TIW4 : SÉCURITÉ DES SYSTÈMES D'INFORMATION

INTRODUCTION À LA CRYPTOGRAPHIE

romuald.thion@univ-lyon1.fr

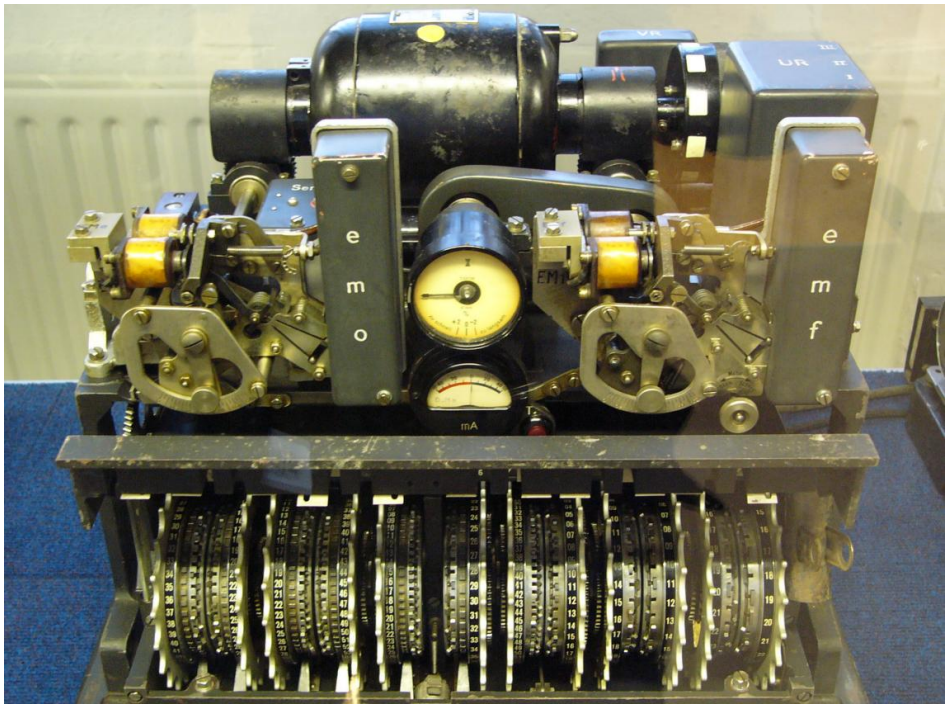
http://liris.cnrs.fr/~rthion/dokuwiki/enseignement:tiw4

Master « Technologies de l'Information »

Objectifs

- placer la cryptographie dans la sécurité
- bases cryptographiques
- intérêts et utilisation des protocoles cryptographique
- 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

Confidentialité Seuls les légitimes ont accès à l'information

Intégrité Le message n'a pas été altéré

Authenticité On communique bien à la bonne personne

Non-répudiation On ne peut pas nier sa participation

Cryptographie en sécurité

- D'autres mécanismes participent également à ces fonctions
- l'usage de la cryptographie seule est inutile . . .
- . . . mal employée, c'est pire encore ! (†)

Buts principaux de la cryptographie

Confidentialité Seuls les légitimes ont accès à l'information

Intégrité Le message n'a pas été altéré

Authenticité On communique bien à la bonne personne

Non-répudiation On ne peut pas nier sa participation

Cryptographie en sécurité

- D'autres mécanismes participent également à ces fonctions
- l'usage de la cryptographie seule est inutile . . .
- . . . mal employée, c'est pire encore ! (†)

1 Introduction

2 Briques cryptographiques de base
- Fonctions de hachage
- Cryptographie symétrique
- Cryptographie asymétrique

3 Cryptanalyse et preuve de sécurité
- Problèmes difficiles
- Modélisation
- Attaques

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

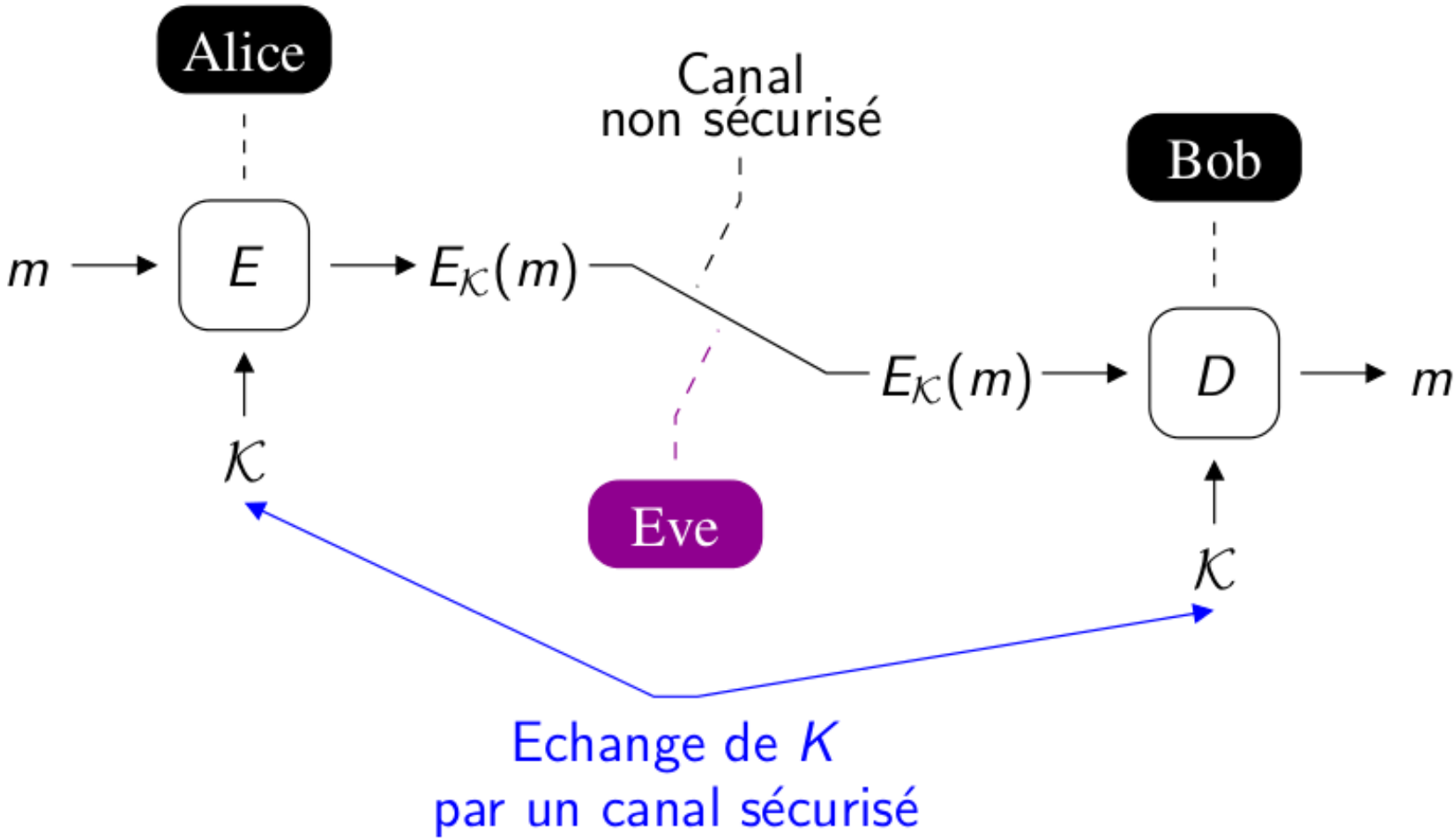
- Compresser de grande quantité de données
  pour la signature
- Chiffrer « sans clef » (et pouvoir comparer les chiffrés)
  stockage de mots de passe
- Assurer l'intégrité d'un message
  résumés md5
- Produire un identifiant unique d'une donnée
  protocole pairs-à-pairs/DHT

Fonctions de hachage

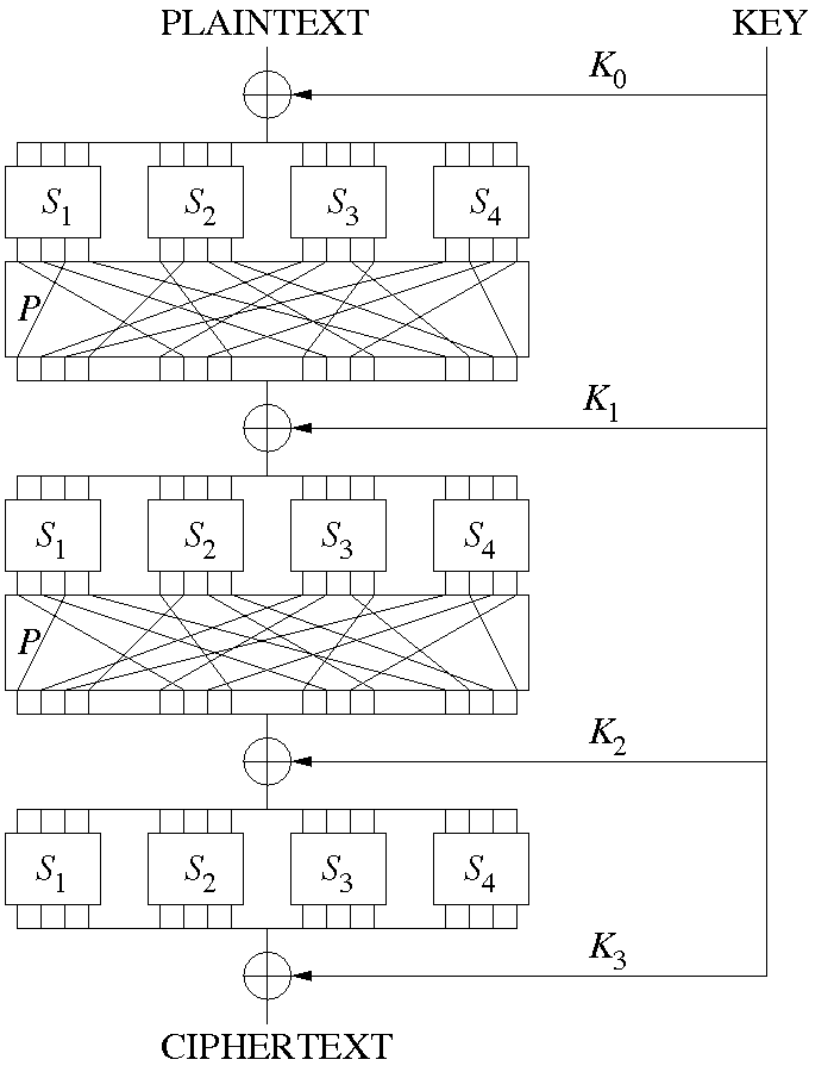
Fonctions de hachage courantes :

- MD4 (Rivest, 1990, collissions 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)

Cryptographie symétrique



Cryptographie symétrique



Substitution-permutation network

Cryptographie symétrique

Canaux auxilliaire

Un secret est partagé entre les participants, via un canal auxilliaire *réputé*[a] sûr :

- par téléphone/SMS
- par courier 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 auxilliaire

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

Cryptographie symétrique

Chiffrement par flux

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

Chiffrement par blocs

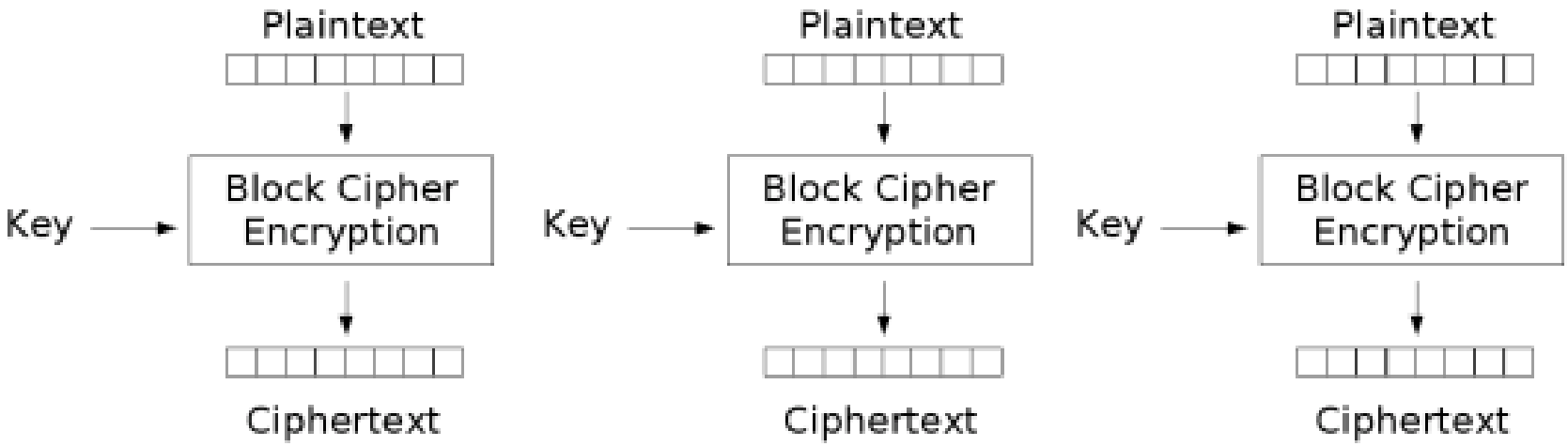
- DES : utilisé de 1977 à 2004 clef de 56 bits, bloc de 64 bits (voir Chronologie)
- Triple DES : encore utilisé (variante avec clefs de 112 ou 168 bits)
- AES : standard américain (concours international), rapide et sûr, clef de 128, 192 ou 256 bits, blocs de 128 bits
- IDEA : breveté (jusqu'en 2011),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

Chiffrement par blocs

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

Modes de chiffrement

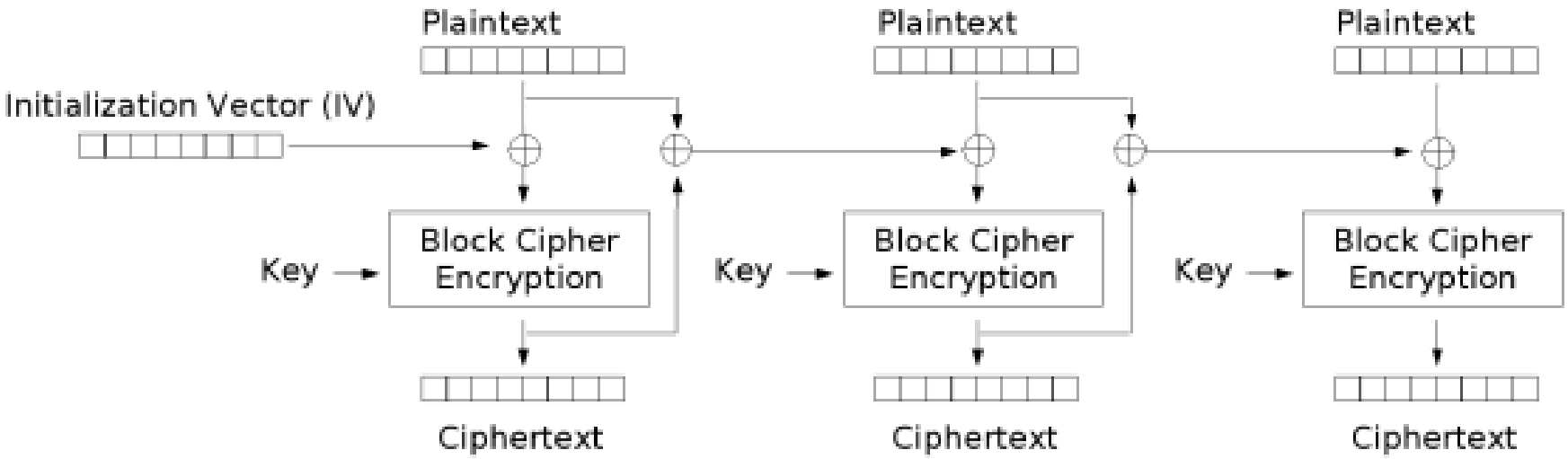
Electronic Code Block (EBC)



Electronic Codebook (ECB) mode encryption

Modes de chiffrement

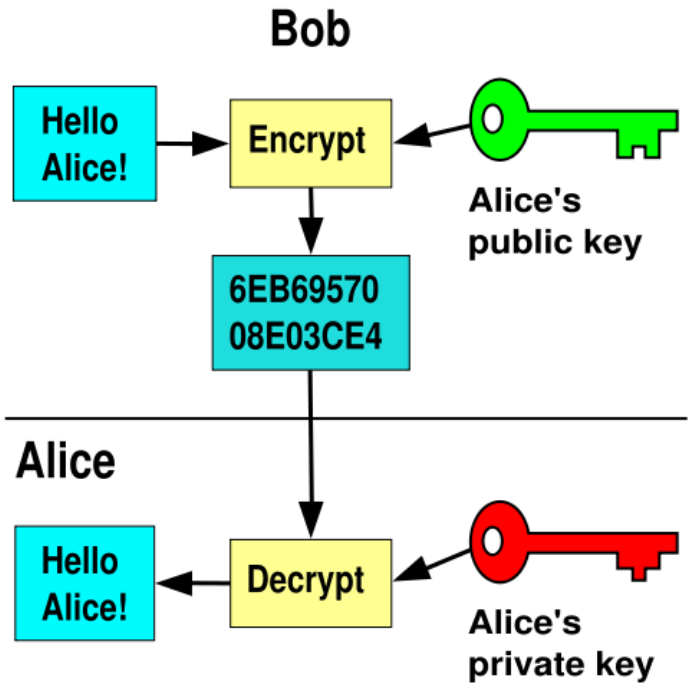
Cipher Block Chaining (CBC)



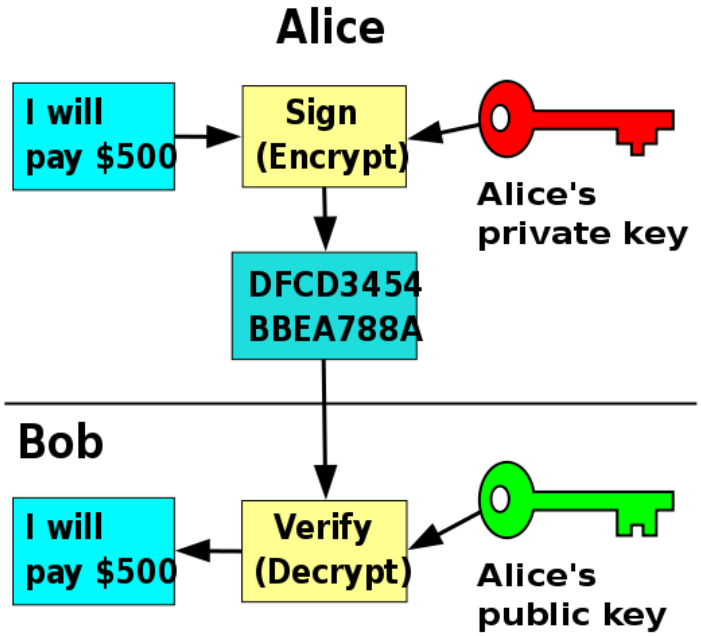
Propagating Cipher Block Chaining (PCBC) mode encryption

Cryptographie asymétrique

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



Chiffrement



Signature

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 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

Extrait de Wikipedia : *Semantic Security*

The original cryptosystem as shown above does provide semantic security against chosen-plaintext attacks (IND-CPA). The ability to successfully distinguish the challenge ciphertext *essentially amounts* to the ability to decide composite residuosity. The so-called decisional composite residuosity assumption (DCRA) is believed to be intractable.

Problèmes difficiles

Sécurité du système : difficulté du décryptage

La sécurité des algorithmes à clefs publiques 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

Modélisation

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 (†)

Modélisation

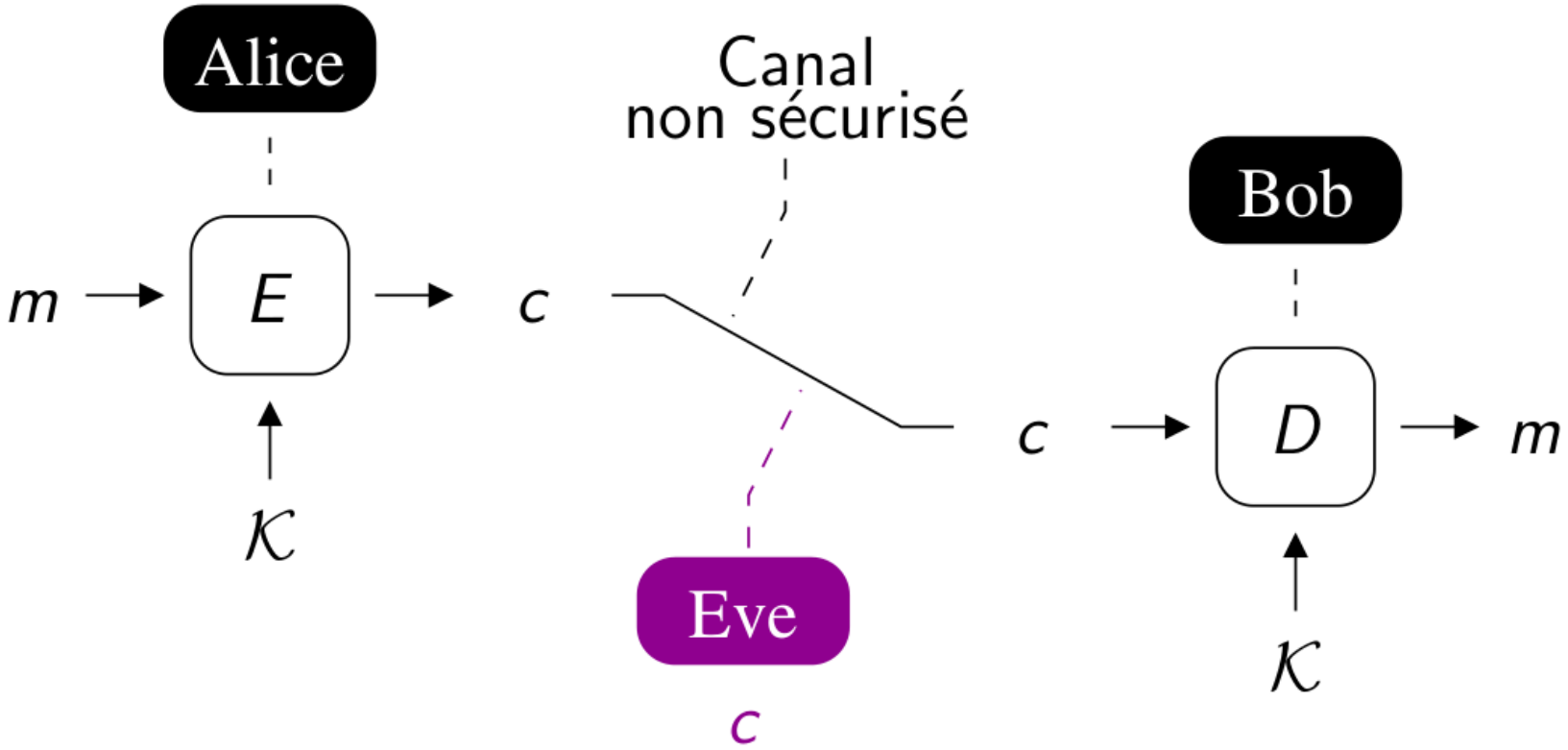
Modélisation de l'adversaire

- 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 ?

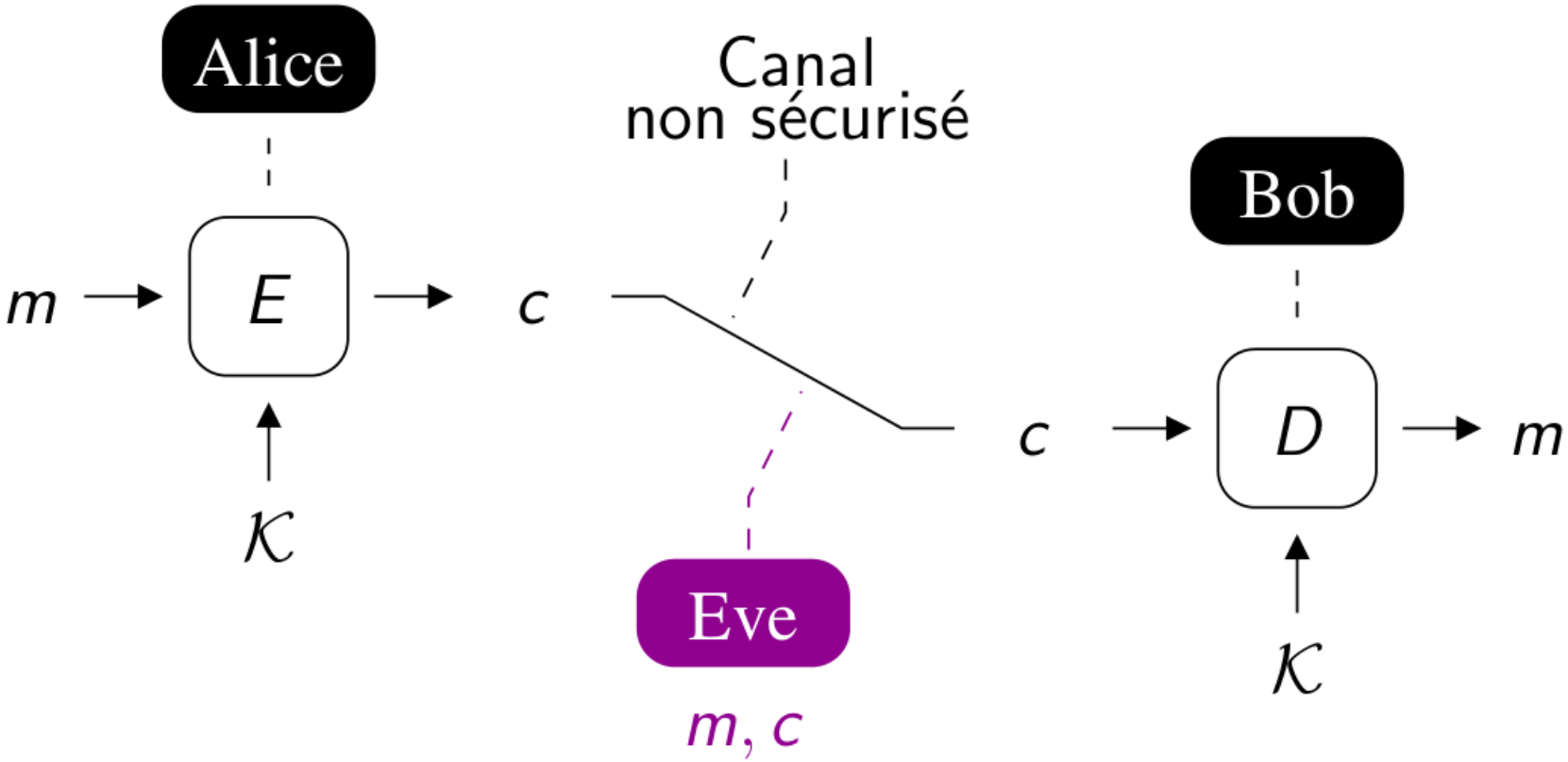
La preuve de sécurité

- 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*)