

Chapitre 1 - Introduction

Alexandra Bruasse-Bac

Historique

- Premières traces il y a 4000 ans (Egypte)

Historique

- Premières traces il y a 4000 ans (Egypte)
- Essentiellement 20ème siècle

Historique

- Premières traces il y a 4000 ans (Egypte)
- Essentiellement 20ème siècle
- Jusqu'aux années 60 : surtout l'armée

Historique

- Premières traces il y a 4000 ans (Egypte)
- Essentiellement 20ème siècle
- Jusqu'aux années 60 : surtout l'armée
- Années 70 : Feistel (IBM)
1977 - **DES**

Historique

- Premières traces il y a 4000 ans (Egypte)
- Essentiellement 20ème siècle
- Jusqu'aux années 60 : surtout l'armée
- Années 70 : Feistel (IBM)
1977 - **DES**
- 1976 : Diffie-Hellman, *New Directions in Cryptography*
Cryptographie à clé publique

Historique

- Premières traces il y a 4000 ans (Egypte)
- Essentiellement 20ème siècle
- Jusqu'aux années 60 : surtout l'armée
- Années 70 : Feistel (IBM)
1977 - **DES**
- 1976 : Diffie-Hellman, *New Directions in Cryptography*
Cryptographie à clé publique
- 1978 : Rivest, Shamir, Adelman
RSA

Historique

- Premières traces il y a 4000 ans (Egypte)
- Essentiellement 20ème siècle
- Jusqu'aux années 60 : surtout l'armée
- Années 70 : Feistel (IBM)
1977 - **DES**
- 1976 : Diffie-Hellman, *New Directions in Cryptography*
Cryptographie à clé publique
- 1978 : Rivest, Shamir, Adelman
RSA
- 1985 : **El Gamal**

Historique

- Premières traces il y a 4000 ans (Egypte)
- Essentiellement 20ème siècle
- Jusqu'aux années 60 : surtout l'armée
- Années 70 : Feistel (IBM)
1977 - **DES**
- 1976 : Diffie-Hellman, *New Directions in Cryptography*
Cryptographie à clé publique
- 1978 : Rivest, Shamir, Adelman
RSA
- 1985 : **El Gamal**
- 1991 : Signature Digitale ISO/EIC 9796 (RSA)

Historique

- Premières traces il y a 4000 ans (Egypte)
- Essentiellement 20ème siècle
- Jusqu'aux années 60 : surtout l'armée
- Années 70 : Feistel (IBM)
1977 - **DES**
- 1976 : Diffie-Hellman, *New Directions in Cryptography*
Cryptographie à clé publique
- 1978 : Rivest, Shamir, Adelman
RSA
- 1985 : **El Gamal**
- 1991 : Signature Digitale ISO/EIC 9796 (RSA)
- 1994 : Digital Signature Standard (El Gamal)

Buts de la cryptographie

Etude de techniques mathématiques liées aux aspects suivants :

- **Confidentialité**
informations secrètes, privées

Buts de la cryptographie

Etude de techniques mathématiques liées aux aspects suivants :

- **Confidentialité**
informations secrètes, privées
- **Intégrité des données**
empêcher la modification non autorisée des données

Buts de la cryptographie

Etude de techniques mathématiques liées aux aspects suivants :

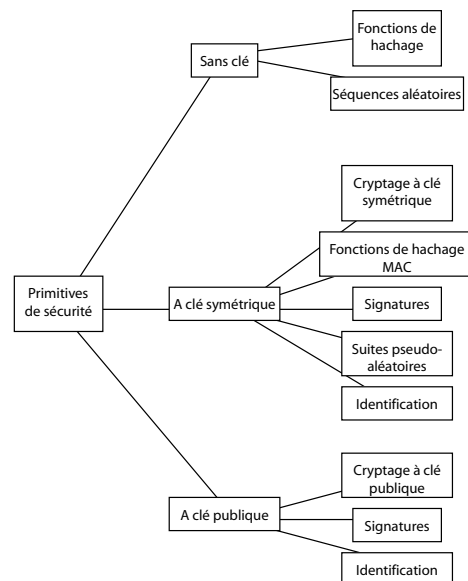
- **Confidentialité**
informations secrètes, privées
- **Intégrité des données**
empêcher la modification non autorisée des données
- **Authentification**
Relié à l'identification (des entités et des informations)

Buts de la cryptographie

Etude de techniques mathématiques liées aux aspects suivants :

- **Confidentialité**
informations secrètes, privées
- **Intégrité des données**
empêcher la modification non autorisée des données
- **Authentification**
Relié à l'identification (des entités et des informations)
- **Non répudiation**
Garantir qu'un service ou des privilèges accordés ne seront pas retirés sans raison

Buts de la cryptographie



Terminologie et concepts de base

Terminologie

- Alphabet (Σ)
- Espace des messages ($\mathcal{M} = \Sigma^*$)

Terminologie

- Alphabet (Σ)
- Espace des messages ($\mathcal{M} = \Sigma^*$)
- Espace des codes ($\mathcal{C} = \Sigma'^*$)

Terminologie

- Alphabet (Σ)
- Espace des messages ($\mathcal{M} = \Sigma^*$)
- Espace des codes ($\mathcal{C} = \Sigma'^*$)
- Espace des clés (\mathcal{K})

Terminologie

- Alphabet (Σ)
- Espace des messages ($\mathcal{M} = \Sigma^*$)
- Espace des codes ($\mathcal{C} = \Sigma'^*$)
- Espace des clés (\mathcal{K})

- Fonction de cryptage
pour tout $e \in \mathcal{K}$, bijection $E_e : \mathcal{M} \rightarrow \mathcal{C}$

- Alphabet (Σ)
 - Espace des messages ($\mathcal{M} = \Sigma^*$)
 - Espace des codes ($\mathcal{C} = \Sigma'^*$)
 - Espace des clés (\mathcal{K})
-
- Fonction de cryptage
 - Fonction de décryptage
- pour tout $d \in \mathcal{K}$, bijection $D_d : \mathcal{C} \rightarrow \mathcal{M}$

- Alphabet (Σ)
 - Espace des messages ($\mathcal{M} = \Sigma^*$)
 - Espace des codes ($\mathcal{C} = \Sigma'^*$)
 - Espace des clés (\mathcal{K})
-
- Fonction de cryptage
 - Fonction de décryptage
 - Schéma de codage
- ensembles $\{E_e, e \in \mathcal{K}\}$ et $\{D_d, d \in \mathcal{K}\}$: pour tout $e \in \mathcal{K}$ il existe un unique $d \in \mathcal{K}$ avec $D_d = E_e^{-1}$
(e, d) **paire de clés**

Cryptage à clés symétriques

Cryptage symétrique

Cryptage symétrique

Schéma de codage tel que e et d se déduisent aisément l'une de l'autre

Exemple :

Cas où $e = d$

Cryptage symétrique

Cryptage symétrique

Schéma de codage tel que e et d se déduisent aisément l'une de l'autre

- **Cryptage par bloc**

Texte décomposé en blocs de longueur t sur l'alphabet Σ

Cryptage bloc par bloc

- DES
- AES
- IDEA
- Blowfish ...

Cryptage symétrique

Cryptage symétrique

Schéma de codage tel que e et d se déduisent aisément l'une de l'autre

- **Cryptage par bloc**

- **Cryptage d'un flux**

Cryptage caractère par caractère

Eviter la propagation des erreurs, équipements aux performances limitées

- RC4 (propriétaire)
- SEAL
- LFSR-based ...

Signatures digitales

Primitive indispensable pour l'authentification

Processus de **signature** : transformer le message et une information secrète en une *signature*

Signatures digitales

Primitive indispensable pour l'authentification

Processus de **signature** : transformer le message et une information secrète en une *signature*

- Entité A
- **Transformation de signature**

$$S_A : \mathcal{M} \rightarrow \mathcal{S}$$

Signatures digitales

Primitive indispensable pour l'authentification

Processus de **signature** : transformer le message et une information secrète en une *signature*

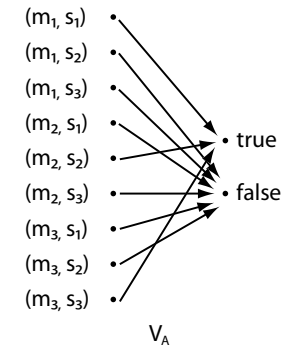
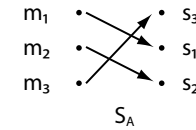
- Entité A
- Transformation de signature

$$S_A : \mathcal{M} \rightarrow \mathcal{S}$$

- Transformation de vérification

$$V_A : \mathcal{M} \times \mathcal{S} \rightarrow \{\text{true}, \text{false}\}$$

Signatures digitales



Cryptage à clés publiques

Cryptage à clé publique

Cryptage à clé publique

Schéma de codage tel qu'il est impossible de calculer d à partir de e

Cryptage à clé publique

Cryptage à clé publique

Schéma de codage tel qu'il est impossible de calculer d à partir de e

- Clé publique (cryptage) : e
- Clé privée (décryptage) : d

Cryptage à clé publique

Cryptage à clé publique

Schéma de codage tel qu'il est impossible de calculer d à partir de e

- Clé publique (cryptage) : e
- Clé privée (décryptage) : d

Nécessité d'authentifier les clés publiques

Signatures digitales et clés publiques

Schéma de cryptage publique réversible

Schéma tel que $\mathcal{M} = \mathcal{C}$

Signatures digitales et clés publiques

Schéma de cryptage publique réversible

Schéma tel que $\mathcal{M} = \mathcal{C}$

$$D_d(E_e(m)) = E_e(D_d(m)) \quad \forall m \in \mathcal{M}$$

Signatures digitales et clés publiques

Schéma de cryptage public réversible

Schéma tel que $\mathcal{M} = \mathcal{C}$

Schéma de signature digitale :

- Espace de messages : \mathcal{M}
- Espace de signatures : $\mathcal{S} = \mathcal{M}$
- (e, d) paire de clés de A : $S_A = D_d$
- Fonction de vérification :

$$V_A(s) = \begin{cases} \text{true} & \text{si } E_e(s) = m \\ \text{false} & \text{sinon} \end{cases}$$

Signatures digitales et clés publiques

Schéma de cryptage public réversible

Schéma tel que $\mathcal{M} = \mathcal{C}$

Schéma de signature digitale :

- Espace de messages : \mathcal{M}
- Espace de signatures : $\mathcal{S} = \mathcal{M}$
- (e, d) paire de clés de A : $S_A = D_d$
- Fonction de vérification :

$$V_A(s) = \begin{cases} \text{true} & \text{si } E_e(s) = m \\ \text{false} & \text{sinon} \end{cases}$$

Forge existentielle

Signatures digitales et clés publiques

- Espace de messages : $\mathcal{M}' \subseteq \mathcal{M}$
- Espace de signatures : $\mathcal{S} = \mathcal{M}$
- (e, d) paire de clés de A :

$$S_A = D_d$$

- Fonction de vérification :

$$V_A(s) = \begin{cases} \text{true} & \text{si } E_e(s) \in \mathcal{M}' \\ \text{false} & \text{sinon} \end{cases}$$

Symétrique vs. publique

Symétrique

- **Avantages**
 - Peuvent avoir des débits élevés
 - Clé assez courtes
 - Outil de base pour d'autres primitives (nombres pseudo-aléatoires, signatures digitales efficaces)
 - Composition

- **Inconvénients**

Publique

- **Avantages**
- **Inconvénients**

Symétrique vs. publique

Symétrique

- Avantages
- Inconvénients
 - Pour une communication : clé secrète partagée
 - Gestion des clés : autorité de centralisation (TTP - Trusted Third Party)
 - Pour une communicationé : changement régulier des clés
 - Signature digitale : clés importantes ou TTP

Publique

- Avantages
- Inconvénients

Symétrique vs. publique

Symétrique

- Avantages
- Inconvénients

Publique

- Avantages
 - Seule la clé privée doit être protégée
 - Administration des clés simplifiée
 - Une paire de clé peut rester inchangée pendant un temps important sans problème de sécurité
 - Signature digitale souvent efficace
 - Dans un réseau de grande tailles : moins de clés nécessaires

Symétrique vs. publique

Symétrique

- Avantages
- Inconvénients

Publique

- Avantages
- Inconvénients
 - Débits bas
 - Taille des clés plus importante
 - Aucun schéma prouvé comme étant sûr

Fonctions de hachage

Fonctions de hachage

Fonction de hachage

$$h : \Sigma^* \rightarrow \underbrace{\Sigma^n}_{\text{Valeur de hachage}}$$

Fonctions de hachage

Fonction de hachage

$$h : \Sigma^* \rightarrow \underbrace{\Sigma^n}_{\text{Valeur de hachage}}$$

Collision

Couple (x, y) tel que $h(x) = h(y)$

Fonctions de hachage

Fonction de hachage

$$h : \Sigma^* \rightarrow \underbrace{\Sigma^n}_{\text{Valeur de hachage}}$$

Collision

Couple (x, y) tel que $h(x) = h(y)$

Principales applications :

- Signatures digitales
- Intégrité des données

Classes d'attaque et modèles de sécurité

Principaux types d'attaques

- Attaque en force
- Attaque à l'aide de texte chiffré seulement

Le cryptographe cherche à déduire le message d'origine ou la clé à partir du texte crypté.

Un système vulnérable à ce type d'attaques est complètement non sûr

Principaux types d'attaques

- Attaque en force
- Attaque à l'aide de texte chiffré seulement
- Attaque à l'aide de texte clair

Le cryptographe dispose des messages ou parties de message clairs et de leur version chiffrée.

Principaux types d'attaques

- Attaque en force
- Attaque à l'aide de texte chiffré seulement
- Attaque à l'aide de texte clair
- Attaque à l'aide de texte clair choisi

Le cryptographe dispose des messages clairs et de leur version chiffrée. Il a aussi la possibilité de tester des messages et d'obtenir le résultat chiffré.

Chiffrements asymétriques

Principaux types d'attaques

- Attaque en force
- Attaque à l'aide de texte chiffré seulement
- Attaque à l'aide de texte clair
- Attaque à l'aide de texte clair choisi
- Attaque d'une tierce personne

Dans une transaction entre deux entités, une troisième entité s'interpose entre les deux et termine la transaction normalement en captant les messages et en transmettant d'autres messages.