

TIW4 : SÉCURITÉ DES SYSTÈMES D'INFORMATION

INTRODUCTION À LA CRYPTOGRAPHIE

romuald.thion@univ-lyon1.fr

<http://liris.cnrs.fr/~rthion/dokuwiki/enseignement:tiw4>



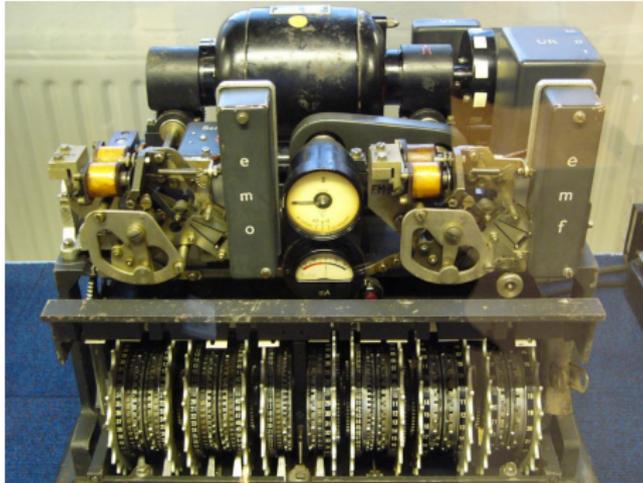
Master « Technologies de l'Information »

- 1 Introduction
- 2 Briques cryptographiques de base
 - Fonctions de hachage
 - Chiffrement symétrique
 - Chiffrement asymétrique
- 3 Cryptanalyse et preuve de sécurité
 - Problèmes difficiles
 - Modèles de l'attaquant

Objectifs

- bases cryptographiques
- intérêts et usage des protocoles cryptographique
- techniques d'authentification et limites des mots de passes

Activité



Quelle est cette machine ?

Vocabulaire

Cryptologie la science du secret

Cryptographie la branche de la cryptologie qui s'intéresse à la **conception** des écritures secrètes

Cryptanalyse la branche de la cryptologie qui s'intéresse à l'**analyse** des écritures secrètes

Texte clair information dont la confidentialité n'est **pas protégée**

Text chiffré information protégée (†)

Clef **paramètre secret** d'un algorithme cryptographique

Protocole Protocole qui **garantit des fonctions de sécurité** via l'utilisation de primitives cryptographiques.

La cryptographie et la cryptanalyse sont deux domaines antagonistes

Vocabulaire

Cryptologie la science du secret

Cryptographie la branche de la cryptologie qui s'intéresse à la **conception** des écritures secrètes

Cryptanalyse la branche de la cryptologie qui s'intéresse à l'**analyse** des écritures secrètes

Texte clair information dont la confidentialité n'est **pas protégée**

Text chiffré information protégée (†)

Clef **paramètre secret** d'un algorithme cryptographique

Protocole Protocole qui **garantit des fonctions de sécurité** via l'utilisation de primitives cryptographiques.

La cryptographie et la cryptanalyse sont deux domaines antagonistes

Buts principaux de la cryptographie

Principaux critères de sécurité – CIA

Confidentialité Seuls les utilisateurs légitimes ont accès à l'information/services

Intégrité Les informations/services ne sont pas altérées

Availability Les informations/services

Plus spécifiques en cryptographie

Authenticité On communique bien à la bonne personne

Non-répudiation On ne peut pas nier sa participation

Cryptographie et sécurité au sens large

- D'autres mécanismes participent **également** à ces fonctions
- l'usage de la cryptographie **seule** est inutile !

- 1 Introduction
- 2 Briques cryptographiques de base
 - Fonctions de hachage
 - Chiffrement symétrique
 - Chiffrement asymétrique
- 3 Cryptanalyse et preuve de sécurité
 - Problèmes difficiles
 - Modèles de l'attaquant

- 1 Introduction
- 2 Briques cryptographiques de base
 - Fonctions de hachage
 - Chiffrement symétrique
 - Chiffrement asymétrique
- 3 Cryptanalyse et preuve de sécurité
 - Problèmes difficiles
 - Modèles de l'attaquant

Fonctions de hachage

Principe

Hacher \cong calculer une **empreinte** cryptographique

Caractéristiques d'une fonction de hachage *cryptographique*

Résistance aux collisions impossible (en pratique) de trouver m et m' différents tels que $h(m) = h(m')$

Résistante à la première préimage connaissant d , il est impossible (en pratique) de trouver m t.q. $d = h(m)$

Résistante à la seconde préimage connaissant m , il est impossible (en pratique) de trouver m' différent de m t.q. $h(m) = h(m')$

Efficacité le calcul de $h(m)$ doit être fait efficacement

Question : que signifie *en pratique* ?

Fonctions de hachage

Principe

Hacher \cong calculer une **empreinte** cryptographique

Caractéristiques d'une fonction de hachage *cryptographique*

Résistance aux collisions impossible (en pratique) de trouver m et m' différents tels que $h(m) = h(m')$

Résistante à la première préimage connaissant d , il est impossible (en pratique) de trouver m t.q. $d = h(m)$

Résistante à la seconde préimage connaissant m , il est impossible (en pratique) de trouver m' différent de m t.q. $h(m) = h(m')$

Efficacité le calcul de $h(m)$ doit être fait efficacement

Question : que signifie *en pratique*?

Application du hachage

Principaux usages

- **Compresser** de grande quantité de données
pour la signature (éviter de signer un trop gros objet)
- Chiffrer « **sans clef** » (et pouvoir comparer les chiffrés)
stockage de mots de passe (détaillé dans un autre cours)
- Assurer l'**intégrité** d'un message
résumés md5 ou sha d'une image Linux
- Produire un **identifiant unique** d'une donnée
protocole pairs-à-pairs/DHT ou (pseudo-)identifiants des objets dans les langages de programmation (pour accélérer le test d'égalité).

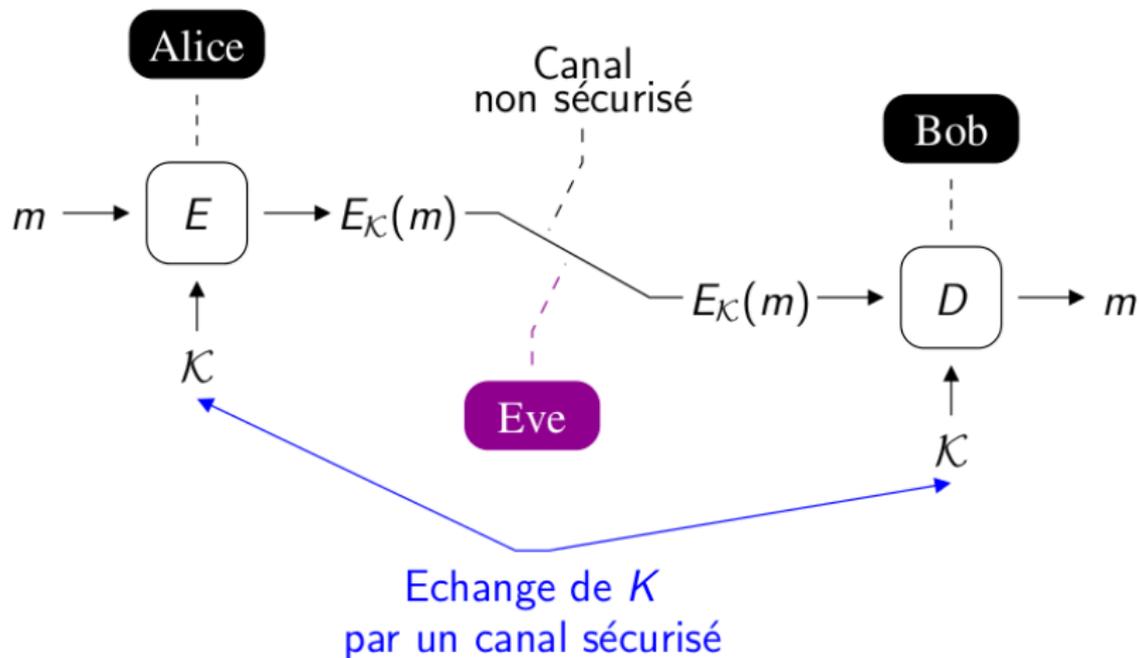
Fonctions de hachage

Fonctions de hachage courantes :

- MD4 (Rivest, 1990, collisions trouvées en 1995, attaques à la préimage en 2005)
- MD5 (Rivest, 1991, collisions trouvées en 2004, voir [MD5 considered harmful today](#))
- La famille des [Secure Hash Algorithms](#)
 - SHA-0, SHA-1 (NIST, 1993, collisions possibles)
 - SHA-256/224, SHA-512/384 (considérés comme sûrs)
 - [SHA-3](#) (lauréat concours 2015)

- 1 Introduction
- 2 Briques cryptographiques de base
 - Fonctions de hachage
 - Chiffrement symétrique
 - Chiffrement asymétrique
- 3 Cryptanalyse et preuve de sécurité
 - Problèmes difficiles
 - Modèles de l'attaquant

Chiffrement symétrique



Chiffrement symétrique

Canaux auxiliaire

Un secret est **partagé entre les participants**, via un canal auxiliaire *réputé^a sûr* :

- par téléphone/SMS
- par courrier classique
- par email
- par rencontre physique

a. Pas forcément très sûr en lui-même, mais que l'on considère comme tel !

Exemple d'utilisation d'un canal auxiliaire

2-step verification : lors de l'authentification depuis un nouveau service, un code de confirmation envoyé par SMS doit être saisi.

Chiffrement symétrique

Chiffrement par flux (*stream*, bit à bit)

- RC4 : utilisé dans SSL et WEP, très rapide et simple, mais vulnérable
- eSTREAM : famille de chiffrements, projet de 2004 à 2008

Chiffrement par blocs de k bits

- DES : utilisé de 1977 à 2004 clef de 56 bits, bloc de 64 bits (voir [Chronologie](#))
- Triple DES : encore utilisé (variante avec clefs de 112 ou 168 bits)
- AES : standard américain (concours international), rapide et sûr, clef de 128, 192 ou 256 bits, blocs de 128 bits
- IDEA : breveté (jusqu'en 2011), clefs de 128 bitsn blocs de 64 bits

Chiffrement symétrique en flux

One-Time Pad (Vernam Cipher)

- $m \in \mathcal{M} = \{0, 1\}^L$ un message clair (de longueur L bits)
- $k \in \mathcal{K} = \{0, 1\}^L$ une clef (de longueur L bits)
- $c \in \mathcal{C} = \{0, 1\}^L$ un message chiffré (de longueur L bits)
- $E_k(m)$ la fonction de chiffrement (paramétrée par k)
- $D_k(m)$ la fonction de déchiffrement (paramétrée par k)

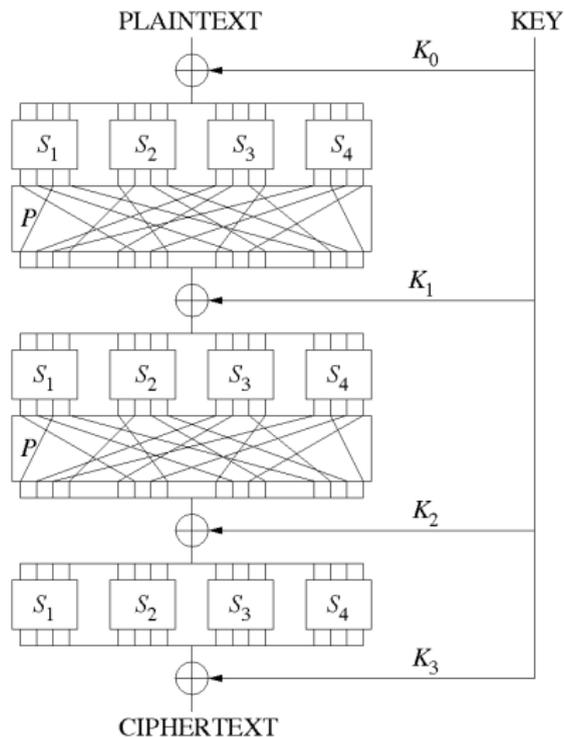
$$c = E_k(m) = k \oplus m \text{ (le ou exclusif bit à bit)}$$

$$m = D_k(c) = k \oplus c \text{ (le ou exclusif bit à bit)}$$

$$D_k(E_k(m)) = k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0^L \oplus m = m$$

Remarque : ici $E_k = D_k$ mais ce n'est pas toujours le cas.

Chiffrement symétrique par blocs



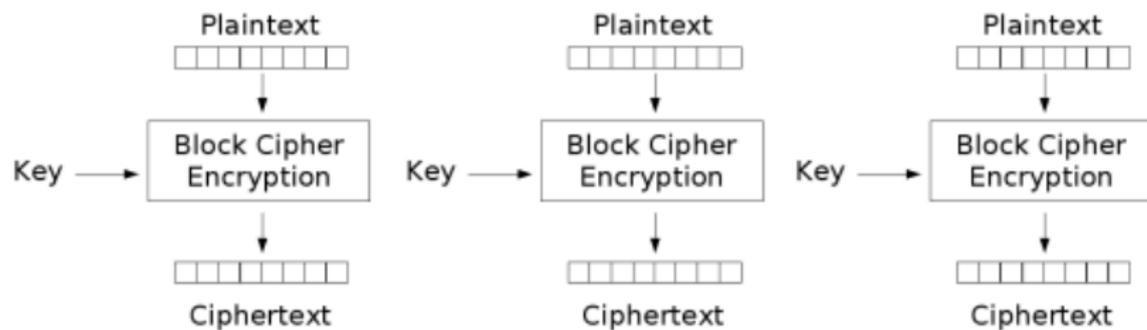
Substitution-permutation network

Chiffrement par blocs

Question : comment faire pour chiffrer des textes de tailles supérieures à celle des blocs ?

Modes de d'opérations

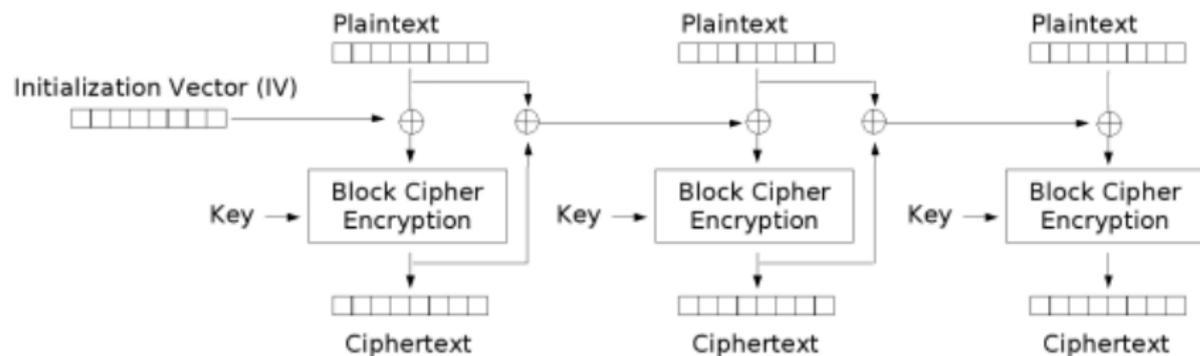
Electronic Code Block (EBC)



Electronic Codebook (ECB) mode encryption

Modes de chiffrement

Cipher Block Chaining (CBC)



Propagating Cipher Block Chaining (PCBC) mode encryption

Chiffrement symétrique

Autres modes d'opération

[Block cipher mode of operation](#) (Wikipedia) pour d'autres exemples :

PCBC Propagating cipher block chaining

CFB Cipher feedback

OFB Output feedback

CTR Counter

GCM Galois/Counter

Critères : simplicité, nécessité IV, parallélisation, effet cascade, attaque par rejeux

Exemple PostgreSQL

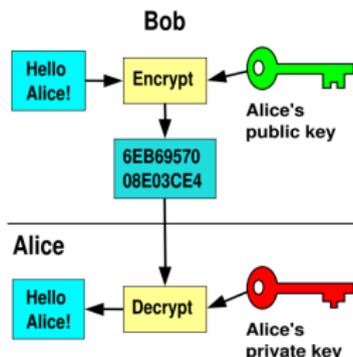
[The difference in five modes in the AES encryption algorithm](#) (pas de GCM)

- 1 Introduction
- 2 Briques cryptographiques de base
 - Fonctions de hachage
 - Chiffrement symétrique
 - Chiffrement asymétrique
- 3 Cryptanalyse et preuve de sécurité
 - Problèmes difficiles
 - Modèles de l'attaquant

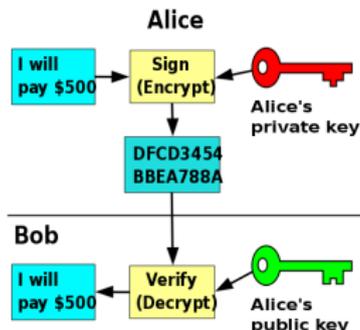
Chiffrement asymétrique

- Plus de secret partagé mais une **paire** de clefs
 - une **privée**
 - une **publique**

Signature et chiffrement asymétrique ne diffèrent que de l'usage qui est fait des clefs publiques et privée d'Alice et Bob.



Chiffrement



Signature

- 1 Introduction
- 2 Briques cryptographiques de base
 - Fonctions de hachage
 - Chiffrement symétrique
 - Chiffrement asymétrique
- 3 **Cryptanalyse et preuve de sécurité**
 - **Problèmes difficiles**
 - **Modèles de l'attaquant**

- 1 Introduction
- 2 Briques cryptographiques de base
 - Fonctions de hachage
 - Chiffrement symétrique
 - Chiffrement asymétrique
- 3 Cryptanalyse et preuve de sécurité
 - Problèmes difficiles
 - Modèles de l'attaquant

Problèmes difficiles

Question (cs.stackexchange.com)

Given RSA, why do we not know if public-key cryptography is possible?

Réponse

We don't know for sure that RSA is safe. It could be that RSA can be broken in polynomial time, for example if factoring can be done efficiently. What is open is the existence of a provably secure public-key cryptosystem. We don't know for sure that such a cryptosystem exists at all; for all we know, every cryptosystem could be broken efficiently. [...]

Problèmes difficiles

Sécurité du système : difficulté du décryptage ^a

a. décrypter = tenter de déchiffrer sans connaître le secret

La **sécurité** des algorithmes (à clefs publiques ou secrète) reposent sur la **difficulté** (supposée . . .) de problèmes **combinatoires**.

Problèmes difficiles

Cryptosystème	Problème calculatoire
RSA	integer factorization problem
Rabin	square roots modulo composite n
ElGamal	discrete logarithm problem
Merkle-Hellman knapsack	subset sum problem

Voir [Handbook of Applied Cryptography – Ch8 Public-Key Encryption](#)

- 1 Introduction
- 2 Briques cryptographiques de base
 - Fonctions de hachage
 - Chiffrement symétrique
 - Chiffrement asymétrique
- 3 Cryptanalyse et preuve de sécurité
 - Problèmes difficiles
 - Modèles de l'attaquant

Modèles de l'attaquant

Modélisation de l'adversaire

- Que **sait-il**, qu'est-il **capable** de faire ?
- Quelle **nouvelle information** peut-il déduire ?
- De quelle **puissance** dispose-t-il ?
- À **quoi** s'attaque-t-il ?

La preuve de sécurité

- formalisation des hypothèses de confiance
- résultat **prouvé** mathématiquement (arithmétique, probabilités)
- *réduction* à un problème **supposé difficile** (†)

Modèles de l'attaquant

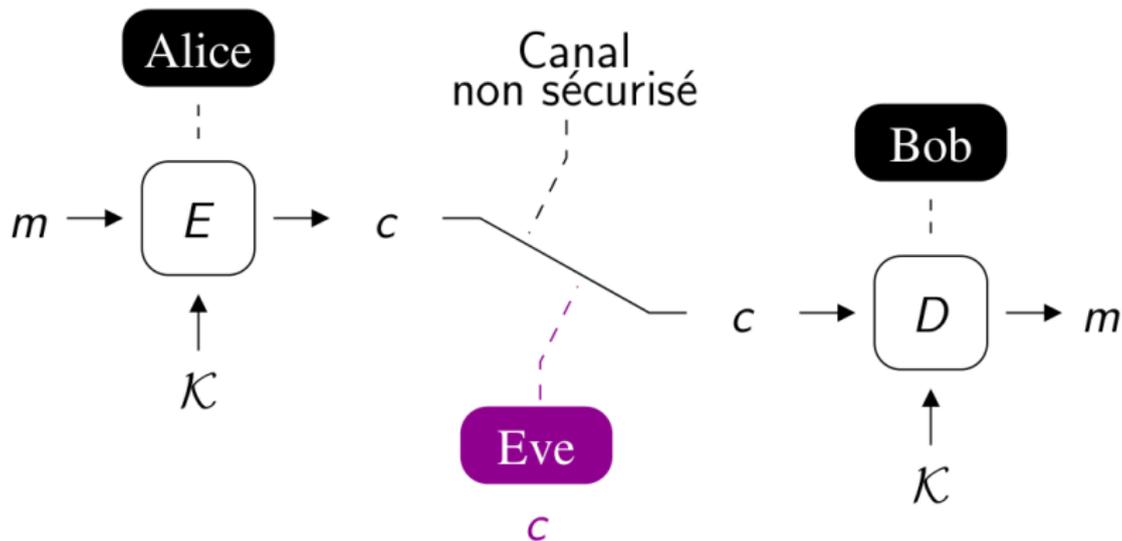
Modélisation de l'adversaire

- Que **sait-il**, qu'est-il **capable** de faire ?
- Quelle **nouvelle information** peut-il déduire ?
- De quelle **puissance** dispose-t-il ?
- À **quoi** s'attaque-t-il ?

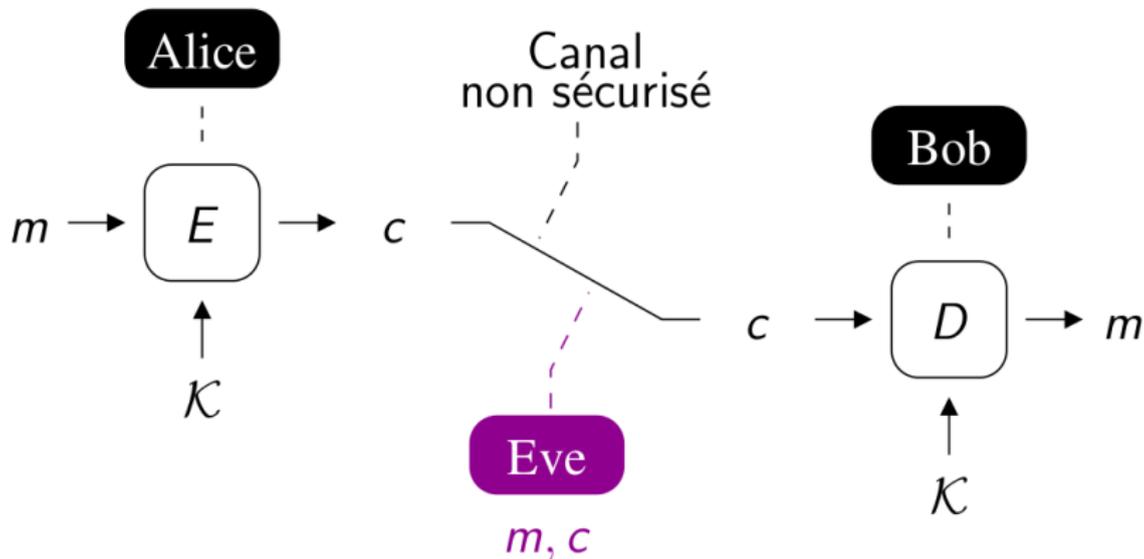
La preuve de sécurité

- formalisation des hypothèses de confiance
- résultat **prouvé** mathématiquement (arithmétique, probabilités)
- *réduction* à un problème **supposé difficile** (†)

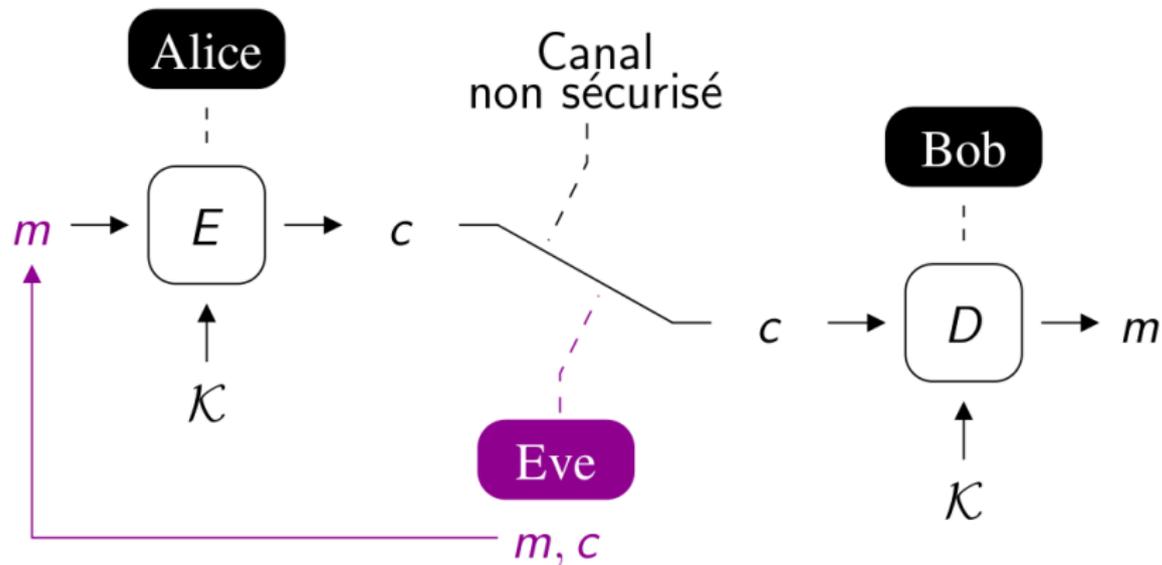
Attaque à chiffrés seuls (*ciphertext-only*)



Attaque à clairs connus (*known-plaintext*)



Attaque à clairs choisis (*chosen-plaintext*)



Modèles de l'attaquant

One-Time Pad avec réemploi de la clef

Dans le cas où k est réutilisée :

- OTP *résiste* à une attaque *ciphertext-only* : connaissant, $c = k \oplus m$, on ne peut pas retrouver m
- OTP *ne résiste pas* à une attaque *known-plaintext* : connaissant, $c = k \oplus m$, et m on ne peut pas retrouver $k = c \oplus m$ et donc déchiffrer $c' = k \oplus m$
- OTP *ne résiste pas* à une attaque *chosen-plaintext* : demander de chiffrer 0^L on obtient $c = k \oplus 0^L = k$

Par contre, si k est aléatoire et fraîche (nouvelle à chaque usage) alors OTP résiste^a.

a. il est même parfait en un sens technique