Module 1 – Fondamentaux techniques et règlementaires

Fondamentaux de la sécurité des SI et réseaux

Séquence 5 : Sécurisation des échanges et des données

OIDANEOS

Présentation de la séquence
Objectifs et notions abordées

Appliquer les principes de sécurité au travers de mesures cryptographiques

- Principes généraux de la cryptologie
- Principaux systèmes cryptographiques
- Les infrastructures de gestion de clés publiques

Principes généraux de la cryptologie

Principes généraux de la cryptographie
Définitions

CRYPTOLOGIE

Science mathématique qui permet d'étudier les principes, méthodes et techniques liées à la sécurité de l'information sous toutes ses formes (texte, image ou son) et qui comporte deux branches : cryptographie et cryptanalyse

CRYPTOGRAPHIE

Science qui consiste à transformer l'information (chiffrement) pour la rendre inintelligible (cryptogramme) à ceux ne possédant pas les capacités de la déchiffrer

Principes généraux de la cryptographie
Définitions

- **Clés symétriques** : mêmes clés utilisées pour le chiffrement et le déchiffrement (chiffrement symétrique)
- **Clés asymétriques** : clés différentes utilisées pour le chiffrement et le déchiffrement (chiffrement asymétrique)

Principes généraux de la cryptographie
Définitions

CRYPTANALYSE

Ensemble des moyens mathématiques qui permettent d'analyser une information préalablement chiffrée, afin de la reconstruire en un message clair. Un système de chiffrement doit être résistant à la cryptanalyse, sinon il est « cassé »

Méthodes de cryptanalyse

- **Attaque sur texte chiffré seulement**
- **Attaque sur texte clair connu**
- **Attaque sur texte clair choisi**
- **Attaque sur texte chiffré choisi**

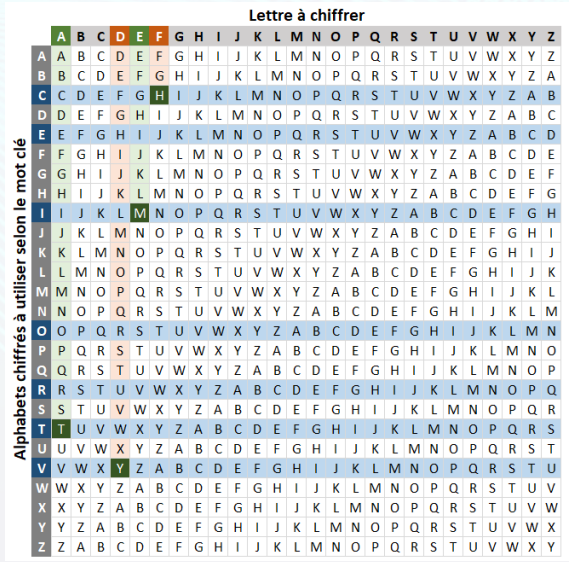
Principes généraux de la cryptographie
Caractéristiques d'un cryptosystème

- Algorithme de chiffrement
- Algorithme de déchiffrement
- Espace de clés possibles
- Protocoles de fonctionnement de l'algorithme

Principes généraux de la cryptographie

Les premiers systèmes cryptographiques (chiffrement classique)

- **Chiffrement monoalphabétique**
  - Chiffrement par décalage
  - Chiffrement linéaire
- **Chiffrement polyalphabétique**
  - Chiffrement de Vigenère
  - Chiffrement de Hill
  - Chiffrement par permutation



Principes généraux de la cryptographie
Le cadre règlementaire en France

- Loi pour la Confiance dans l'Économie Numérique (LCEN), 2004
- Articles L.851-1 et suivants et R. 871-1 et suivants du Code de la Sécurité Intérieure
- Article 434-15-2 du Code Pénal

- Règlement « Biens à double usage » (Règlement (UE°) 2021/821)
- Règlement Général sur la Protection des Données (RGPD)
- Règlement eIDAS et eIDAS 2.0
- Directives NIS2 et DORA

Chiffrement moderne

Chiffrement moderne
Les principes de Kerckhoffs (1883)

- Le système doit être matériellement, sinon mathématiquement indéchiffrable
- Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi
- La clé doit pouvoir être communiquée et retenue sans le secours de notes écrites et être changée ou modifiée au gré des correspondants
- Il faut qu'il soit applicable à la correspondance télégraphique
- Il faut qu'il soit portatif et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes
- Il est nécessaire, vu les circonstances qui en commandent l'application, que le sys

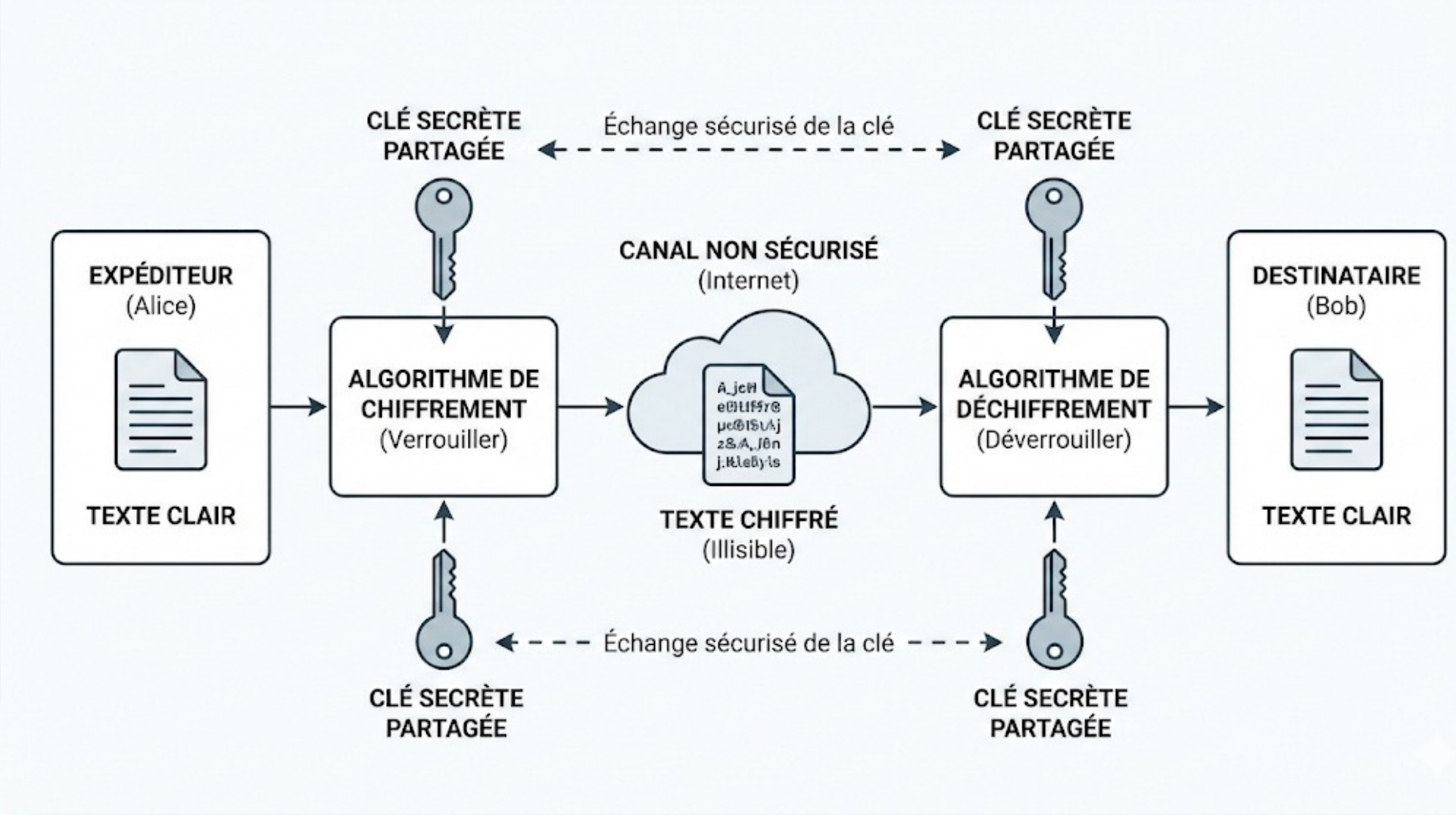
Chiffrement moderne

Les catégories de chiffrement moderne

Chiffrement symétrique

Chiffrement asymétrique

Chiffrement moderne
Principe du chiffrement symétrique



Chiffrement moderne

Principes et applications du chiffrement symétrique

Plus on a d'interlocuteurs, plus il faut de clés

Difficulté dans la gestion et la diffusion des clés

Parfait pour le chiffrement de données en temps réel ou en différé

Chiffrement moderne

Les algorithmes du chiffrement symétrique

Data Encryption Standard (DES)

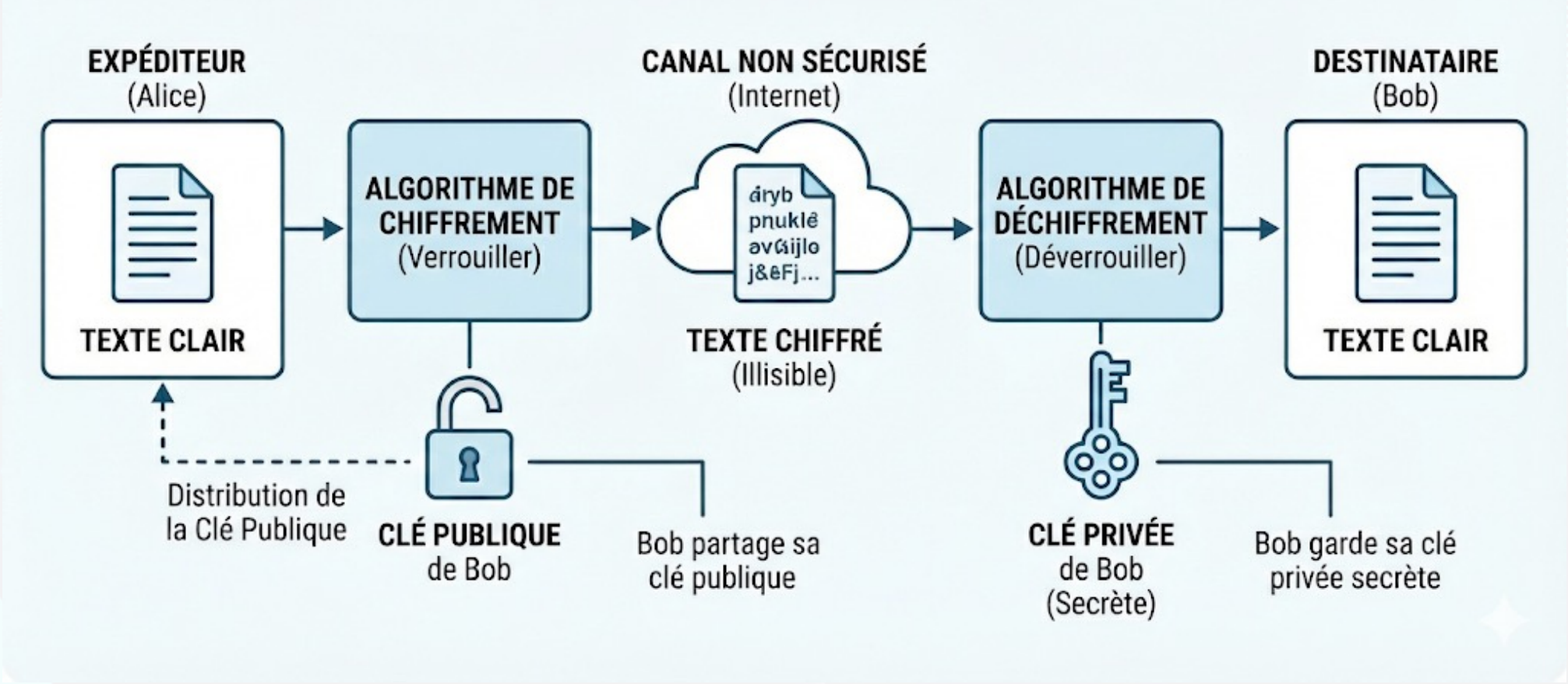
Rivest's Cypher (RC2 / RC4 / RC5 / RC6)

International Data Encryption Algorithm (IDEA)

Blowfish

Advanced Encryption Standard (AES)

Chiffrement moderne
Le chiffrement asymétrique



Chiffrement moderne

Principes et applications du chiffrement asymétrique

Vérification de l'authenticité de la clé publique par le certificat numérique et la signature électronique

Signature électronique d'un document

Consommation énergétique et longueur d'exécution

Chiffrement moderne

Les algorithmes du chiffrement asymétrique

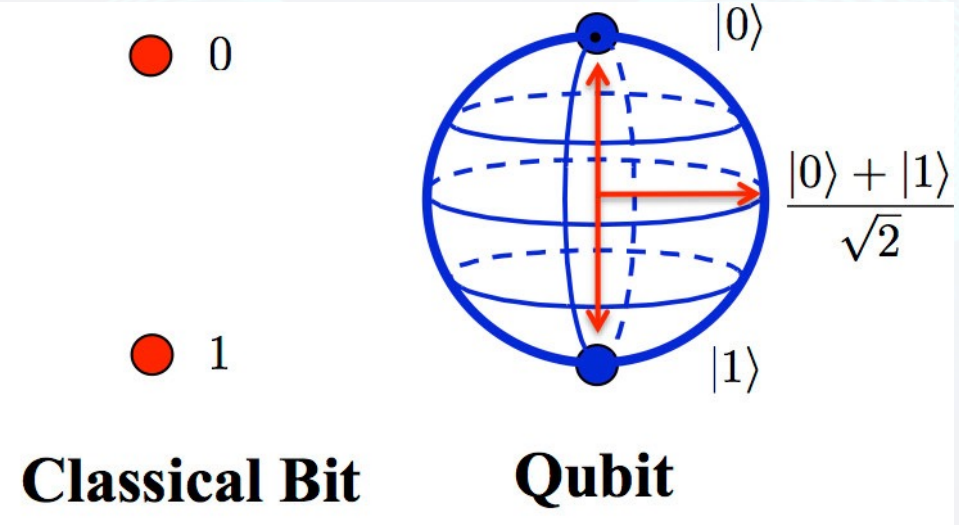
Algorithme RSA

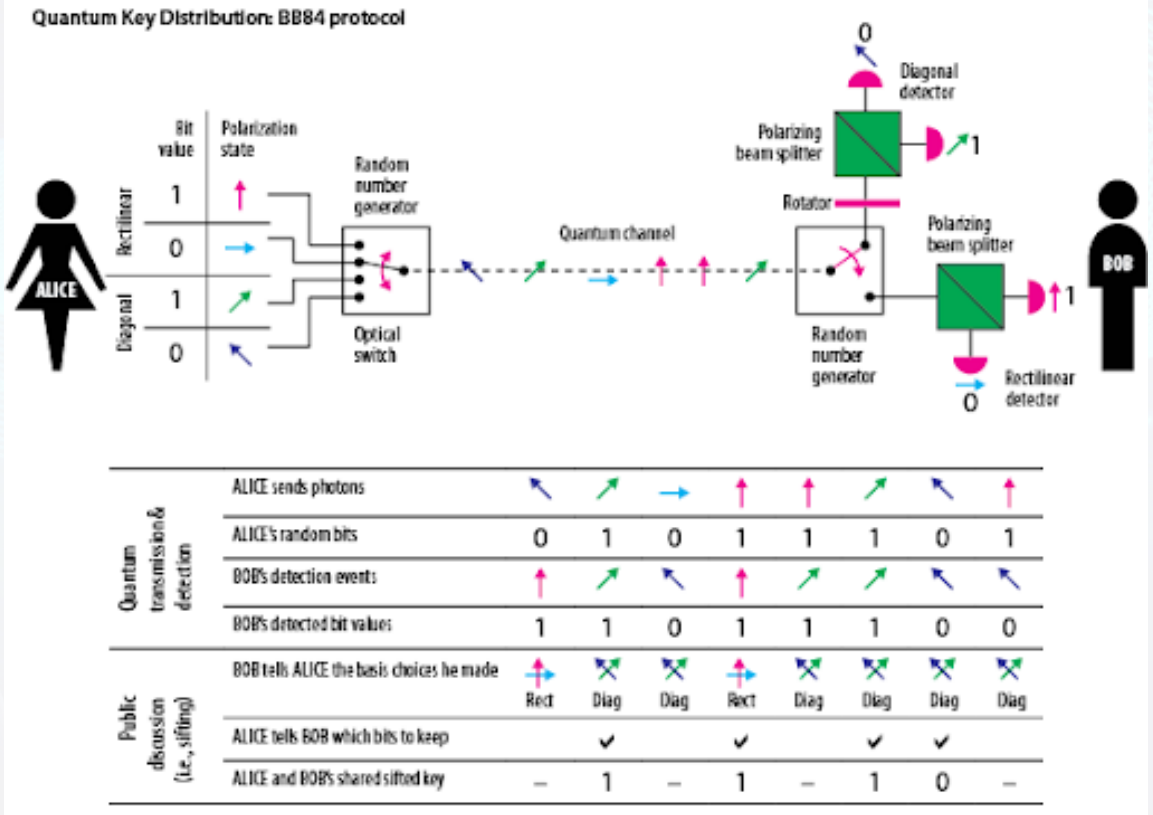
Diffie-Helmann

Cryptographie à courbe elliptique (ECC)

Chiffrement homomorphe

Chiffrement moderne
La cryptographie quantique





Chiffrement moderne
Le chiffrement post-quantique

Mécanisme de chiffrement asymétrique résistant aux ordinateurs quantiques.

Cryptographie

L'algorithme Falcon sélectionné pour la nouvelle norme de cryptographie postquantique

Date: 27 Jan. 2023

Voir le fil d'Ariane

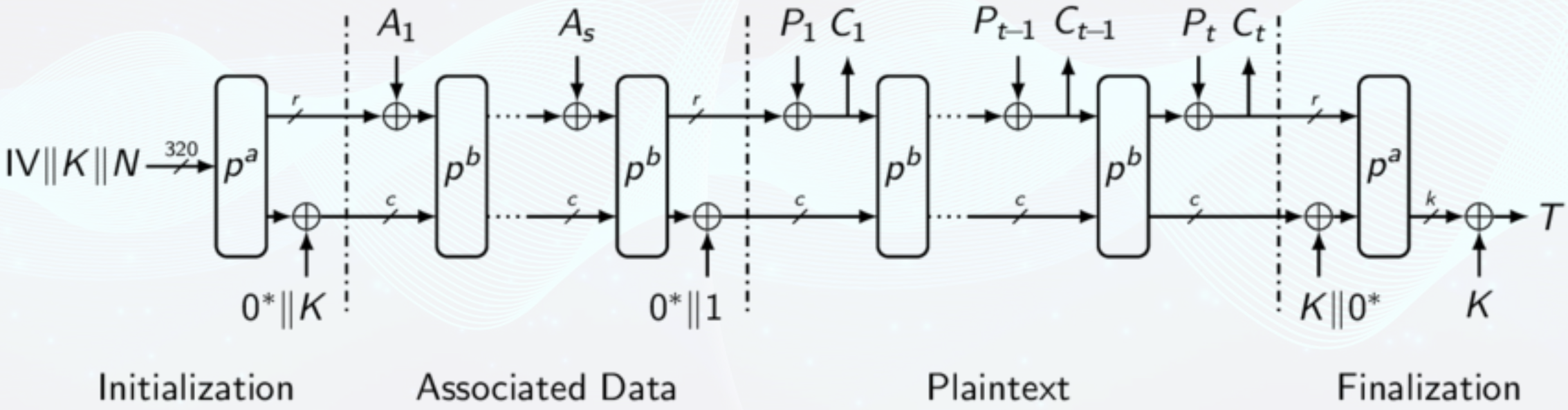
L'algorithme HAETAE lauréat de la compétition coréenne de cryptographie post-quantique

Publié le jeudi 6 février 2025

La compétition KpqC qui a débuté en 2022, visait à sélectionner des algorithmes de cryptographie post-quantique. Julien Devevey, cryptologue du Laboratoire de Cryptographie de l'ANSSI, a participé à la conception de l'algorithme HAETAE qui a remporté cette compétition le 16 janvier 2025.

Chiffrement moderne

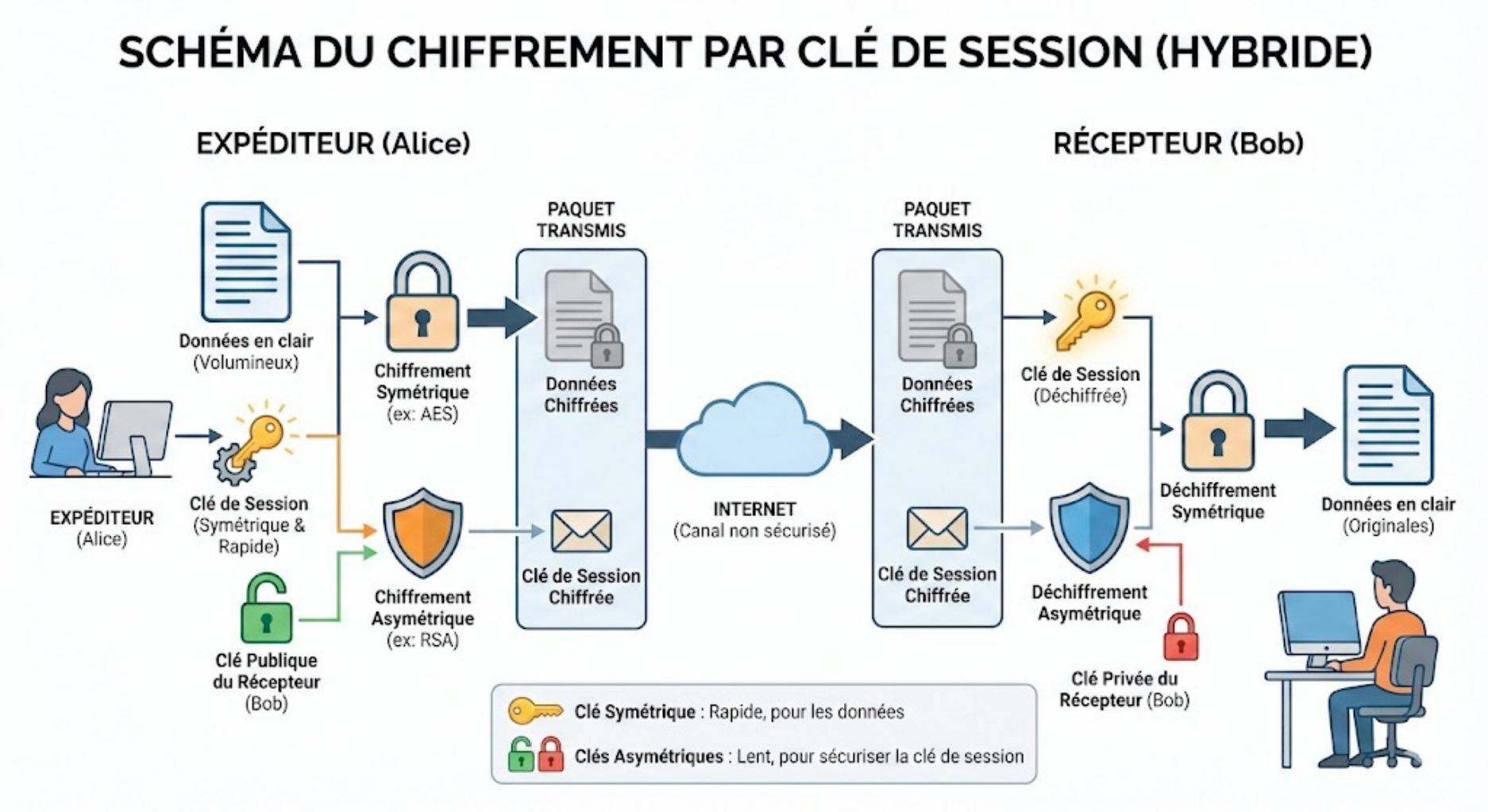
Le chiffrement à faible empreinte



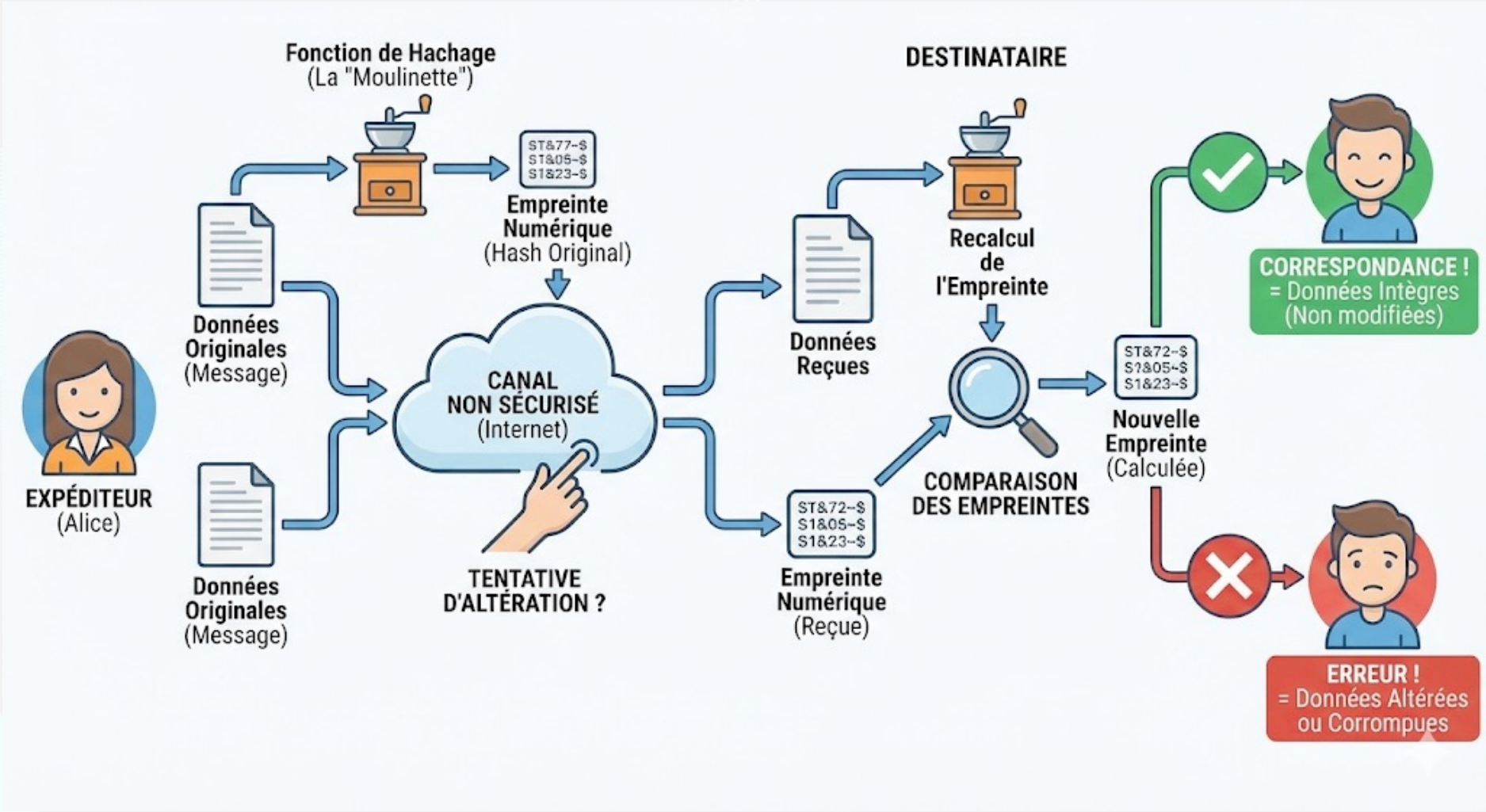
Algorithme ASCON

Les usages de la cryptographie

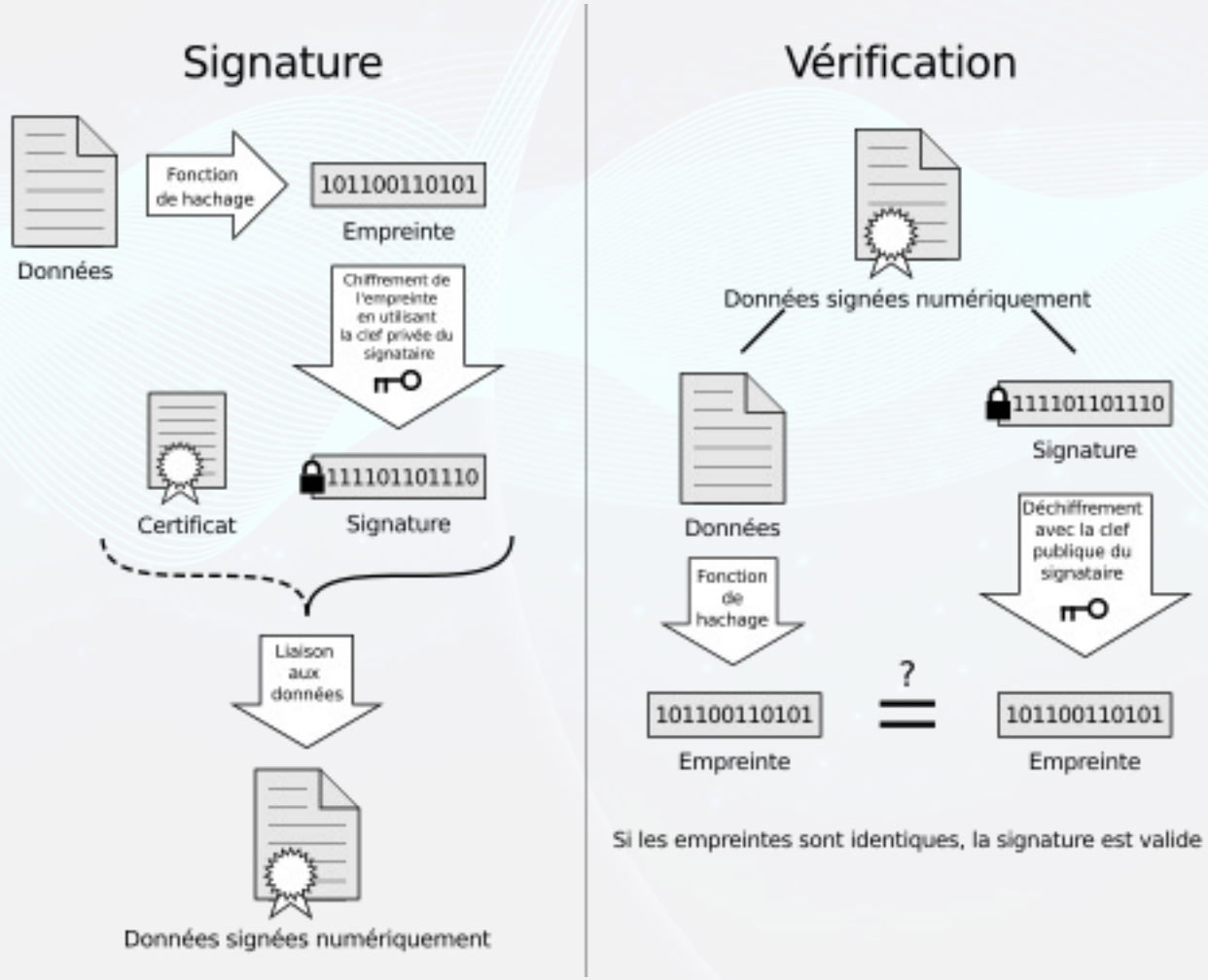
Les usages de la cryptographie
Le chiffrement par clé de session



Les usages de la cryptographie
La vérification de l'intégrité des données



Les usages de la cryptographie
L'authentification et la signature électronique



Les usages de la cryptographie
Infrastructure de gestions des clés (IGC ou PKI)

Génération de clés

Distribution des clés

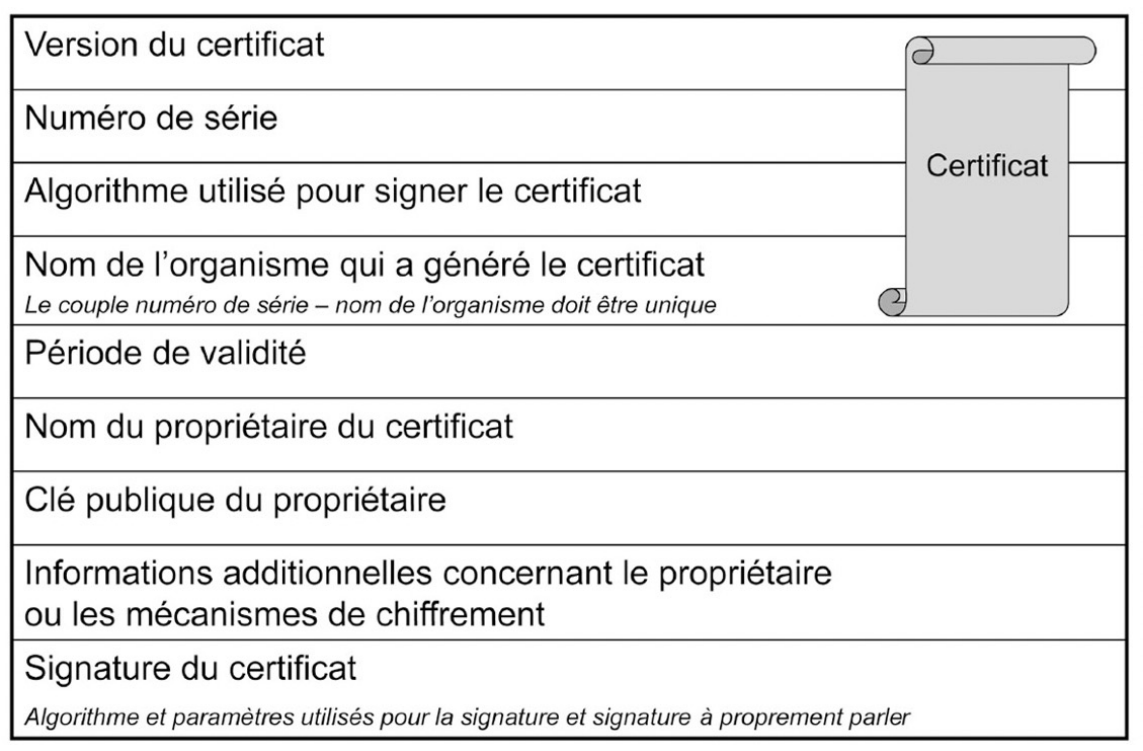
Stockage sécurisée des clés

Surveillance

Destruction des clés

Les usages de la cryptographie
Le certificat numérique

- Le certificat numérique représente la carte d'identité numérique d'une entité
- Les informations du certificat sont chiffrées avec la clé privée de l'organisme de certification
- Le propriétaire du certificat le déchiffre avec la clé publique de l'organisme de certification
- Il existe différents types de certificats avec des niveaux variables de sécurité qui peuvent être émis
    - La recommandation X.509 de l'UIT propose un cadre architectural pour la réalisation d'un service d'authentification basé sur l'usage de certificats



Les usages de la cryptographie
Le certificat numérique

Il existe différentes classes de certificat

1	Attribution sans vérification de l'identité du propriétaire
2	Le propriétaire précise son identité sans qu'elle soit vérifiée
3	Le propriétaire du certificat est physiquement présent pour sa remise pour procéder à son contrôle d'identité
3+	Idem que la classe 3 avec remise du certificat sur un support matériel

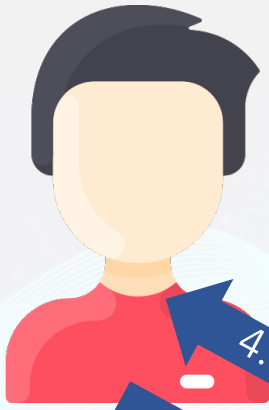
Les usages de la cryptographie
La notion d'organisme de certification

Organisme de certification

- Tiers de confiance
- Autorité d'enregistrement
- Autorité de certification
- Autorité de dépôt et de séquestre

Les usages de la cryptographie

Le cas d'une PKI dans une entreprise



2. Connexion sur le site Internet

5. Génération d'une session

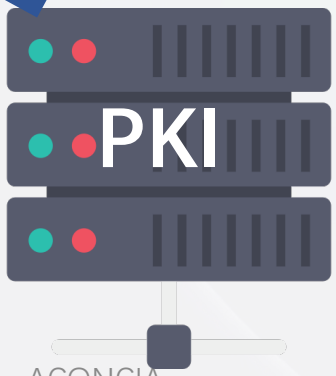
Envoi d'une clé de session symétrique chiffrée avec la clé publique de l'entreprise

Clé privée de l'entreprise

4. Téléchargement du certificat de l'entreprise

3. Connexion au site de la PKI

1. Distribution du certificat



Certificat entreprise

- *Version*
- *Numéro de série*
- *Algorithme de signature*
- *Nom de l'AC émettrice*
- *Valide à partir du …*
- *Jusqu'au …*
- *Clé publique de l'entreprise*
- *Paramètres spécifiques au certificat*
- *Algorithme d'empreinte*
- *Empreinte numérique du certificat*