Chapitre 4: Bases cryptographiques

Polytech Nancy

Année 2021/2022

Bases cryptographiques

1. Principes
2. Cryptographie symétrique
3. Cryptographie asymétrique
4. Checksums / MAC
5. Fonctions à sens unique
6. Principes annexes

Point route

1 Principes

2 Cryptographie symétrique

3 Cryptographie asymétrique

4 Checksums / MAC

5 Fonctions à sens unique

6 Principes annexes

Principes : Chiffrement des messages

Objectifs : confidentialité, authentification et intégrité.

Chiffrement symétrique

- Les partenaires partagent une clef secrète unique.
- Cette même clef est utilisée pour chiffrer et déchiffrer.

Chiffrement asymétrique

- Deux clefs complémentaires : l'une publique, l'autre privée.
- La première sert à tout le monde à chiffrer, la seconde sert au propriétaire à déchiffrer.

Principes : Signature des messages

Objectifs : authentification, intégrité et non répudiation.

Fonctions de hachage

- Fonction à sens unique

Chiffrement asymétrique

- Deux clefs complémentaires : l'une privée, l'autre publique.
- La première sert au propriétaire à signer, la seconde sert à tout le monde à déchiffrer.

Principes : Fraîcheur des messages

Objectifs : éviter l'utilisation d'anciennes informations.

Nonces

- *Numbers used only once*
- Nombres engendrés au cours de l'exécution du protocole.

Timestamps

- Datation du message.

Clefs de session

- Clefs fraîches pour le chiffrement (symétrique).
- Engendrées au cours de l'exécution du protocole.

Point route

1 Principes

2 Cryptographie symétrique

3 Cryptographie asymétrique

4 Checksums / MAC

5 Fonctions à sens unique

6 Principes annexes

Cryptographie symétrique

Historiquement la plus ancienne.

Méthodes variées

- Chiffrement par substitution et transposition, avec ou sans clef.
- Chiffrement par blocs.
- Chiffrement à flots.

Chiffrement par substitution et transposition

Sans clef

- Chiffrement de Jules César : décalage de 3 lettres.
- Chiffrement ROT13 : décalage de 13 lettres.

Mécanismes très simples, mais protection limitée.

Chiffrement par substitution et transposition

Avec clef

- Chiffrement de Blaise de Vigenère : une clef indique les décalages à effectuer.
- Chiffrement par addition (XOR).
- Chiffrement par dictionnaire : substitution de mots.
- Chiffrement par transposition : ordre des symboles modifié.

Remarque : Enigma utilisait un chiffrement par substitutions, mais plus complexe.

Chiffrement par blocs

Les plus connus

- DES (Data Encryption Standard), 1976
- Triple DES
- AES (Advanced Encryption Standard), 2001

Chiffrement par blocs

DES

- Découpage du message en blocs de 64 bits.
- Clef symétrique de 56 bits (+8 bits de parité) ; calcul de 16 sous-clefs K_i de 48 bits.
- Chaque bloc est scindé en deux blocs de 32 bits : L_0, R_0.
- Chiffrement par 16 cycles consécutifs :
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

  où f combine permutations et substitutions.

Chiffrement par blocs

DES, mode ECB

- Constitution d'un carnet de codage électronique.
- Chaque bloc est chiffré séparément.
  $\Rightarrow$ constitution d'un carnet de blocs en clair/chiffrés.
- *Fuite d'information :* blocs chiffrés identiques $\rightarrow$ blocs en clair identiques.
- Pas de contrôle d'intégrité (le déchiffrement n'indique pas si un bloc a été remplacé, enlevé ou dupliqué).

Chiffrement par blocs

DES, mode CBC

- Chiffrement avec chaînage des blocs.
- Chiffrement d'un nouveau bloc par XOR du bloc en clair (T_j) avec le précédent bloc chiffré (C_j).
  - $C_0 = VI$ (vecteur d'initialisation)
  - Chiffrement : $C_i = Enc_{K_i}(T_i \oplus C_{i-1})$
  - Déchiffrement : $T_i = C_{i-1} \oplus Dec_{K_i}(C_i)$
- *Correction :*
  - $C_{i-1} \oplus Dec_{K_i}(C_i) = C_{i-1} \oplus Dec_{K_i}(Enc_{K_i}(T_i \oplus C_{i-1}))$
  - $= C_{i-1} \oplus (T_i \oplus C_{i-1}) = T_i$

Chiffrement par blocs

Propriétés de DES, mode CBC

- Textes clairs identiques $\rightarrow$ codages différents.
- Le codage d'un bloc dépend de tous les blocs précédents.
- Auto-synchronisation : en cas d'erreur (changement de bit ou perte d'un bloc) dans C_j mais pas dans C_{j+1}, alors C_{j+2} sera correctement déchiffré.

Chiffrement par blocs

3DES

- 3 chiffements consécutifs avec DES.
- 3 clefs différentes.

AES

- Blocs plus grands.
- Clefs plus grandes.
- Combinaison de multiples transformations, permutations et sélections.

Chiffrement à flots

Principe :

- Chiffrement effectué bit par bit sur le modèle de Vernam (aussi appelé *One Time Pad*, ou masque jetable).
- Une suite de bits de chiffrement est engendrée au fur et à mesure, pour les ajouter (XOR) au flux à chiffrer.

Chiffrement considéré comme le seul totalement sûr. . . mais pas pratique du tout !

Limites du chiffrement symétrique

Partage de clefs

- Deux individus voulant communiquer doivent partager une clef secrète.
- Comment échanger la clef ?
- Quelle est la durée de validité de la clef ?
- Comment gérer les clefs pour un groupe d'individus voulant communiquer ?

Point route

1 Principes

2 Cryptographie symétrique

3 Cryptographie asymétrique

4 Checksums / MAC

5 Fonctions à sens unique

6 Principes annexes

Cryptographie asymétrique

Concept inventé par Diffie, Hellmann et Merkle en 1976.

Principe :

Deux clefs complémentaires (l'une privée, l'autre publique)

Applications :

- échange de messages
- distribution de clefs (symétriques) de sessions
- signatures digitales
- certificats

Fondements théoriques

Basée sur la difficulté de factoriser les entiers :

- Facile de trouver 2 grands nombres premiers.
- Difficile de factoriser le produit de 2 nombres premiers.

Déterministe :

- Pour chaque texte en clair et chaque clef publique, un seul texte chiffré.

Fondements théoriques

Petit théorème de Fermat :

- Soient p premier, $a > 0$ et a non divisible par p,
  - $a^{p-1} \equiv 1 \pmod{p}$
  - $a^p \equiv a \pmod{p}$

Fonction totient d'Euler :

- Soit p premier, $\phi(p) = p - 1$
- Soient p, q premiers, $n = p * q$, $\phi(n) = (p-1) * (q-1)$

Théorème d'Euler :

- Soient a, n,
  - $a^{\phi(n)} \equiv 1 \pmod{n}$
  - $a^{\phi(n)+1} \equiv a \pmod{n}$

Cryptographie asymétrique

Exemples de systèmes :

- Merkle-Hellman
- Rivest-Shamir-Adleman
- Rabin
- El Gamal

Cryptographie asymétrique

RSA

- Génération de clefs :
  - Choisir p et q, grands nombres premiers.
  - Calculer $n = pq$ et $\phi(n) = (p-1)(q-1)$.
  - Choisir e (pas trop grand) premier avec $\phi(n)$.
  - Calculer d, unique, tel que $ed \equiv 1 \pmod{\phi(n)}$ (algorithme d'Euclide).
  - Effacer p et q.
  - Clef publique : (n, e).
  - Clef privée : (n, d).
- Chiffrement de m : $c \equiv m^e \pmod{n}$
- Déchiffrement de c : $m \equiv c^d \pmod{n}$

Cryptographie asymétrique

RSA : justification

- $m^{p-1} \equiv 1 \pmod{p}$ pour $m \neq 0$ par Fermat
- $m^{\phi(n)} \equiv 1 \pmod{p}$ car $p-1$ divise $\phi(n)$
- $m^{k\phi(n)} \equiv 1 \pmod{p}$ pour tout k
- $m^{k\phi(n)+1} \equiv m \pmod{p}$ pour tout k et tout m
- $m^{ed} \equiv m \pmod{p}$ car $ed \equiv 1 \pmod{\phi(n)}$, donc $\exists k, ed = 1 + k\phi(n)$
- $m^{ed} \equiv m \pmod{q}$ même raisonnement
- $m^{ed} \equiv m \pmod{n}$ par Fermat/Euler
- Donc : $c^d \equiv (m^e)^d \equiv m \pmod{n}$

Cryptographie symétrique versus asymétrique

Symétrique :

Avantages :

- rapidité (jusqu'à un facteur 1000)
- facilement implantable sur hardware
- taille de la clef : 128 bits (mémorisable)

Inconvénients :

- Nombre de clefs à gérer
- Distribution des clefs
- Propriétés parfois difficiles à réaliser

Cryptographie symétrique versus asymétrique

Asymétrique :

Avantages :

- nombre réduit de clefs à distribuer
- distribution facilitée
- permet facilement de signer des messages

Inconvénients :

- taille importante des clefs
- vitesse de chiffrement

Cryptographie symétrique versus asymétrique

Problèmes communs :

- La gestion des clefs « secrètes » reste le maillon faible
- La sécurité est basée sur des arguments empiriques et non théoriques

Point route

1 Principes

2 Cryptographie symétrique

3 Cryptographie asymétrique

4 Checksums / MAC

5 Fonctions à sens unique

6 Principes annexes

Checksums / MAC

Objectif : protection de l'intégrité d'un message.
(Message Authentication Code)

Principe :

- Utilisation d'une clef secrète symétrique
- Décomposition d'un message en blocs de taille prédéfinie
- Chiffrement combiné d'un bloc et du résultat du chiffrement appliqué aux blocs précédents

Avantages :

1. Résultat de petite taille (connue à l'avance)
2. Toute altération d'un bloc initial modifie le résultat
3. Et sans connaître la clef utilisée, c'est encore plus difficile

Checksums / MAC

Utilisation :

- Envoi du message accompagné de son MAC
- Vérification : calculer le MAC du message reçu et le comparer avec le MAC reçu
- Pour garantir confidentialité et intégrité, nécessité de traiter deux fois le messsage

Remarque : la même clef symétrique peut être utilisée pour des envois de messages dans les deux sens.

Point route

1 Principes

2 Cryptographie symétrique

3 Cryptographie asymétrique

4 Checksums / MAC

5 Fonctions à sens unique

6 Principes annexes

Fonctions à sens unique

Une fonction à sens unique (ou de hachage) est une variante (moderne) du MAC.

Quelques techniques (trop ?) simples :

- modulo
- amputation ou extraction
- compression
- pliage
- multiplication
- etc.

Fonctions à sens unique

Une fonction de hachage $H()$ opère sur un message m de longueur arbitraire et fournit une valeur h de longueur fixe.

Propriétés ciblées :

- Étant donné m, il est facile de calculer $H(m)$
- Étant donné $H(m)$, il est difficile de calculer m (sens unique)
- Étant donné m, il est difficile de trouver un autre m' tel que $H(m) = H(m')$ (collisions faibles)

Remarque : La troisième propriété peut être remplacée par

- Il est difficile de trouver deux messages m et m' tels que $H(m) = H(m')$ (collisions fortes)

Intérêt de la condition forte sur les collisions

Attaque d'un protocole de signature de contrat par signature de l'empreinte.

1. Alice prépare 2 versions d'un contrat, l'une favorable à Bob (*docf*), l'autre défavorable (*docd*).
2. Alice introduit des modifications subtiles dans chaque document (espaces supplémentaires et retours à la ligne) et calcule les empreintes de chacun.
3. Alice compare les empreintes jusqu'à en trouver 2 qui concordent : $H(docf) = H(docd)$.
4. Alice présente *docf* à Bob qui signe l'empreinte $H(docf)$.
5. Alice peut ensuite convaincre un juge que Bob a signé *docd*.

Remarque : si la fonction de hachage produit des empreintes de 64 bits il suffit d'engendrer 2^{32} versions de chaque document pour avoir une bonne chance d'obtenir 2 empreintes égales.

Intérêt de la condition forte sur les collisions

Paradoxe des anniversaires

Nombre minimal de personnes pour avoir plus d'une chance sur deux que...

- l'une d'entre elles soit née le même jour que vous ?
- deux d'entre elles soient nées le même jour ?

Intérêt de la condition forte sur les collisions

Paradoxe des anniversaires

Nombre minimal de personnes pour avoir plus d'une chance sur deux que...

- l'une d'entre elles soit née le même jour que vous ? 254
- deux d'entre elles soient nées le même jour ? 23

Intérêt de la condition forte sur les collisions

Paradoxe des anniversaires

Nombre minimal de personnes pour avoir plus d'une chance sur deux que...

- l'une d'entre elles soit née le même jour que vous ? 254
- deux d'entre elles soient nées le même jour ? 23

Et pour plus de 99% de chances : 1680 vs. 57 !

Fonctions à sens unique

Algorithmes classiques :

- MD4, MD5 (Message Digest, par Rivest)
- SHA-1, SHA-256, SHA-512,... (Secure Hash Algorithm)

Attention à leur utilisation !

- Naïve : ne protège pas
- Nécessité de les combiner avec d'autres techniques, comme le chiffrement symétrique

MACing versus hashing

Les deux méthodes sont toujours utilisées et ont chacunes avantages et inconvénients.

- Le hachage est beaucoup plus rapide que le MACing
- Le MACing demande le partage de clefs secrètes, ce qui complique la tâche d'un attaquant
- Le MACing apporte plus de confiance, car utilise une clef secrète partagée

Point route

1 Principes

2 Cryptographie symétrique

3 Cryptographie asymétrique

4 Checksums / MAC

5 Fonctions à sens unique

6 Principes annexes

Nonce

Number used only Once

- Nombre supposé unique...

Principe :

- Nombre engendré au cours de l'exécution du protocole
  $\rightarrow$ garantie de fraîcheur !
- Peut être utilisé en tant que tel, ou comme clef, identifiant,...

Nonce

Remarques

- Nécessite une fonction aléatoire, couvrant le type de l'objet engendré.
- Nécessite éventuellement une gestion des nonces rencontrés : mémorisation des anciens, comparaison avec les nouveaux, ...
- Comportement du protocole pouvant varier selon la gestion effectuée des nonces.

Mais qui dit nombre aléatoire, dit risque de collision...

Timestamp

Datage des messages

- Attachement de la date et de l'heure au message.
- Nécessité de protection de cette information (comme pour un MAC).
- Souvent utilisé en combinaison avec une période de validité.

Bases cryptographiques (résumé)

Chiffrement symétrique :

- pour chiffrer $\{M\}_K$,
- et déchiffrer $\{\{M\}_K\}_K = M$.

Chiffrement asymétrique :

- clef publique pour chiffrer $\{M\}_{PK_A}$,
- clef privée pour déchiffrer $\{\{M\}_{PK_A}\}_{SK_A} = M$ ou signer $\{M\}_{SK_A}$

Fonctions de hachage :

- non inversibles ; exemple : $M, \{h(M)\}_{SK_A}$

Crédits

- Bruce Schneier, *Cryptographie appliquée*, Vuibert
- Jon C. Graff, *Cryptography and E-commerce*, Wiley Tech Brief
- Laurence Herbiet, Université de Liège
- Équipe Pesto, LORIA
- Wikipedia