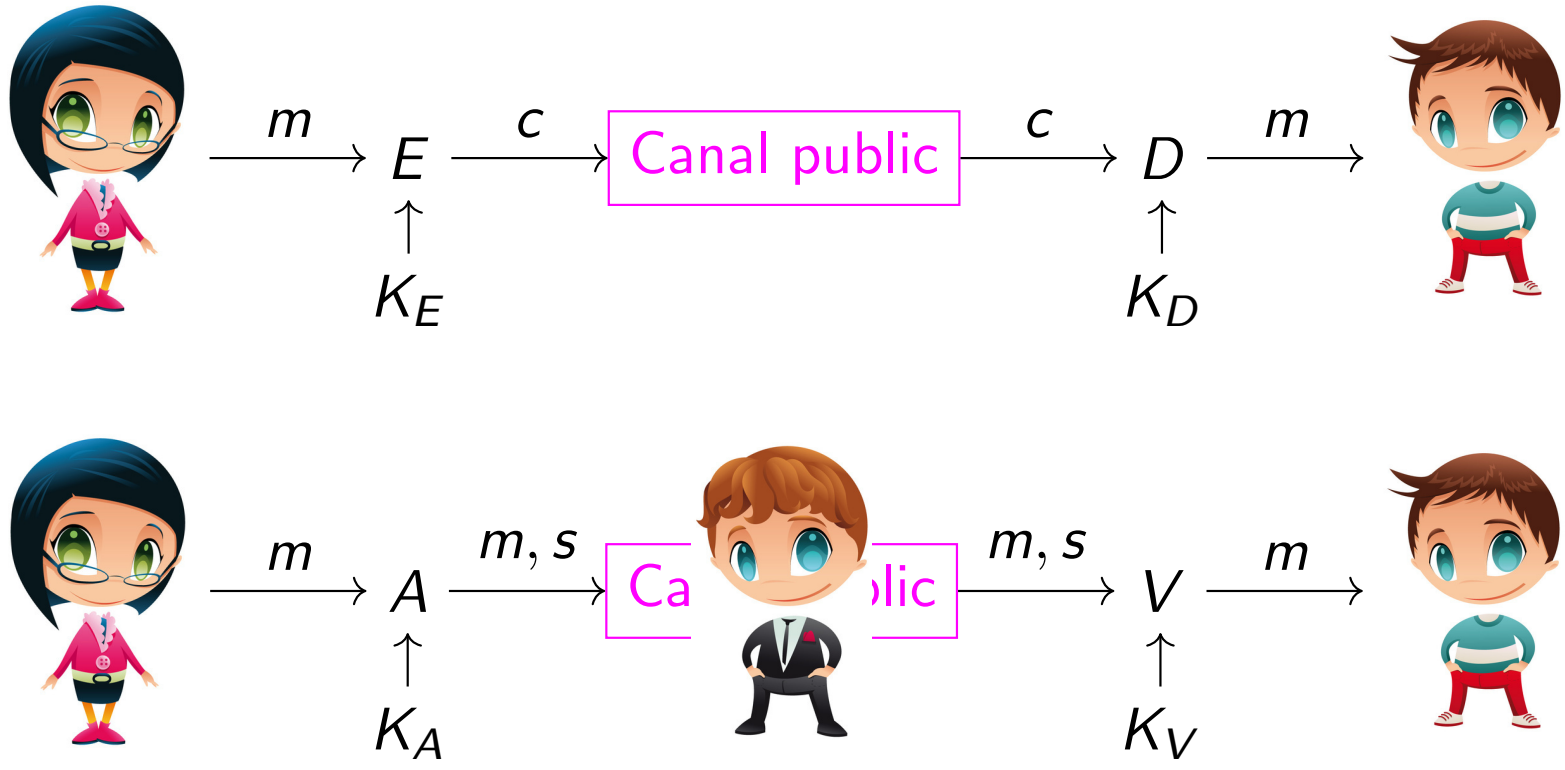
Les algorithmes cryptographiques

- Un algorithme :
  - est long à concevoir
  - doit être implanté sur du matériel
  - doit être transmis aux utilisateurs
  - doit être maintenu
- Confidentialité $\Rightarrow$ déchiffrement possible **seulement** par le récepteur
- Authentification $\Rightarrow$ authentifiant calculable **seulement** par l'émetteur
- Les algorithmes doivent-ils être secrets ?
  Si le secret tombe entre les mains de l'ennemi, c'est fichu.

Les desiderata de Kerckhoffs (1883)

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
2. Il faut qu'il **n'**exige **pas** le secret [...]
3. La clef doit pouvoir en être [...] retenue sans le secours de notes écrites, et être changée [...]
4. Il faut qu'il soit applicable à la correspondance télégraphique ;
5. Il faut qu'il soit portatif [...]
6. Enfin, il est nécessaire [...] que le système soit d'un usage facile, [...]

Cryptographie avec clé

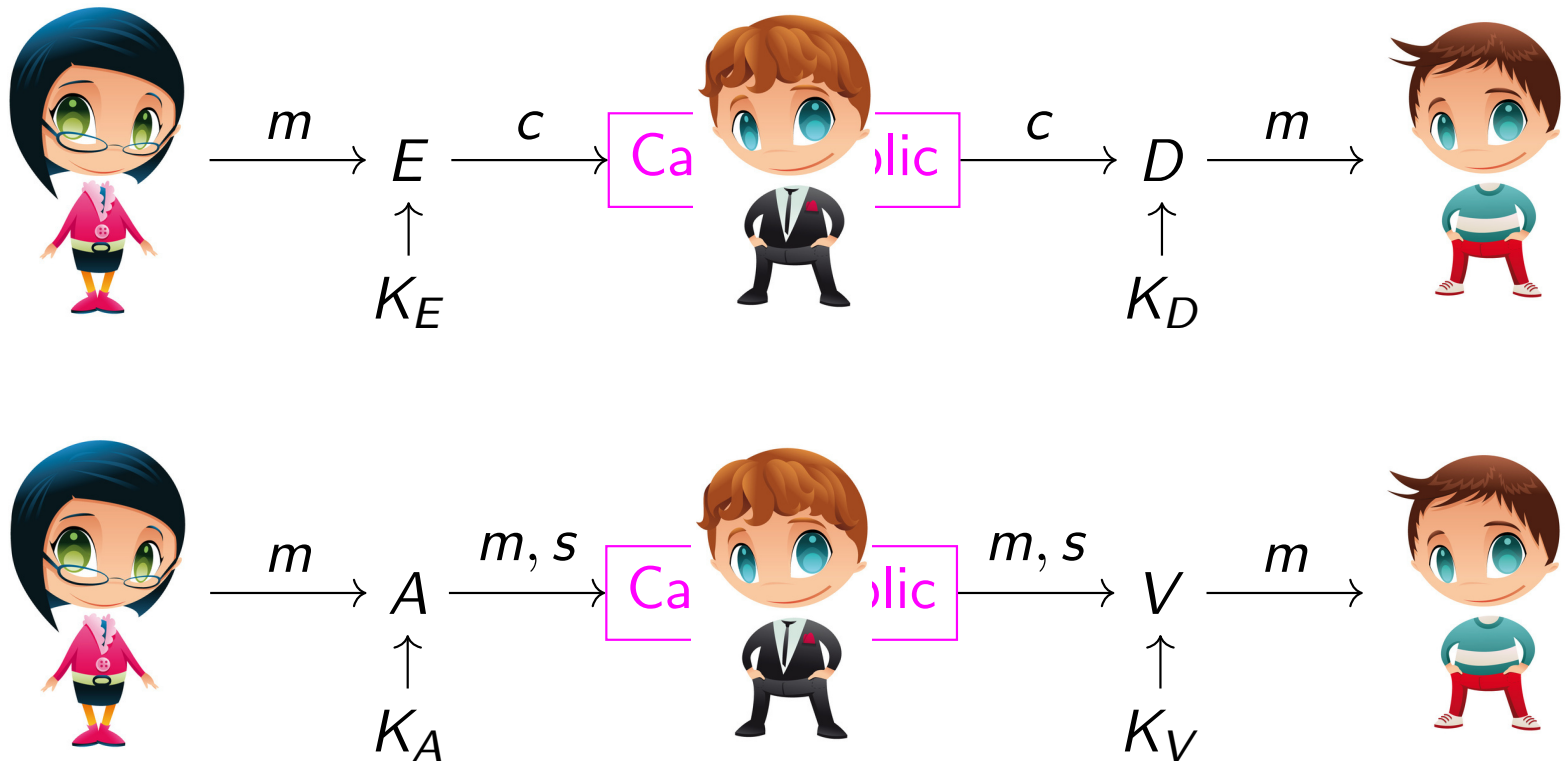


- $D = E$ et $K_D = K_E$ (resp $A = V$ et $K_A = K_V$) : crypto symétrique
- Sinon, clés potentiellement distinctes : $\Rightarrow$ crypto asymétrique

Cryptographie avec clé

- $D = E$ et $K_D = K_E$ (resp $A = V$ et $K_A = K_V$) : crypto symétrique
- Sinon, clés potentiellement distinctes : $\Rightarrow$ crypto asymétrique

Cryptographie avec clé



- $D = E$ et $K_D = K_E$ (resp $A = V$ et $K_A = K_V$) : crypto symétrique
- Sinon, clés potentiellement distinctes : $\Rightarrow$ crypto asymétrique

Retour sur le modèle de communication

Différents types de canaux de communications :

- public (ni authentifié ni confidentiel) — ex. Internet [universel]
- authentifié — ex. (partiellement) le réseau téléphonique [voix]
- confidentiel — ex. le réseau postal [loi]
- authentifié et confidentiel — ex. le téléphone rouge [dédié]

Sécurité, disponibilité, débit, coût variables

Intervention de la cryptographie

Construire des canaux authentifiés et/ou confidentiels à partir

- d'un canal public et
- d'un canal authentifié et/ou confidentiel

Utilisation différente et/ou asynchrone des canaux $\Rightarrow$ souplesse d'utilisation, nouvelles fonctionnalités, *etc.*

Exemple : améliorer un canal authentifié

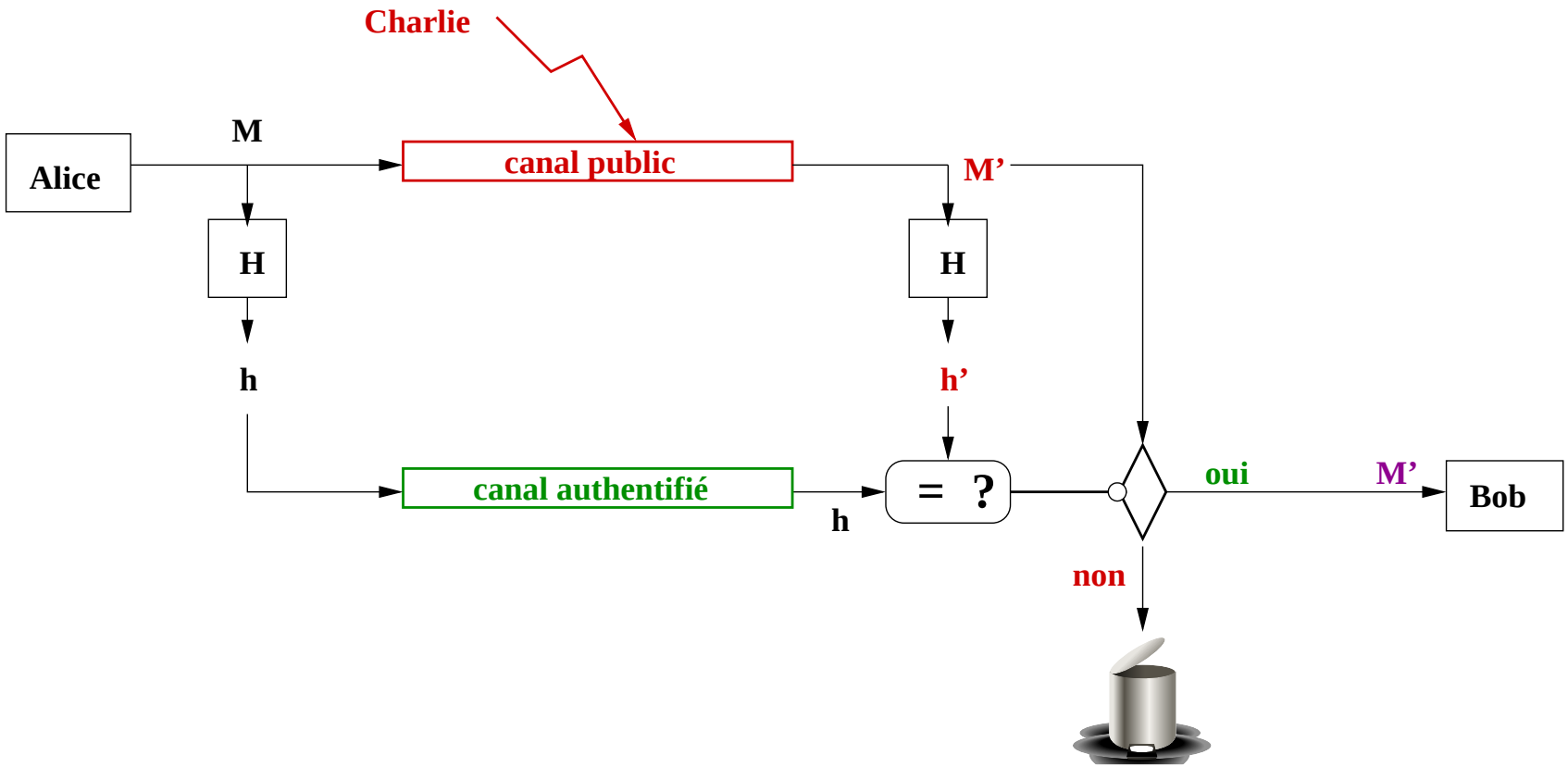
Contrôle d'intégrité avec fonction de hachage

- Un canal public pour transmettre des messages de grande taille
- Un canal authentifié pour transmettre un contrôle d'intégrité de petite taille

Définition (partielle)

Une fonction de hachage est un algorithme (efficace) qui calcule une valeur de taille fixe, appelée empreinte ou haché, à partir de messages de taille quelconque.

Améliorer un canal authentifié



- On utilise le canal authentifié après la création du message
- Exemple "folklorique" : juste un autre canal pour transmettre h ; "Charlie n'est pas partout".

Modèle d'attaques

- Pour que H soit qualifié de cryptographique, il faut que H résiste aux attaques par calcul de
  - premier antécédent :
    étant donné y il est difficile de trouver x tel que $y = H(x)$
  - deuxième antécédent :
    étant donné $(x, H(x))$ il est difficile de trouver x' tel que $H(x') = H(x)$
  - collision :
    il est difficile de trouver x et x' tels que $H(x') = H(x)$
- La pertinence des modèles d'attaques dépend des applications.

Créer un canal authentifié (I)

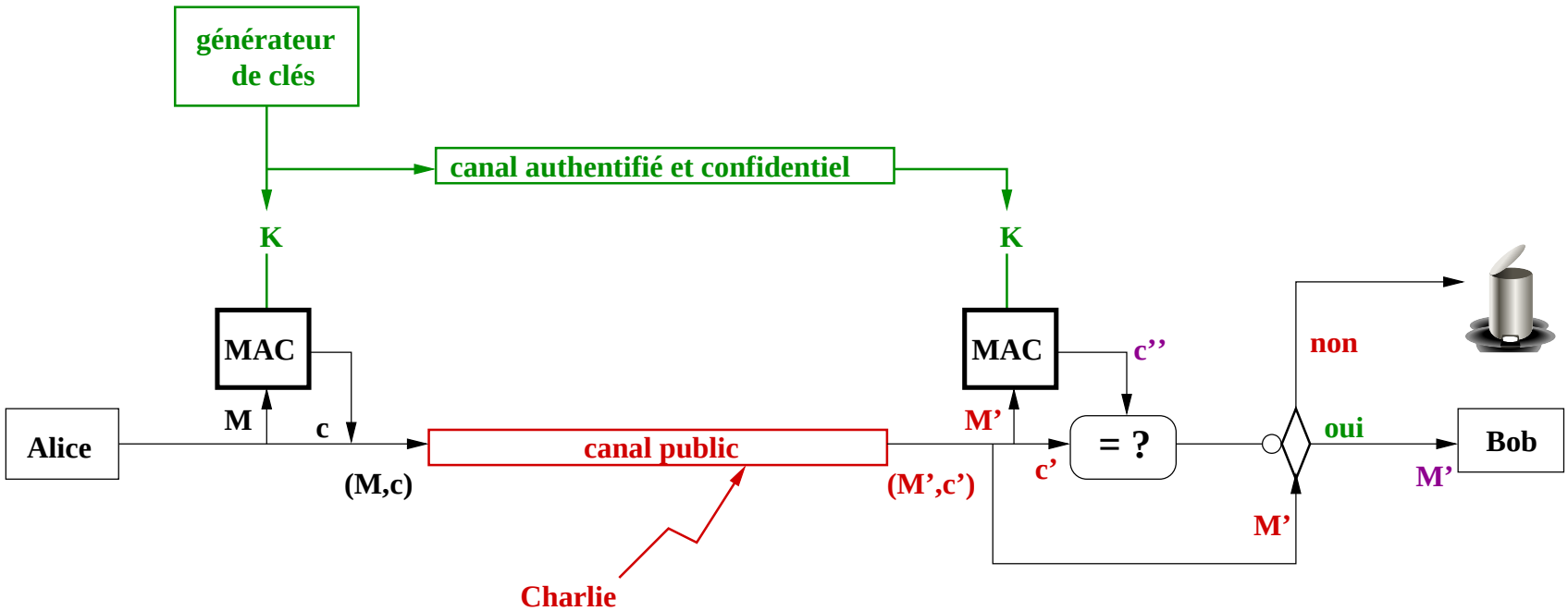
Symétrique : code d'authentification de messages (MAC)

- Un canal public pour transmettre des messages et leur code d'authentification
- Un canal authentifié et confidentiel pour transmettre la clé secrète

Définition (partielle)

Un code d'authentification de message (MAC) est un algorithme qui calcule une valeur de taille fixe, appelée (aussi) MAC, à partir de messages de taille quelconque et d'une clé secrète partagée entre émetteur et récepteur.

Créer un canal authentifié (I)



- On utilise le canal authentifié et confidentiel préalablement au message
- Exemple évident : pratiquement tous les protocoles Internet avec un peu de sécurité.

Modèle d'attaques

- Connaissant certains couples (M, c), un attaquant ne doit pas pouvoir
  - retrouver la clé secrète K
  - créer un nouveau couple (M', c') valide sans connaître la clé secrète K
  - distinguer l'algorithme de MAC d'une fonction aléatoire
- Le contrôle d'intégrité est assuré sur le canal public par l'authentification de l'origine des messages.

Les MAC sont un outil fondamental, et parfois assez subtil à mettre en œuvre. Il y a des pièges.

Créer un canal authentifié (II)

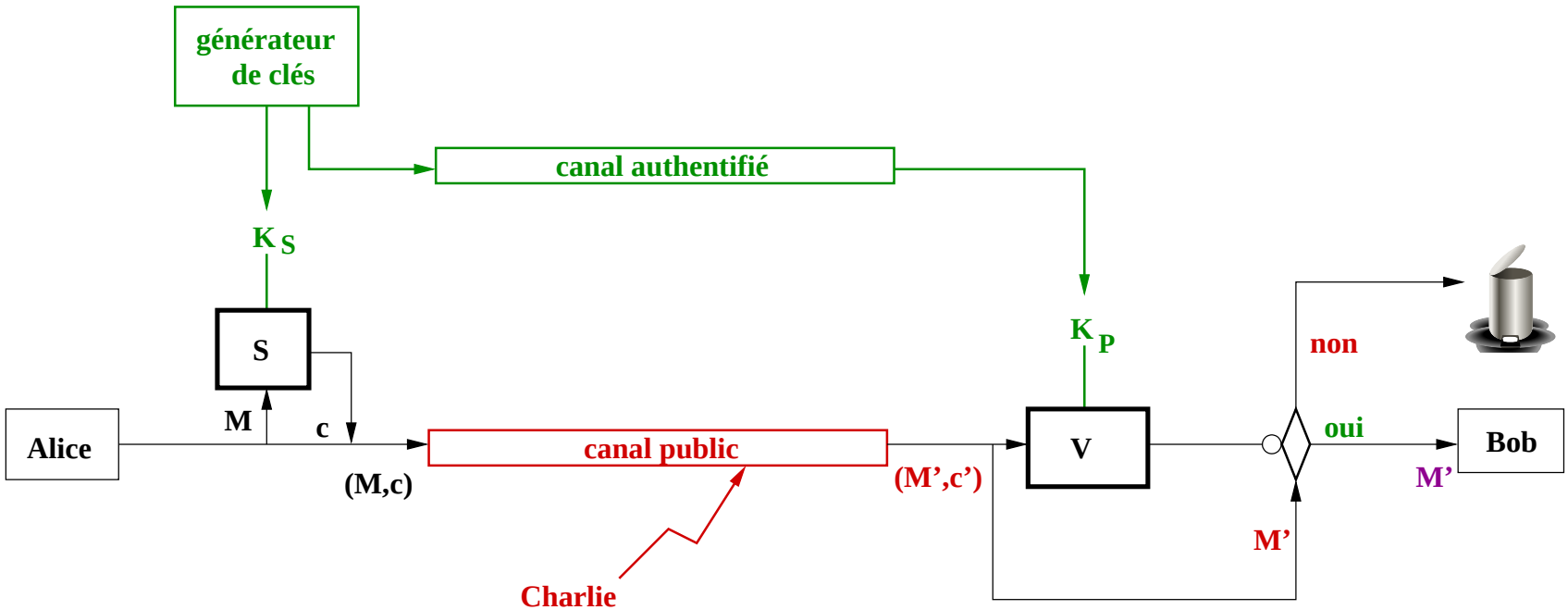
Asymétrique : un algorithme de signature

- Un canal public pour transmettre des messages et leur signature
- Un canal authentifié pour transmettre la clé publique

Définition (partielle)

Un algorithme de signature calcule une valeur appelée signature, usuellement de taille fixe, à partir de messages de taille quelconque et de la clé privée de l'émetteur. La vérification par le récepteur se fait grâce à la clé publique de l'émetteur.

Créer un canal authentifié (II)



- On utilise le canal authentifié préalablement au message
- La clé de signature K_S ne transite pas. Elle est propre à Alice.

Modèle d'attaques

- Connaissant certains couples (M, c) et la clé publique K_P, un attaquant ne doit pas pouvoir
  - retrouver la clé privée K_S
  - créer un nouveau couple (M', c') valide sans connaître la clé privée K_S
  - distinguer l'algorithme de signature d'une fonction aléatoire
- Le contrôle d'intégrité est assuré sur le canal public par l'authentification de l'origine des messages.

Authentification/Signature

- L'authentification permet de répondre à la question :

  Qui a émis le message ?

  Mais qui pose la question ?
- MAC : l'autre possesseur de la clé secrète $\Rightarrow$ 1 personne
  2 personnes peuvent calculer l'authentifiant
- Signature : un possesseur de la clé publique $\Rightarrow$ tout le monde
  Une seule personne peut calculer l'authentifiant $\Rightarrow$
  non-répudiation

Seule la solution de crypto asymétrique permet la non-répudiation et des signatures vérifiables par des tiers.

Créer un canal confidentiel (I)

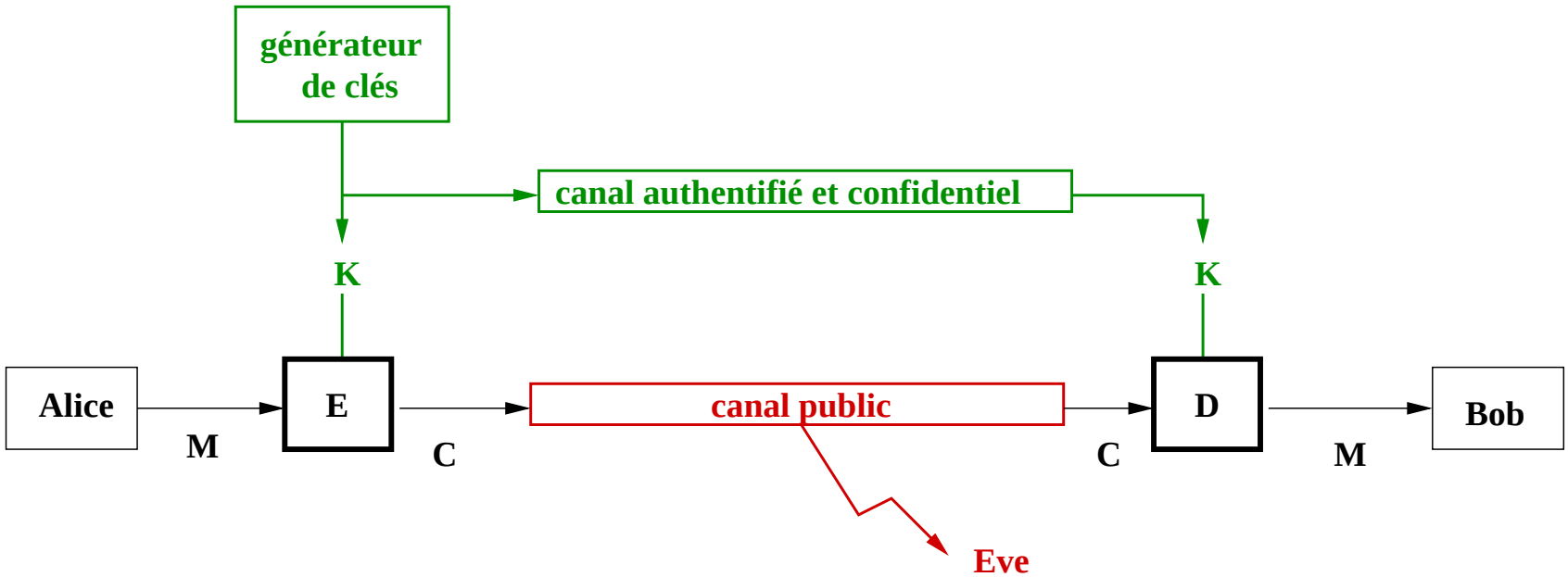
Symétrique : un chiffrement à clé secrète

- Un canal public pour transmettre des messages chiffrés
- Un canal authentifié et confidentiel pour transmettre la clé secrète

Définition (partielle)

Un chiffrement à clé secrète, E, est un algorithme paramétré par une chaîne binaire secrète, K, partagée entre deux entités qui transforme un message clair M en un message chiffré C. Le déchiffrement associé, D, utilise le même paramètre K.

Créer un canal confidentiel (I)



- On a besoin du canal authentifié et confidentiel au préalable de l'envoi d'un nombre élevé de messages

Modèle d'attaques

- Connaissant certains couples (M, C) et un chiffré C_0, un attaquant ne doit pas pouvoir
  - retrouver la clé secrète K
  - retrouver le clair M_0 correspondant à C_0 sans connaître la clé secrète K
  - distinguer C_0 d'une suite aléatoire ($\Rightarrow$ randomisation)
- Attention : chiffrer $\neq$ authentifier (ce n'est pas le même modèle de sécurité)

Créer un canal confidentiel (II)

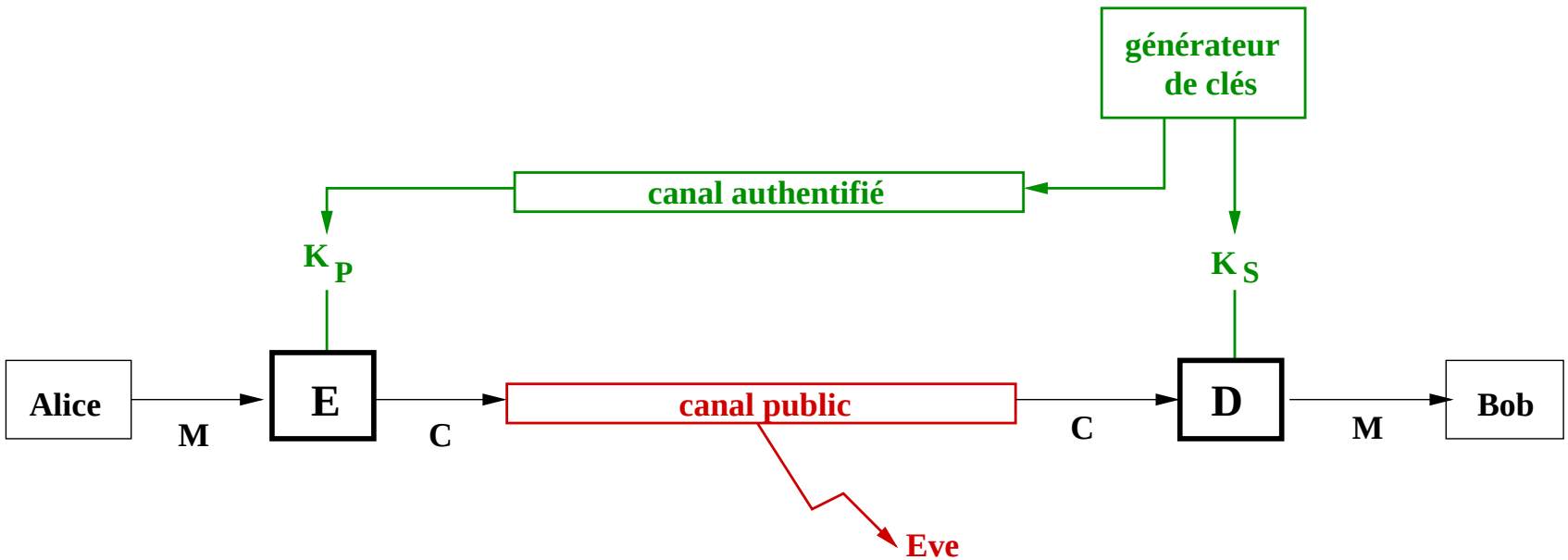
Asymétrique : utiliser un chiffrement à clé publique

- Un canal public pour transmettre des messages chiffrés
- Un canal authentifié pour transmettre la clé publique

Définition (partielle)

Un chiffrement à clé publique, E, est un algorithme paramétré par une chaîne binaire publique, K_P, connue de tous qui transforme un message clair M en un message chiffré C. Le déchiffrement associé D utilise un paramètre privé K_S.

Créer un canal confidentiel (II)



- On a besoin du canal authentifié une fois au préalable

Modèle d'attaques

- Connaissant certains couples (M, C), un chiffré C_0, et la clé publique K_P, un attaquant ne doit pas pouvoir
  - retrouver la clé privée K_S
  - retrouver le clair M_0 correspondant à C_0 sans connaître la clé privée K_S
  - distinguer C_0 d'une suite aléatoire ($\Rightarrow$ randomisation)
- Attention : chiffrer $\neq$ authentifier (ce n'est pas le même modèle de sécurité)

Au fait : pourquoi veut-on un canal authentifié ?

Chiffrement à clé secrète : le coffre-fort

- Alice et Bob ont la clé du coffre
- Alice envoie un message à Bob
  1. Alice utilise la clé pour déposer un courrier dans le coffre ;
  2. Bob utilise la clé pour lire le courrier déposé par Alice.
- Propriétés du coffre-fort
  - seuls Alice et Bob peuvent déposer du courrier dans le coffre ;
  - seuls Alice et Bob peuvent retirer le courrier déposé dans le coffre.

Chiffrement à clé publique : la boîte aux lettres

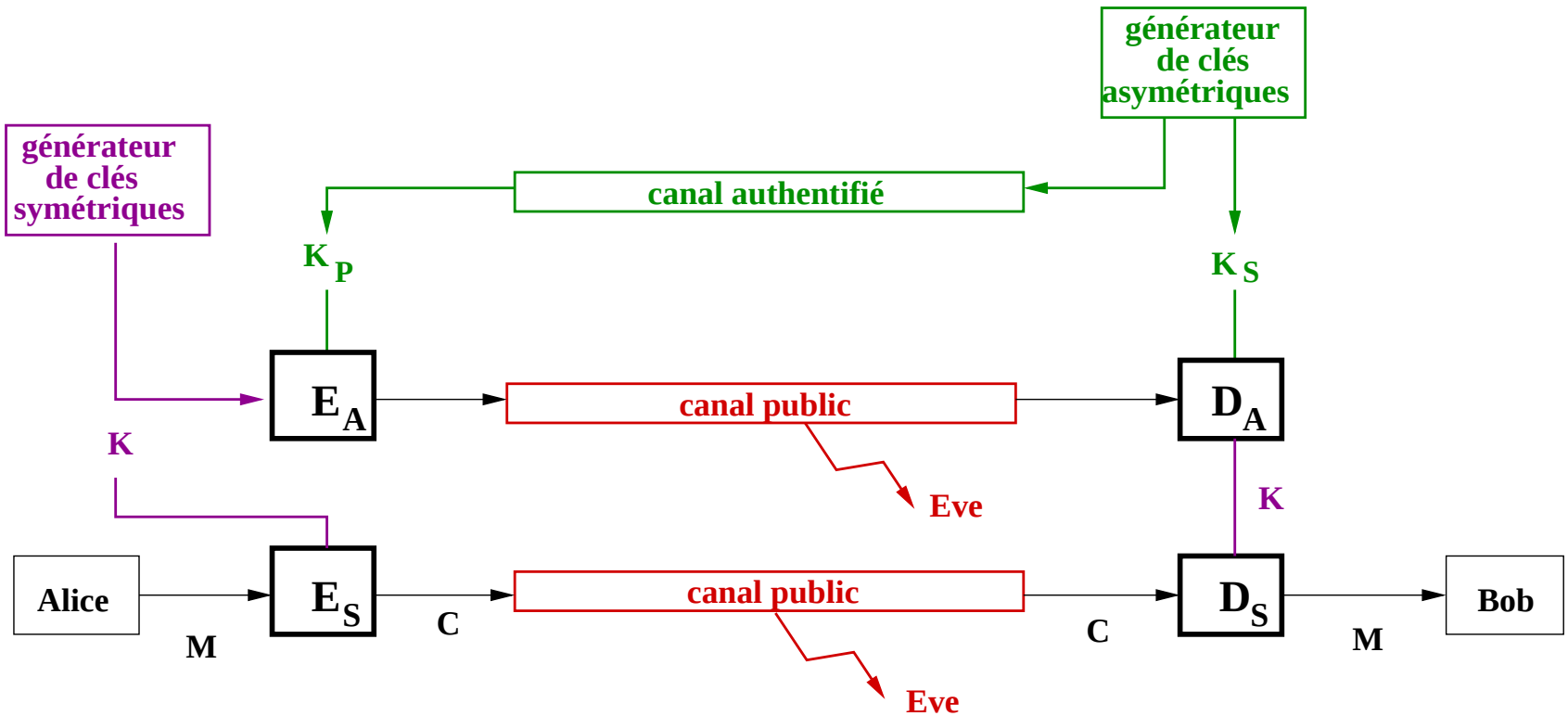
- Seul Bob a la clé de sa boîte
- Alice obtient l'adresse de Bob dans un annuaire
- Alice envoie un message à Bob
  1. Alice dépose un courrier dans la boîte de Bob ;
  2. Bob utilise sa clé pour retirer le courrier déposé dans sa boîte.
- Propriétés de la boîte aux lettres
  - tout le monde peut envoyer du courrier à Bob ;
  - seul Bob peut lire le courrier déposé dans sa boîte aux lettres.

Algorithmes à clé secrète / à clé publique

	clé secrète	**clé publique**
gestion	la clé est secrète aux deux extrémités canal auxiliaire authentifié et confidentiel	seule la clé privée est secrète canal auxiliaire authentifié
sécurité	pas de preuve formelle de sécurité	repose sur la difficulté supposée de problèmes mathématiques
taille clé	ex. AES : 128 bits	ex. RSA : 3072 bits
perf.	très rapides 10-100 Mbits/s (software)	très lents 10-100 Kbits/s

Créer un canal confidentiel (III)

Utiliser un système hybride



Canal confidentiel

Le schéma précédent est pratiquement universel (SSL, IPSEC, SSH, . . .).

- Alice et Bob doivent d'abord s'entendre sur les algorithmes de crypto qu'ils vont utiliser (suite cryptographique).
- Divers mécanismes sont utilisés pour l'authentification initiale.
- Une phase d'échange de clé emploie d'abord un système asymétrique. Alice et Bob en déduisent une clé de session.
- La clé de session est utilisée pour chiffrer la suite des échanges.
- Selon le protocole, des renégociations de clé de session peuvent intervenir périodiquement.

Quelques leçons de l'histoire

- Les desiderata de Kerckhoffs : la sécurité ne doit pas reposer sur le secret des spécifications
- La loi de Moore : la puissance des processeurs double tous les 18 mois, gare à la recherche exhaustive
- La loi de Murphy : un trou de sécurité finira toujours par être découvert... au pire moment
- Le principe de réalité : un procédé inadapté (cher, contraignant, lent, etc.) ne sera pas utilisé
- Ne pas réinventer la roue : utiliser un standard / une librairie existante plutôt que faire son propre algorithme cryptographique (surtout si on n'est pas expert...)