V. Chiffrement à clé publique

- **Cryptographie asymétrique**
- **2 clés** : publique et privée (secrète)

✓ ***Un message chiffré avec une des deux clés ne peut être déchiffré qu'avec l'autre clé***

Les algorithmes : RSA, Diffie-Hellman, Elgamel et l'algorithme de signature digitale DSA…

❑ **Avantages :**

100 utilisateurs mettent en jeu 100 paires de clés (4950 clés pour un système symétrique).

❑ **Inconvénients :**

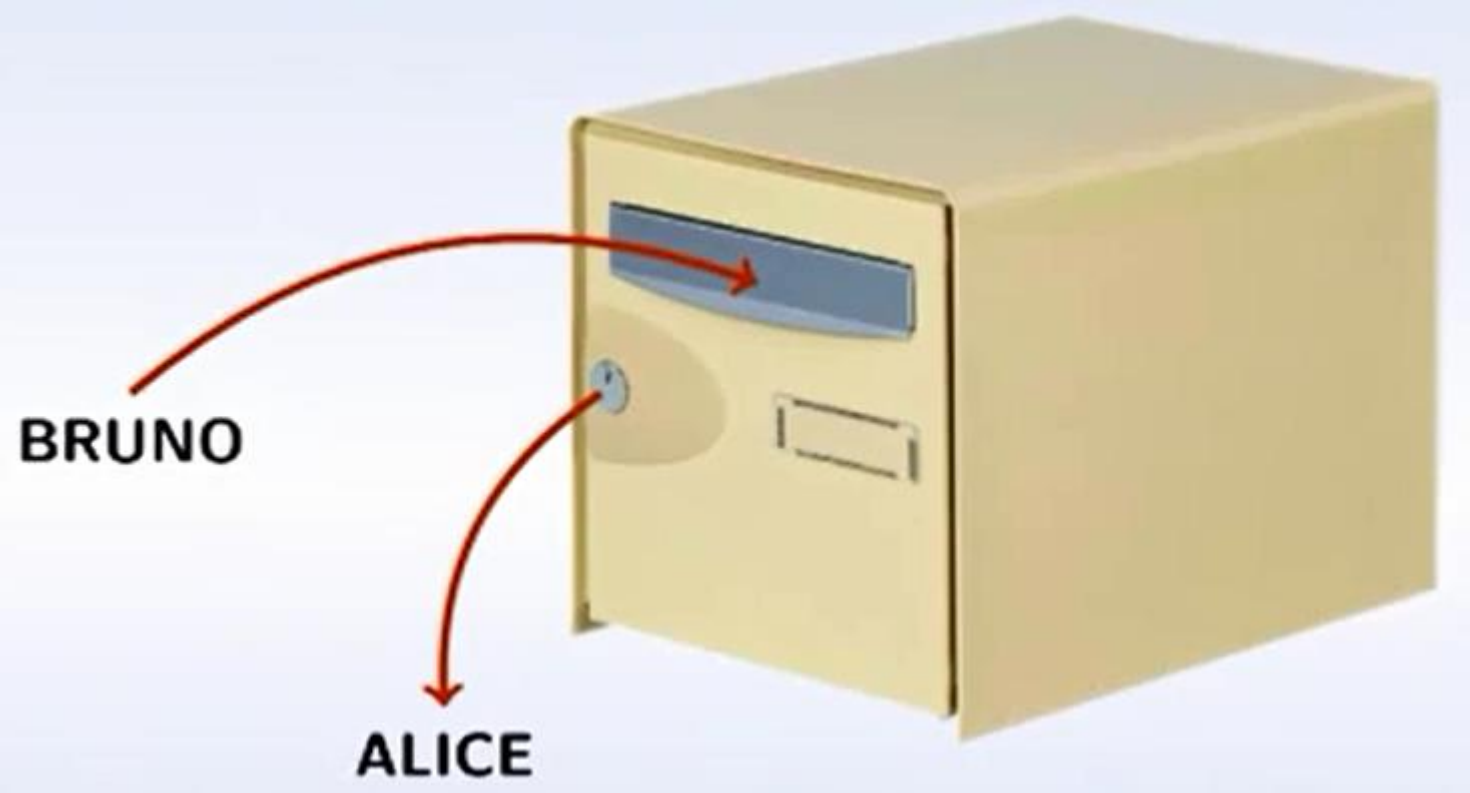
- Les algorithmes à clé publique sont complexes et sont en moyenne de 100 à 1000 fois plus lent que les algorithmes à clé secrète.
- Les crypto-systèmes à clé publique sont vulnérables à certaines attaques

Chiffrement à clé publique

❑ Principe

Chiffrement à clé publique

❑ Principe



❑ L’algorithme RSA (Rivest, Shamir, Adelman)

- Développé en 1978 par Ronald Rivest, Adi Shamir et Leonard Adelman.

- La plus grande partie des crypto-systèmes à clé publique sont basés sur cet algorithme.

- Basé sur la Factorisation

Mathématiques appliquées à RSA

Congruence

Soit **n** un entier tel que : **n ≥ 2**

On dit que a est congru à b modulo n, si (a-b) est divisible par n
On note : **$a \equiv b \pmod{n}$**

Exemple

- $28 \equiv 2 \pmod{26}$, car $28 - 2$ est bien divisible par 26
- $85 = 26 + 59$ donc $85 \equiv 59 \pmod{26}$
- $85 = 3 \times 26 + 7$ donc $85 \equiv 7 \pmod{26}$

Mathématiques appliquées à RSA

Addition modulaire

Soit **a,b et n** des entiers :

$$a + b \pmod n = a \pmod n + b \pmod n$$

Exemple

Calculer : $133 + 64 \pmod{26}$

- $133 + 64 = 197 = 7 \times 26 + 15 \equiv 15 \pmod{26}$
  - $133 = 5 \times 26 + 3 \equiv 3 \pmod{26}$
  - $64 = 2 \times 26 + 12 \equiv 12 \pmod{26}$
  - $133 + 64 \equiv 3 + 12 \equiv 15 \pmod{26}$

Mathématiques appliquées à RSA

Multiplication modulaire

Soit **a,b et n** des entiers :

$$a \times b \pmod n = a \pmod n \times b \pmod n$$

Exemple

Calculer : $3 \times 27 \pmod{26}$

- $3 \times 27 = 81 = 3 \times 26 + 3 \equiv 3 \pmod{26}$
- $27 \equiv 1 \pmod{26}$ puis $3 \times 27 \equiv 3 \times 1 \equiv 3 \pmod{26}$

Mathématiques appliquées à RSA

Nombre premier

Tout entier positif **a (a > 1)** est appelé un nombre premier si ses seuls diviseurs sont **1** et **lui-même**

Nombres premiers entre eux

Deux entiers **a** et **b** sont premiers entre eux si **pgcd(a,b)=1**

Mathématiques appliquées à RSA

Complexité de la factorisation

- $5 \times 7 = ?$
- $35 = ?$
- Factoriser 1591
- Calculer 37×43
- Calculer $p \times q$ est plus facile que de factoriser $n = pq$

La complexité estime le temps de calcul (ou le nombre d'opérations élémentaire) nécessaire pour effectuer une opération.

Mathématiques appliquées à RSA

Complexité de la factorisation

- **Addition**
  - La somme de deux chiffres (par exemple $6 + 8$) est de complexité 1
  - La somme de deux entiers à n chiffres est de complexité n
  - Ex. $1234 + 2323$: 4 additions de chiffres

- **Multiplication**
  - La multiplication de deux entiers à n chiffres est de complexité n^2
  - Ex. 1234×2323 : 16 multiplications de chiffres

- **Factorisation** : $\exp(4n^{\frac{1}{3}})$

Mathématiques appliquées à RSA

- **Complexité de multiplier et de factoriser des nombres à n chiffres**

n	multiplication	factorisation
3	9	320
4	16	572
5	25	934
10	100	5 528
50	2 500	2 510 835
100	10 000	115 681 968
200	40 000	14 423 748 780

Mathématiques appliquées à RSA

Fonction à sens unique

- Fonction f
- Connaissant x, calcul «facile» de $f(x)$
- Pour un y, trouver x tel que $y = f(x)$ est «difficile»
- Fonction à sens unique à *trappe*

Exemple

$f : x \longmapsto x^3 \pmod{100}$ Trouver x tel que $x^3 \equiv 11 \pmod{100}$

- Recherche exhaustive, tester 0, 1, 2, 3, ..., 99

$$71^3 = 357\,911 \equiv 11 \pmod{100}$$

- Trappe secrète : $y \longmapsto y^7 \pmod{100}$ qui fournit directement le résultat !

$$11^7 = 19\,487\,171 \equiv 71 \pmod{100}$$

Mathématiques appliquées à RSA

- **Petit théorème de *Fermat***

  Si p est un nombre premier et a est un entier alors :

$$a^p \equiv a \pmod{p}$$

- **Corollaire**

  Si p ne divise pas a alors :

$$a^{p-1} \equiv 1 \pmod{p}$$

Mathématiques appliquées à RSA

- **Petit théorème de *Fermat amélioré***

  Si p et q deux nombres premiers distincts et soit n = pq

  Pour tout entier a tel que pgcd(a,n)=1 on a:

$$a^{(p-1)(q-1)} \equiv 1 \pmod{n}$$

- Exemple : p = 5, q = 7
  - n = p × q = 35
  - (p - 1) × (q - 1) = 4 × 6 = 24
  - Pour a = 1, 2, 3, 4, 6, 8, 9, 11, 12, 13,.. $a^{24} \equiv 1 \pmod{35}$

Mathématiques appliquées à RSA

- **Principe de l'algorithme d'Euclide**

$$pgcd(a,b) = pgcd(b, a \mod(b))$$

- **Algorithme d'Euclide étendu**

Calculer les coefficients de Bezout u et v tel que :

$$au+bv = pgcd(a,b)$$

Mathématiques appliquées à RSA

- **L'inverse modulo n**

  Soit **a** et **x** deux entiers, on dit que **x** est un inverse de **a** modulo **n** si :

$$ax \equiv 1 \pmod{n}$$

- **a** admet un inverse modulo **n** si et seulement si : **pgcd(a,n)=1**
- Si $au + nv = 1$ alors **u** est un inverse de **a** modulo **n**

Mathématiques appliquées à RSA

Puissance modulaire

Chercher une méthode de calcul efficace de $a^k \pmod n$

Exemple : calcul de $5^{11} \pmod{14}$

On remarque que $11 = 8 + 2 + 1$

$5^{11} = 5^8 \times 5^2 \times 5^1$

Calculons les $5^{2^i} \pmod{14}$

$5 \equiv 5 \pmod{14}$

$5^2 \equiv 25 \equiv 11 \pmod{14}$

$5^4 \equiv 5^2 \times 5^2 \equiv 11 \times 11 \equiv 121 \equiv 9 \pmod{14}$

$5^8 \equiv 5^4 \times 5^4 \equiv 9 \times 9 \equiv 81 \equiv 11 \pmod{14}$

11 en base 2 s'écrit $(1, 0, 1, 1)$

On calcule $5^{2^0}, 5^{2^1}, 5^{2^2}, 5^{2^3}$

$5^{11} = (5^{2^3})^1 \times (5^{2^2})^0 \times (5^{2^1})^1 \times (5^{2^0})^1$

Conséquence

$5^{11} \equiv 5^8 \times 5^2 \times 5^1 \equiv 11 \times 11 \times 5$

$\equiv 11 \times 55 \equiv 11 \times 13 \equiv 143 \equiv 3 \pmod{14}$

Mathématiques appliquées à RSA

Puissance modulaire

Calcul de $17^{154} \pmod{100}$

$k = 154$ en base 2 : $154 = 128 + 16 + 8 + 2 = 2^7 + 2^4 + 2^3 + 2^1$
154 s'écrit donc en base 2 : $(1, 0, 0, 1, 1, 0, 1, 0)$

Calcul $17, 17^2, 17^4, 17^8, \ldots, 17^{128}$ modulo 100

$$17 \equiv 17 \pmod{100}$$
$$17^2 \equiv 17 \times 17 \equiv 289 \equiv 89 \pmod{100}$$
$$17^4 \equiv 17^2 \times 17^2 \equiv 89 \times 89 \equiv 7921 \equiv 21 \pmod{100}$$
$$17^8 \equiv 17^4 \times 17^4 \equiv 21 \times 21 \equiv 441 \equiv 41 \pmod{100}$$
$$17^{16} \equiv 17^8 \times 17^8 \equiv 41 \times 41 \equiv 1681 \equiv 81 \pmod{100}$$
$$17^{32} \equiv 17^{16} \times 17^{16} \equiv 81 \times 81 \equiv 6561 \equiv 61 \pmod{100}$$
$$17^{64} \equiv 17^{32} \times 17^{32} \equiv 61 \times 61 \equiv 3721 \equiv 21 \pmod{100}$$
$$17^{128} \equiv 17^{64} \times 17^{64} \equiv 21 \times 21 \equiv 441 \equiv 41 \pmod{100}$$

$$\begin{aligned} 17^{154} &\equiv 17^{128} \times 17^{16} \times 17^8 \times 17^2 \equiv 41 \times 81 \times 41 \times 89 \\ &\equiv 3321 \times 3649 \equiv 21 \times 49 \equiv 1029 \equiv 29 \pmod{100} \end{aligned}$$

Chiffrement RSA

Paramètres de chiffrement

- **Chercher un problème difficile**

Factoriser un entier produit de deux nombres premiers distincts

- **Calcul des deux clés, publique et privée**

En utilisant l'algorithme d'Euclide et les coefficients de bezout

$au+bv = \text{pgcd}(a,b)$

- **Environnement**

Les calculs sont faits modulo un entier

- **Déchiffrement**

Grace au petit théorème de Fermat

$$a^{(p-1)(q-1)} \equiv 1 \pmod{n}$$

Chiffrement RSA

- **Etapes de chiffrement**
  - ***Calcul de la clé publique et de la clé privée***
  - ***Chiffrement du message***
  - ***Déchiffrement du message***

Chiffrement RSA

Étape 1. Préparation des clés

Étape 1.1 Choix de deux nombres premiers

Alice effectue les opérations suivantes

- choix de deux nombres premiers distincts p et q
- calcul de $n = p \times q$
- calcul de $\varphi(n) = (p-1) \times (q-1) = \varphi(n)$

Exemple

- $p = 5$ et $q = 17$
- $n = p \times q = 85$
- $\varphi(n) = (p-1) \times (q-1) = \varphi(n) = 64$

Chiffrement RSA

Étape 1. Préparation des clés

Étape 1.2 Choix d'un exposant et calcul de son inverse

- Alice choisit un exposant e tel que $\text{pgcd}(e, \varphi(n)) = 1$
- Alice calcule l'inverse d de e module $\varphi(n)$ par l'algorithme d'Euclide étendu : $d \times e \equiv 1 \pmod{\varphi(n)}$

Exemple

- $e = 5$ et on a bien $\text{pgcd}(e, \varphi(n)) = \text{pgcd}(5, 64) = 1$
-
  - $5 \times 13 + 64 \times (-1) = 1$
  - donc $5 \times 13 \equiv 1 \pmod{64}$
  - l'inverse de e modulo $\varphi(n)$ est $d = 13$

Chiffrement RSA

Étape 1. Préparation des clés

Étape 1.3 Clé publique

La *clé publique* d'Alice est constituée des deux nombres

n et e

Étape 1.4 Clé privée

Alice garde pour elle sa *clé privée*

d

Selon l'exemple

$n = 85$ et $e = 5$

$d = 13$

Chiffrement RSA

Étape 2. Chiffrement du message

Étape 2.1 Message

- Bruno veut envoyer un message secret à Alice
- Il transforme son message en un (ou plusieurs) entier m
- L'entier m vérifie $0 \leqslant m < n$

Exemple

$m = 10$

Chiffrement RSA

Étape 2. Chiffrement du message
Étape 2.2 Message chiffré

- Bruno récupère la clé publique d'Alice : n et e
- Il calcule le message chiffré $x \equiv m^e \pmod{n}$
- Il transmet ce message x à Alice

Exemple

- $m = 10$, $n = 85$ et $e = 5$
- $x \equiv m^e \pmod{n} \equiv 10^5 \pmod{85}$
  - $10^2 = 100 \equiv 15 \pmod{85}$
  - $10^4 = (10^2)^2 \equiv 15^2 \equiv 225 \equiv 55 \pmod{85}$
  - $10^5 = 10^4 \times 10 \equiv 55 \times 10 \equiv 550 \equiv 40 \pmod{85}$
- Le message chiffré est donc $x = 40$

Chiffrement RSA

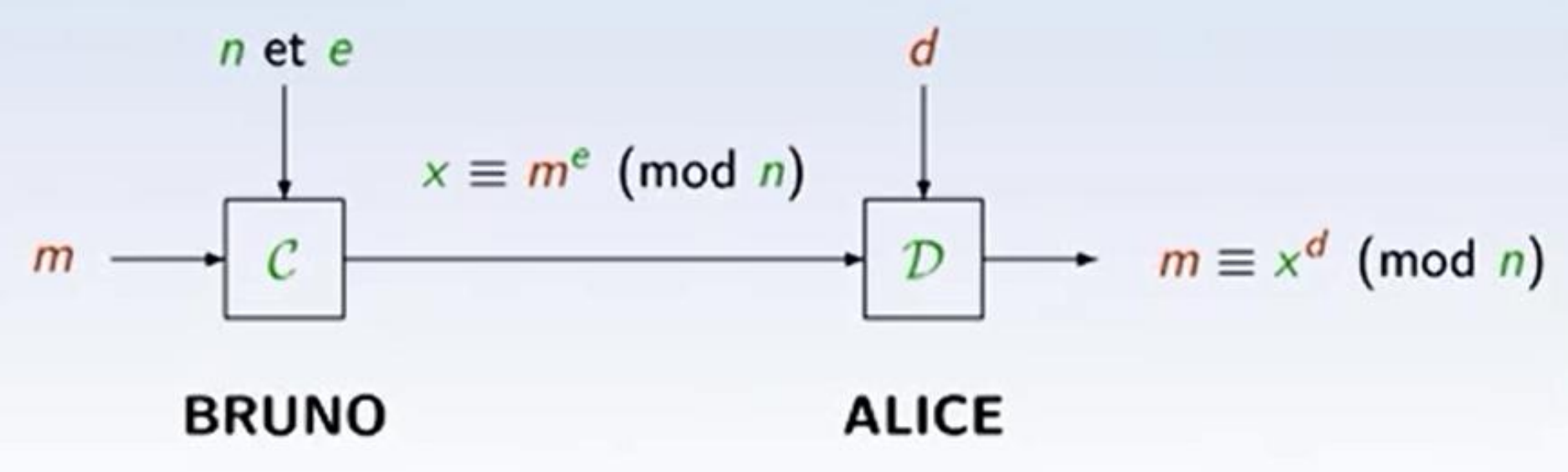
Étape 3. Déchiffrement du message

- Alice reçoit le message x chiffré par Bruno
- Alice le décrypte à l'aide de sa clé privée d
- $$m \equiv x^d \pmod{n}$$

Exemple

- $x = 40$, $d = 13$, $n = 85$ $\qquad 40^{13} \pmod{85}$
  - $40^2 = 1\,600 \equiv 70 \pmod{85}$
  - $40^4 = (40^2)^2 \equiv 70^2 \equiv 4\,900 \equiv 55 \pmod{85}$
  - $40^8 = (40^4)^2 \equiv 55^2 \equiv 3\,025 \equiv 50 \pmod{85}$
- $40^{13} \equiv 40^{8+4+1} \equiv 40^8 \times 40^4 \times 40 \equiv 50 \times 55 \times 40 \equiv 10 \pmod{85}$
- On retrouve bien le message $m = 10$ de Bruno

Chiffrement RSA



Sécurité de RSA

- Il est présumé difficile de déduire la clé privée (d) de la clé publique (n,e). Si on pouvait factoriser n pour retrouver p et q, il serait possible d'obtenir la clé d en utilisant e, l'exposant public. Ainsi, la sécurité de RSA est relative, entre autre, à la difficulté (postulée) du problème de factorisation.

- n étant un nombre très grand, il est très difficile de calculer sa décomposition en facteurs premiers.

- Dans la pratique, n est un nombre dont la représentation binaire est de l'ordre de grandeur de 350 à 400 bits. En effet, il faut bien choisir p et q.

VI. Fonction de hachage

Définition

- Fonction mathématique de compression qui convertit une chaîne de caractères de longueur quelconque en une chaîne de taille fixe (souvent de taille inférieur, appelée empreinte digitale).

- Il est aisé de calculer l ’empreinte à partir d ’une chaîne d ’entrée, mais il est difficile d’engendrer des chaînes qui ont une certaine empreinte.

Utilisation

- La fonction de hachage est publique et est utilisée essentiellement dans les signatures digitales, le contrôle d ’intégrités des données, et l ’identification.

- Par exemple, pour accéder à un compte sous unix, le système calcule l’empreinte, à partir du mot de passe, et la compare à celle qu ’il connaît, qui se trouve dans le fichier etc/passwrd.

VI. Fonction de hachage

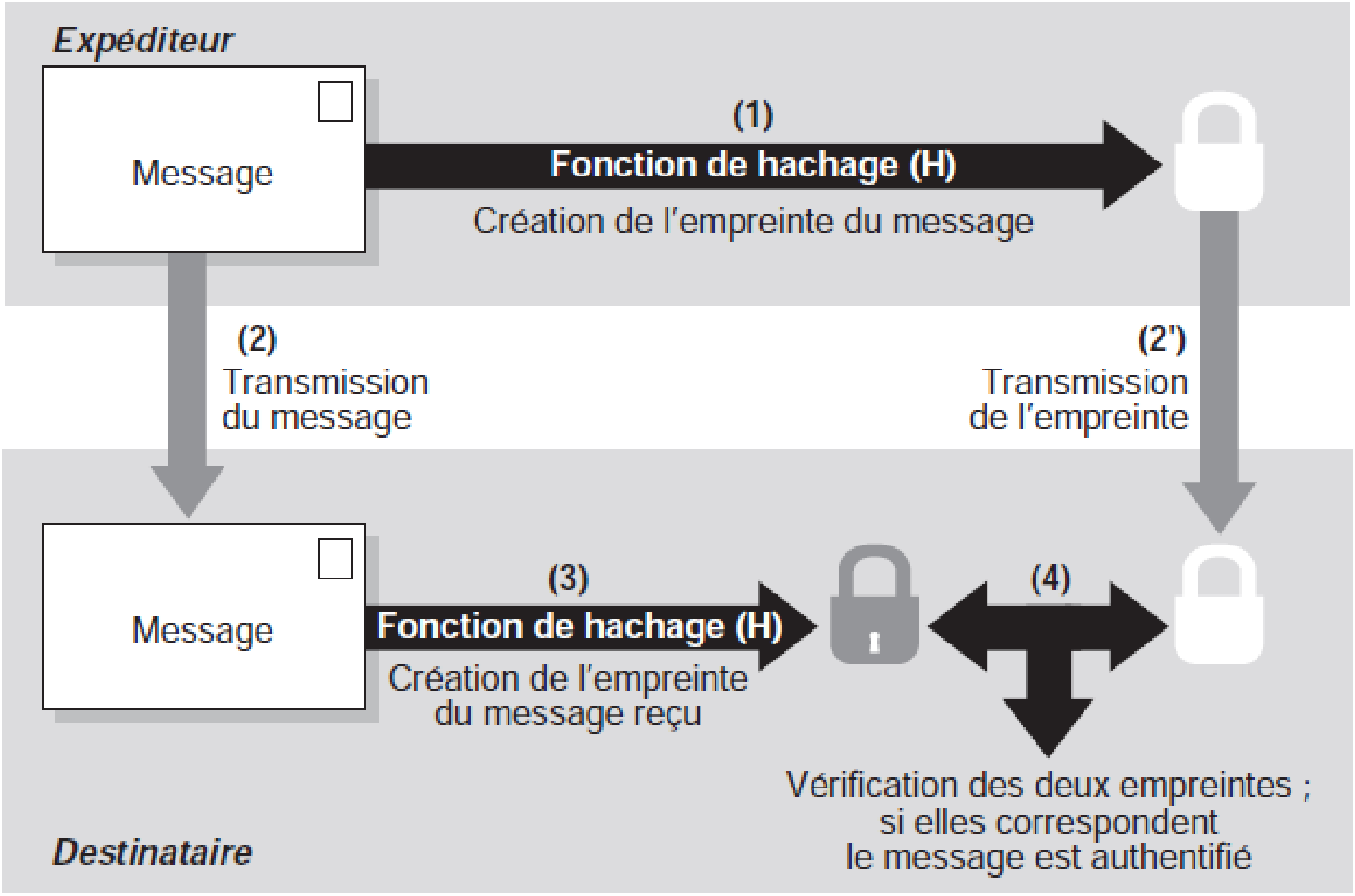
Les algorithmes

- **MD2, MD4 et MD5.** Message Digest 2, 4 et 5 :
  - Développés par Ron Rivest pour RSA Security.
  - fonctions de hachage qui produisent toutes des empreintes d'une taille de 128 bits.

- **SHA, SHA1 et SHA2.** Le SHA (Secure Hash Algorithm) :
  - Développés par la NSA.
  - Les deux algorithmes (SHA et SHA1) produisent des empreintes de 160 bits pour un message pouvant atteindre une taille de deux millions de téraoctets.
  - La taille de son empreinte le rend très difficile à percer, mais il est plus lent que MD5.

- **Snefru** (128 et 256 bits), **N-Hash** (128 bits), …

VI. Fonction de hachage



VII. Signature digitale

Définition

- Une signature digitale est tout procédé d'authentification de documents généré et géré par voie purement électronique et/ou informatique. Une signature numérique a le même objet qu'une signature manuscrite.

- une signature manuscrite est facile à contrefaire. Par contre une signature numérique est pratiquement infalsifiable de plus elle atteste le contenu de l'information autant que l'identité du signataire. Elle est unique, facile à authentifier pour le destinataire, facile à générer et d'un coût économique viable.

Création et utilisation

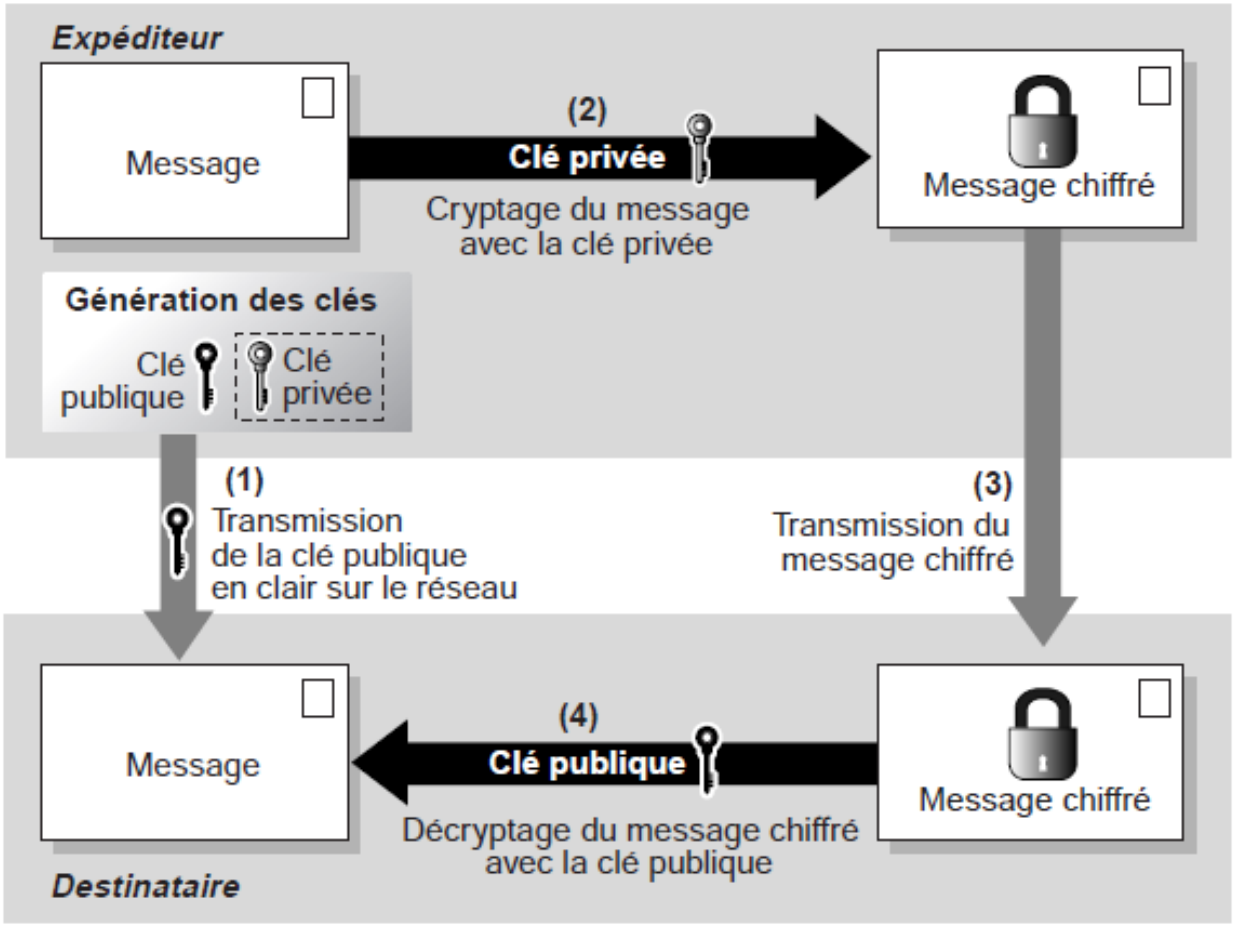
- La méthode de base utilisée pour créer une signature numérique consiste à chiffrer l'information avec la clé privée de l'expéditeur. Le destinataire a la possibilité de vérifier et de contrôler l'authenticité sachant uniquement la clé publique de l'émetteur. En effet, si le destinataire arrive à déchiffrer la signature avec la clé publique de l'expéditeur alors l'information est authentique.

VII. Signature digitale

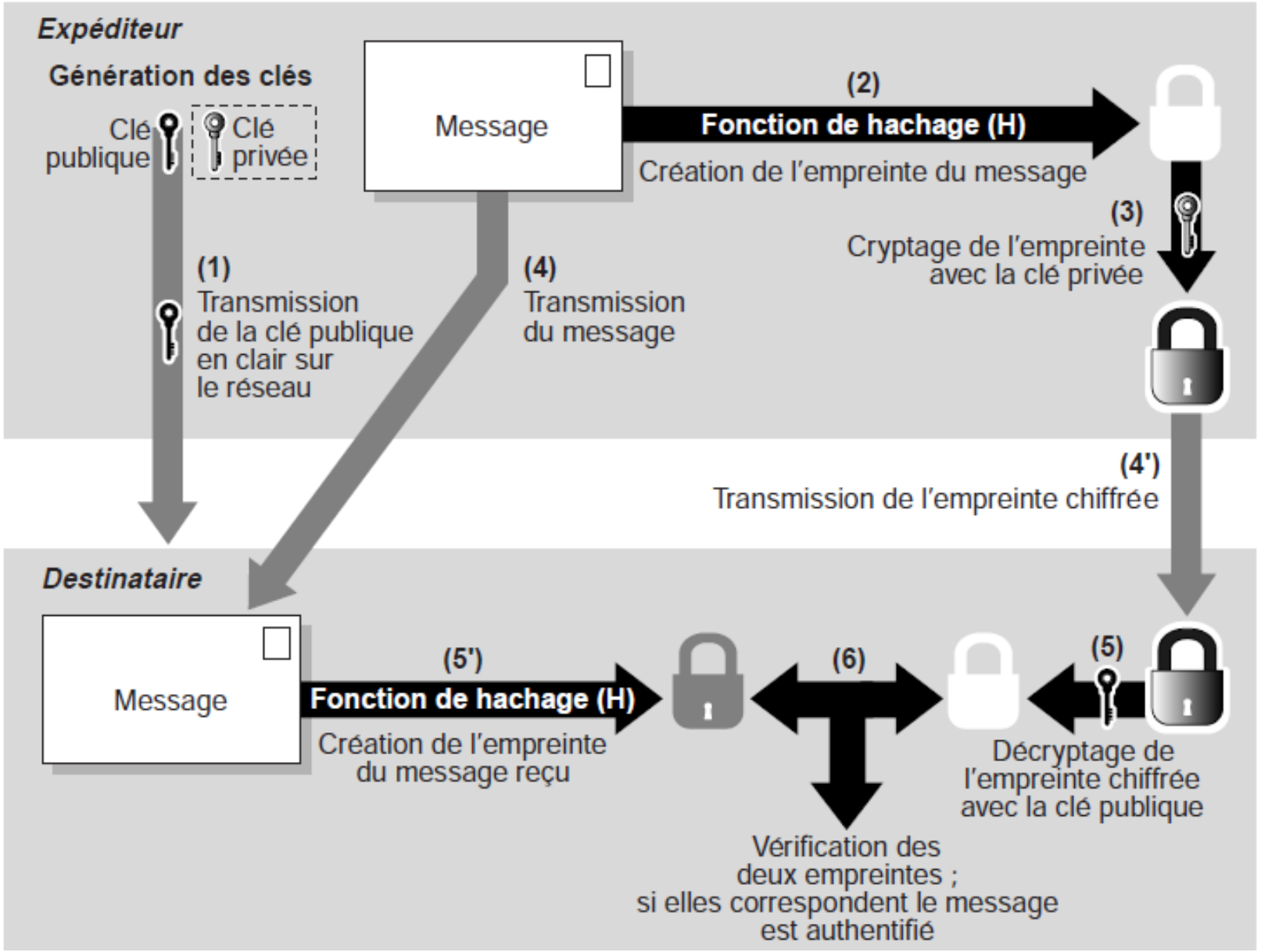
- Pour se faire authentifier, l'émetteur utilise sa clé privée pour signer un message. De son côté, le récepteur utilise la clé publique de l'émetteur pour vérifier si le message est signé.

- De cette façon, le récepteur peut vérifier tout à la fois que les données n'ont pas été modifiées et qu'elles ont bien été envoyées par l'émetteur.

Authentification par clé publique



Combinaison de fonction de hachage et chiffrement à clé publique



VIII. Cryptanalyse

Définition

- La cryptanalyse est l'art d'analyser un message chiffré (les faiblesses) afin de le décoder (et de Casser le code).
- Le but de la cryptanalyse est de retrouver des messages clairs correspondants à des messages chiffrés.

Attaquant

- La personne qui tente de décrypter (sans la connaissance de la clé).
- L'attaquant utilise une combinaison de raisonnement analytique, d'application d'outils mathématiques, et de découvertes de redondances.

Principe de Kerckhoffs

- La sécurité d'un chiffrement doit reposer uniquement sur la protection de la clé. C'est-à-dire l'algorithme (méthode ou procédé) est public (non secret).

VIII. Cryptanalyse

Types de cryptanalyse

- Cryptanalyse partielle : l'attaquant décrypte 1 ou plusieurs messages (mais pas la totalité).
- Cryptanalyse totale : l'attaquant découvre un moyen pour déchiffrer tous les messages (s'il découvre la clé par exemple).

Techniques de cryptanalyse

❖ Recherche exhaustive

Essayer toutes les combinaisons d'une clé.
Les programmes qui utilisent ce procédé sont dits à force brute (moulinette). Ils ont besoin en entrée du nom du fichier à cracker et d'une expression régulière. La moulinette essaie toutes les combinaisons possibles de clé satisfaisant l'expression régulière.

Exemples : Pour le chiffre de César, cette recherche est envisageable, puisqu'il y a peu de possibilités (25).

VIII. Cryptanalyse

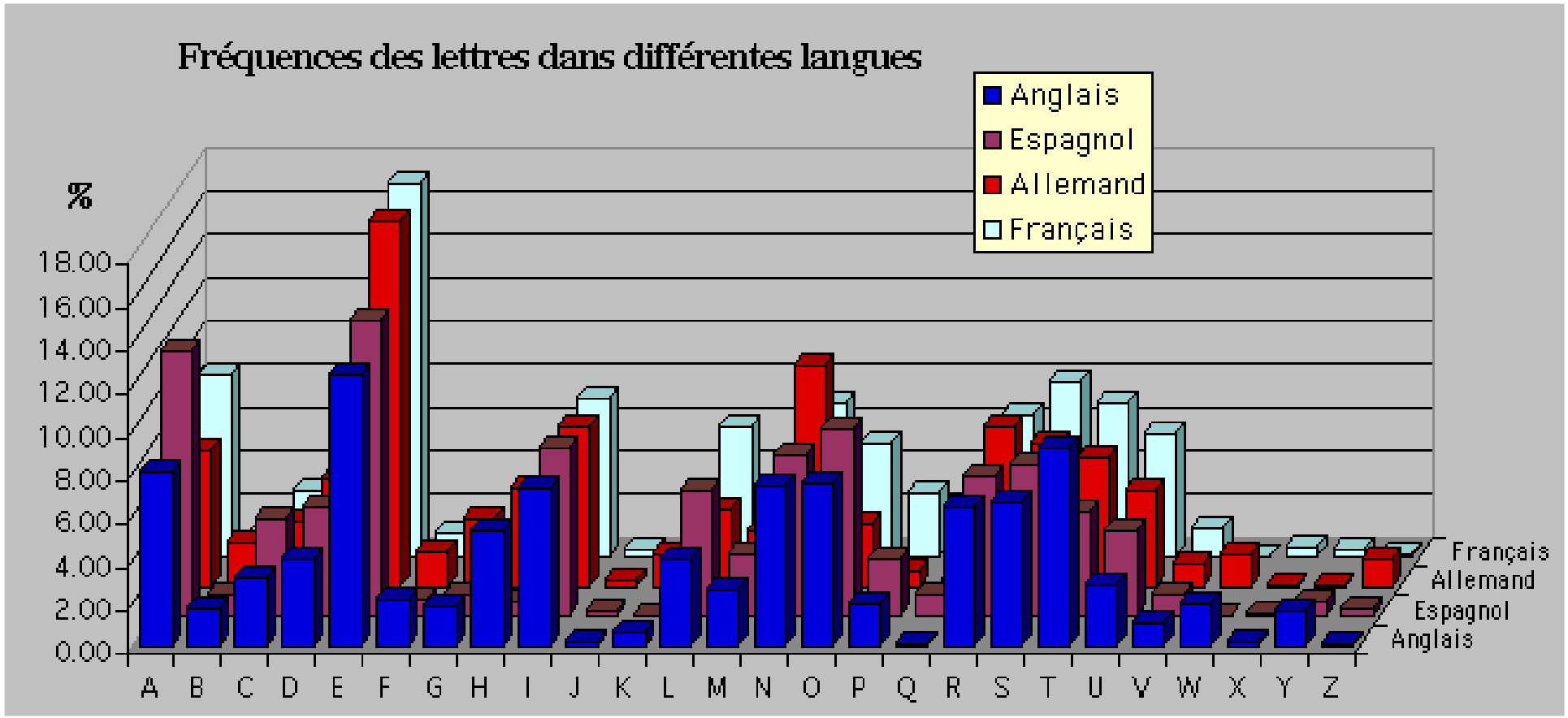
❖ Recherche par dictionnaire

- Retrouver la clé à l'aide de mots courant de la langue contenus dans une base de données (dictionnaire). Ce dictionnaire contient les mots de langue, les noms des acteurs, les héros de films ou dessins animés, des phrases philosophiques….
- La moulinette tente de déchiffrer le texte en essayant ces mots (à l'envers, en minuscule, ou majuscule…).

❖ Analyse statistique (fréquentielle)

- Une attaque statistique consiste à analyser statistiquement les textes cryptés, c'est-à-dire :

- Déterminer les fréquences d'apparition des symboles ;
- Les comparer avec les fréquences types caractéristiques des langues.


Fréquences des lettres dans différentes langues
Anglais
Espagnol
Allemand
Français
%
18.00
16.00
14.00
12.00
10.00
8.00
6.00
4.00
2.00
0.00
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Français
Allemand
Espagnol
Anglais

Fréquences des lettres arabes :

- Dans un corpus de 9 million de mots

ا التكرار 8152955	ح التكرار 1102664	آ التكرار 45349
ن التكرار 6152840	ج التكرار 910197	ى التكرار 21863
ت التكرار 5572441	ش التكرار 780130	
م التكرار 5566423	ط التكرار 702773	
ي التكرار 5345504	ص التكرار 626206	
و التكرار 5116923	خ التكرار 621341	
ل التكرار 4629557	ز التكرار 612241	
ه التكرار 4201915	ض التكرار 420089	
ك التكرار 4098027	غ التكرار 406768	
ف التكرار 3962015	ث التكرار 239856	
ب التكرار 2719120	ئ التكرار 233810	
ر التكرار 2665611	ذ التكرار 209137	
س التكرار 2301475	ة التكرار 204042	
ع التكرار 1397958	إ التكرار 114131	
أ التكرار 1386344	ظ التكرار 112718	
د التكرار 1356333	ؤ التكرار 79020	
ق التكرار 1278780	ء التكرار 54731	

❖ Attaque de protocoles

Il existe deux méthodes pour attaquer les protocoles :

- attaque passive (écouter le canal) : collecter des informations, récupérer une clé secrète ou observer l'écriture du texte en clair par l'expéditeur. Ce type d'attaques est très difficile à détecter ;

- attaque active : intercaler des messages, supprimer des messages ou détruire les canaux de communications. La manière dont est menée l'attaque dépend du réseau.

IX. Outils de chiffrement

- Il existe deux types d'outils : Hard et Soft

❖ PGP (Pretty Good Privacy)

Logiciel de chiffrement de documents, Inventé par Philippe Zimmerman

Caractéristiques de PGP

- PGP offrait des clefs de chiffrement de plus de 1024 bits.
- PGP combine à la fois les meilleures fonctionnalités de la cryptographie conventionnelle et de la cryptographie à clé publique.

Algorithmes utilisés par PGP

- L'algorithme de chiffrement à clé publique RSA, (pour signature et chiffrement),
- L'algorithme de chiffrement à clé secrète IDEA, (pour chiffrement),
- L'algorithme de hachage à sens unique MD5 (pour signature et authentification)

❖ Autres outils

IX. Outils de chiffrement

- Autres outils
  - GNU Privacy Guard (Windows/Mac/Linux)

Implémentation Open-source de PGP

  - Disk Utility(Mac)

Chiffrement à l'aide de AES 128 bits ou 256 bits

  - TrueCrypt(Windows/Mac/Linux)

Créer et sécuriser des disques virtuels

  - AxCrypt(Windows)

Utilise AES 256 bits

  - 7-zip(Windows)

Utilise AES 256 bits