8. Infrastructure de gestion de clés

8.1. Clés publiques : le problème de confiance

- En cryptographie asymétrique, chaque acteur dispose d'un couple de clés : une clé **publique** et une clé **privée**.
- La diffusion de cette clé publique doit respecter plusieurs critères :

- **authentification** : on doit être sûr que la clé est bien celle de la personne avec qui on va échanger des données confidentielles (risque de l'attaque "man in the middle").
- **confiance** : la personne en question doit être digne de confiance.
- **validité** : une clé publique a une durée de vie en général finie. On doit donc pouvoir vérifier cette dernière.
- Un des moyens de résoudre ce problème : les *certificats* et *autorités de certification* gérés au sein d'une **infrastructure de gestion de clés** - IGC (*Public Key Infrastructure - PKI*).

8.2. Certificats

- Document numérique contenant une clé publique ainsi que d'autres informations associées à cette clé.

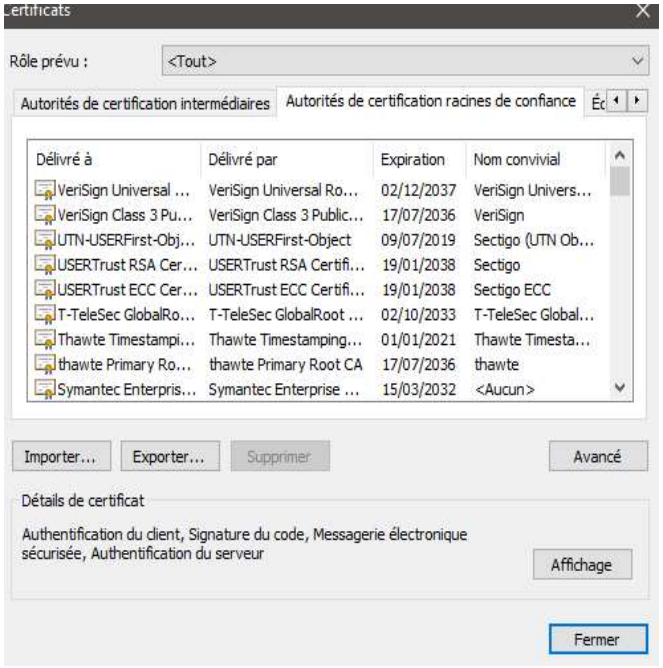
- Authentifié (signature numérique)
  - soit par une **autorité de certification (AC)**. C'est la norme X.509 de l'ISO définie en 1988 dans le cadre du projet X.500. Le modèle sous-jacent est un système hiérarchique d'autorités de certification.
  - soit par quiconque appartenant à un **réseau de confiance**. C'est par exemple la toile de confiance (web of trust) d'OpenPGP.

8.2. Certificats

- Dans le **modèle X.509**, une des limites est la confiance que l'on peut accorder à une AC. Cette confiance est essentielle car elle conditionne tout le reste. En effet si une AC est compromise, l'ensemble des clés qui en dépendent est compromis.

8.2. Certificats

- Quelques autorités de certification



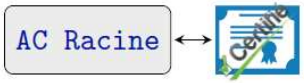
`X509v3 Basic Constraints:`	Indique s'il s'agit du certificat d'une AC ou non
`X509v3 Key Usage:`	Précise les fonctionnalités du certificat. Par exemple, il peut être utilisé pour signer d'autres certificats (*Certificate sign*)
`X509v3 subjectAltName:`	Autres noms du propriétaire du certificat. Ce sont des alias du champ *Subject*
`X509v3 issuerAltName:`	Autres noms de l'émetteur du certificat. Ce sont des alias du champ *Issuer*
`X509v3 CRL Distribution points:`	URI de la *Certificat Revocation List (CRL)* permettant de connaître le statut du certificat

- Une extension peut être qualifiée de **critique** (critical).
- Une application doit **impérativement** traiter les extensions marquées comme critique.
- Une application, ayant à traiter une extension marquée comme critique qui lui est **inconnue**, doit ignorer le certificat contenant cette extension.
- Lorsque l'on utilise les extensions *Basic Constraints* et *Key Usage*, celles-ci doivent être marquées comme *critiques*.

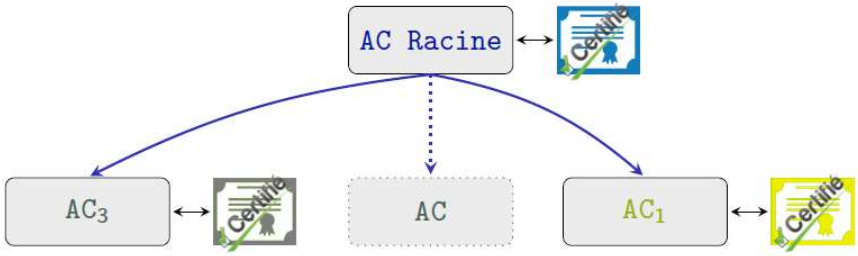
8.3. Autorité de certification (AC)

- Principes
- Pour être valide, un certificat doit être signé par une AC.
- Une AC possède son propre couple (clé privée, clé publique) associé à un certificat qui peut être, soit auto-signé, soit signé par une autre AC.
- La confiance accordée à une AC est héritée par toutes les ACs filles
- Deux ACs peuvent s'entendre afin de signer chacune le certificat de l'autre : c'est la notion de confiance croisée.
- L'AC est garante des informations contenues dans les certificats qu'elle délivre.

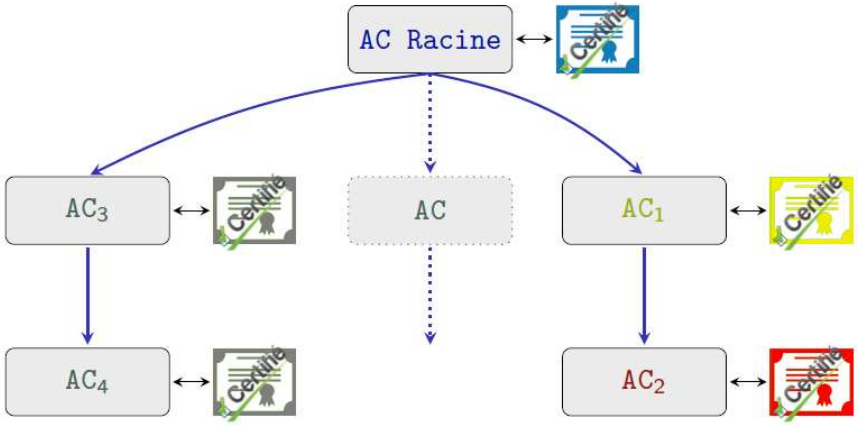
8.3. Autorité de certification (AC)



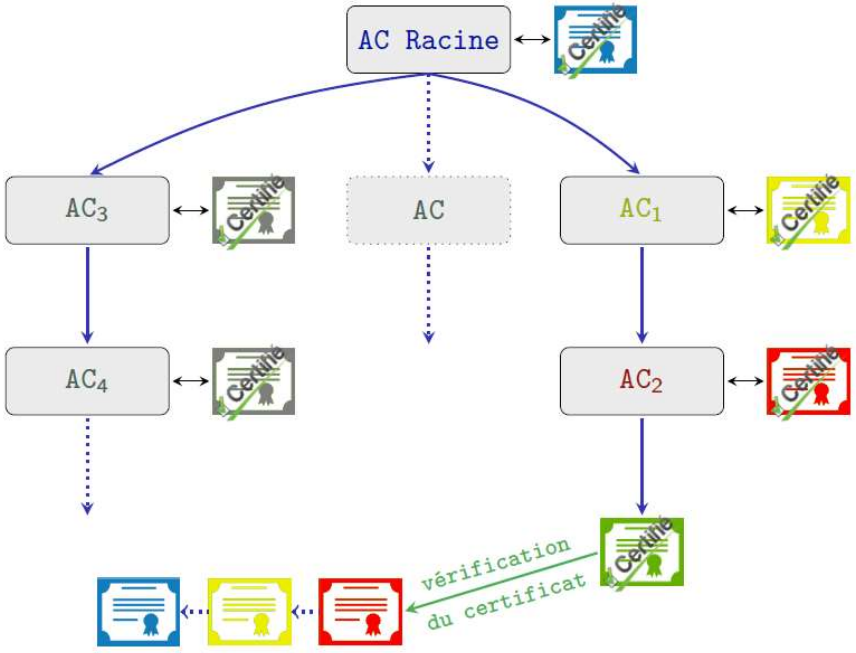
8.3. Autorité de certification (AC)



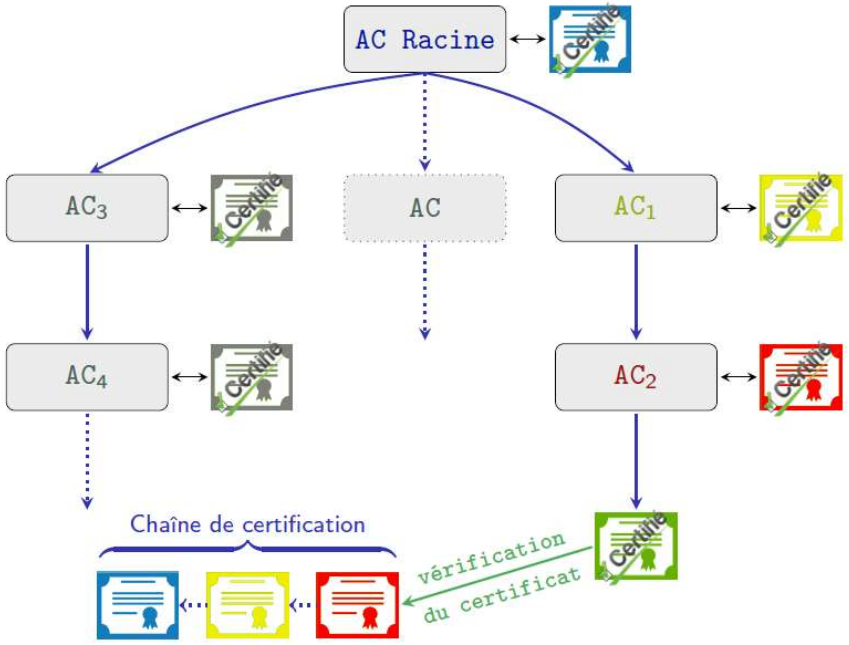
8.3. Autorité de certification (AC)



8.3. Autorité de certification (AC)



8.3. Autorité de certification (AC)



8.4. Structure d'une Infrastructure de gestion de clés

- **Une définition formelle**
- Une IGC (Public Key Infrastructure - PKI) est un ensemble de personnes, matériels et logiciels, régis par des règles et des procédures et permettant de **créer**, **gérer** et **distribuer** des certificats X.509.
- une entité **administrative** et une entité **technique**
- une IGC assure les missions suivantes :
  - Création et révocation des certificats X.509,
  - Diffusion et publication des certificats X.509 (via un annuaire LDAP par exemple),
  - Plus rarement, un service de séquestre et de recouvrement des clés privées. Ce service est bien sûr très utile en cas de perte de la clé privée de votre certificat. Le problème est que votre clé privée perd toute **légitimité** car vous la partagez avec un tiers

8.4. Structure d'une Infrastructure de gestion de clés

Les éléments constitutifs d'une IGC

- **Autorité d'Enregistrement (AE)** : elle reçoit et traite les demandes de création, renouvellement et révocation de certificats. Elle doit notamment s'assurer de l'identité des demandeurs.
- **Opérateur de Certification (OC) :** il effectue toutes les opérations demandées par l'AC nécessitant la clé privée de celle-ci. Il n'est en principe pas connecté au réseau.
- **Service de Publication (SP) :** il met à disposition de tous, via un annuaire (le plus souvent LDAP), les certificats issus de l'IGC, le certificat de l'AC et éventuellement les listes de révocation (CRL).
- **Service de Validation (SV) :** il permet à tout utilisateur de vérifier la validité d'un certificat (expiration, vol/perte de la clé privée associée,).
- **Service de Séquestre (SS)** : il stocke au sein de l'IGC les couples (clé privée, clé publique) des certificats produits. **Dangereux** !

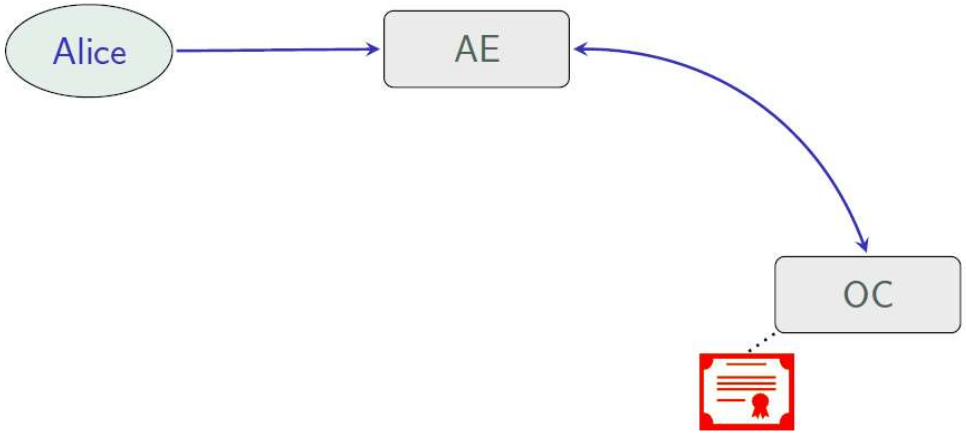
Demande de certificat

Alice souhaite obtenir un certificat

Demande de certificat

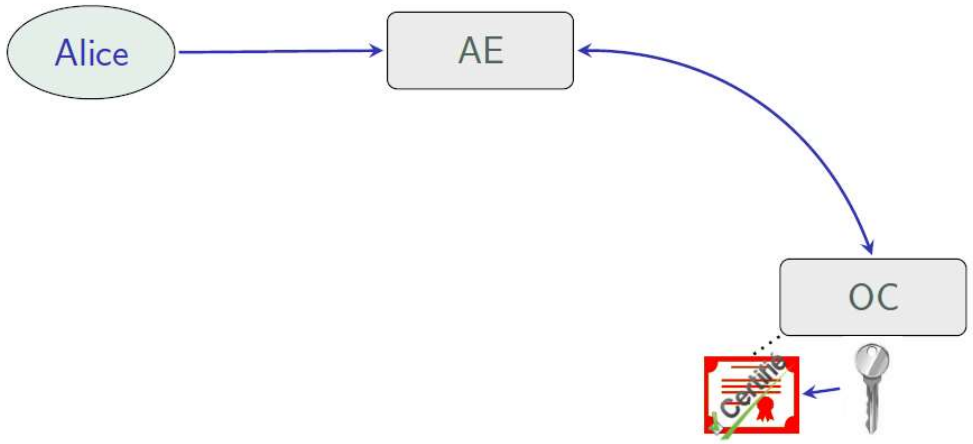
Alice envoie sa requête à l'AE

Demande de certificat



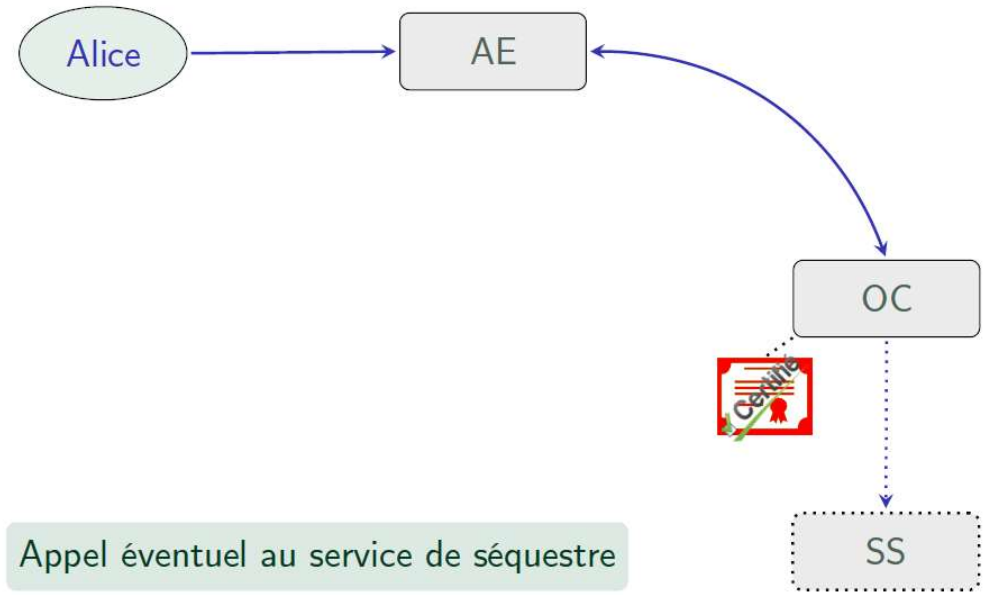
L'AE vérifie l'identité d'Alice et transmet à l'OC

Demande de certificat

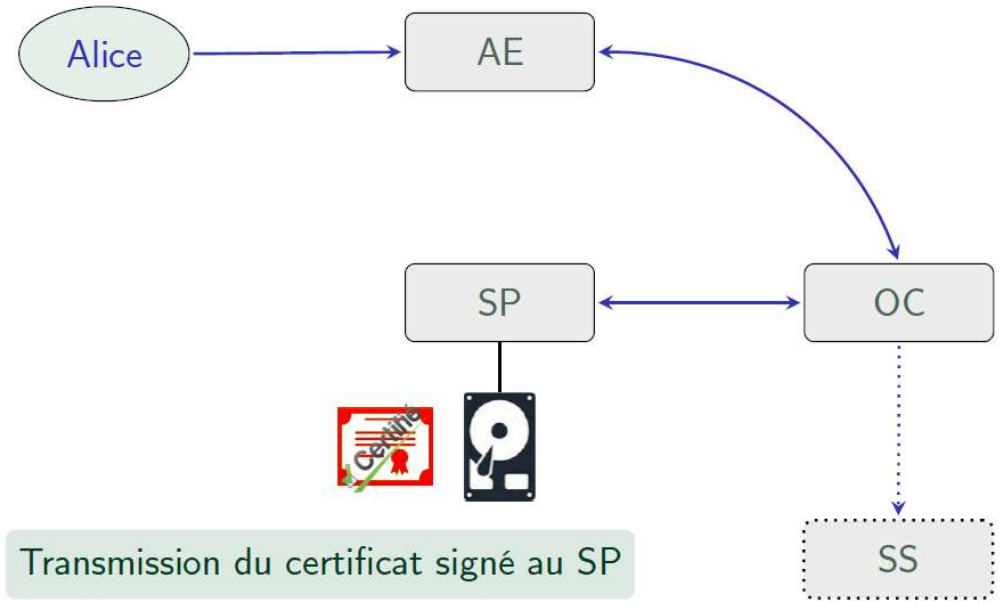


L'OC signe le certificat avec la clé privée de l'AC

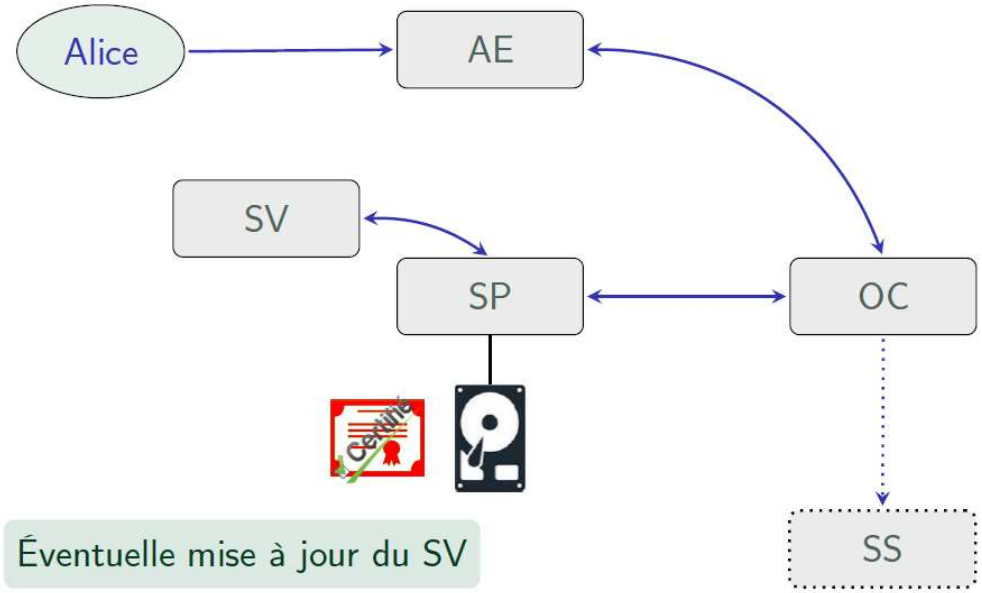
Demande de certificat



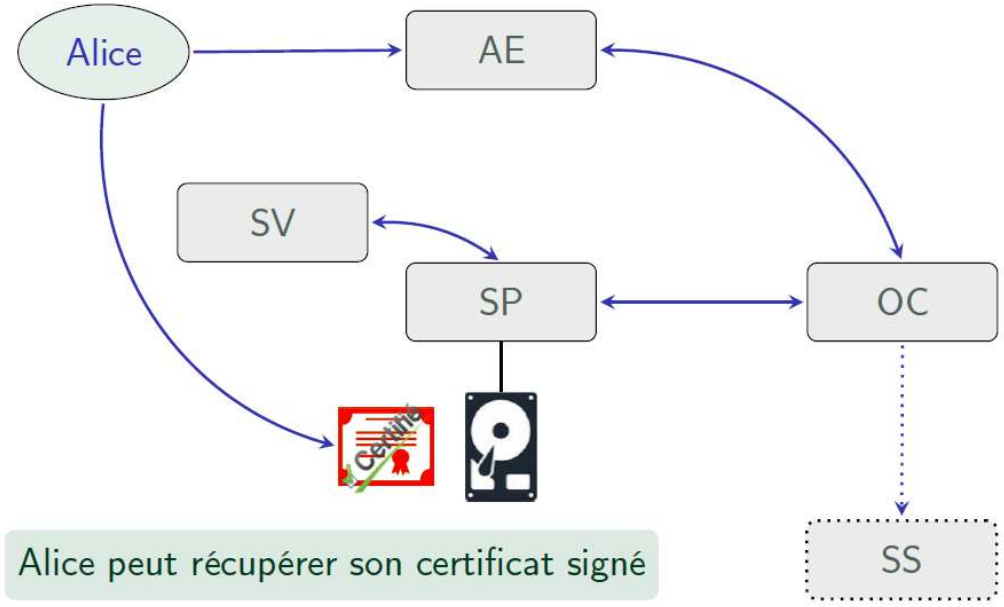
Demande de certificat



Demande de certificat



Demande de certificat



9. Cryptanalyse

9.1 Types d'attaques

On doit distinguer entre les moyens d'attaques (ou types d'attaques) d'un adversaire et les buts d'attaques d'un adversaire. **L'attaquant connaît tout les détails de l'algorithme de chiffrement/déchiffrement et qu'il ne lui manque que la clef spécifique pour le chiffrement** (axiome fondamental de Kerckhoffs).

Les 4 types d'attaques :

- **Attaque à texte crypté uniquement** : L'attaquant ne dispose que d'un ou plusieurs messages chiffrés qu'il souhaite déchiffré. C'est le type d'attaque le plus difficile.
- **Attaque à texte chiffré connu** : Le cryptanalyste a non seulement accès aux textes chiffrés de plusieurs messages, mais aussi aux textes clairs correspondants. La tâche est de retrouver la ou les clés qui ont été utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer d'autres messages chiffrés avec ces mêmes clés.
- **Attaque à texte clair choisi** : (IND − CPA) L'opposant a accès à une machine chiffrante : Le cryptanalyste a non seulement accès aux textes chiffrés et aux textes clairs correspondants, mais de plus il peut choisir les textes en clair. Cette attaque est plus efficace que l'attaque à texte clair connu, car le cryptanalyste peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clé.
- **Attaque à texte chiffré choisi** : (IND − CCA) : L'opposant a accès à une machine déchiffrante: Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer. Les textes déchiffrés lui sont alors fournis. Par exemple, le cryptanalyste a un dispositif qui ne peut être désassemblé et qui fait du déchiffrement automatique. Sa tâche est de retrouver la clé.

9.2 Evaluation d’un algo

- Echelle de succès :
  - Cassage complet : l’attaquant découvre la clé.
  - Déduction globale : l’attaquant découvre des fonctions équivalentes aux fonctions de chiffrement et de déchiffrement sans pour autant connaître la clé.
  - Déduction locale : l’attaquant peut déchiffrer un ou plusieurs nouveaux messages chiffrés.
  - Déduction d’information : L’attaquant obtient de l’information sur la clé ou sur des messages chiffrés.

- Critères d’évaluation :
  - Temps : le nombre d’opérations de bases nécessaires
  - Espace : la quantité de mémoire maximale nécessaire
  - Données : le nombre de messages clairs/chiffrés nécessaires