Vendredi 9 février 2024
2023–2024

Exercices

---

1 Mise en œuvre

Voici un exemple de mise en œuvre d'un système cryptographique utilisé par Alice et Bob pour s'échanger de grandes quantités de données.

- Utiliser un algorithme de cryptographie à clé secrète standardisé avec des clés de 80 bits et des blocs de 64 bits.
- Utiliser le mode CBC pour le contrôle d'intégrité.
- Utiliser l'algorithme ElGamal pour chiffrer les données, avec des clés de 200 bits.

Question.

- Fournissez (i) les bonnes pratiques, (ii) les mauvais choix, et (iii) la façon de les corriger.

Réponse.

- Utiliser un algorithme standardisé : c'est bien.
- Utiliser des clés de 80 bits : pas suffisant, il faut utiliser 128 bits aujourd'hui.
- Utiliser le mode CBC en intégrité : c'est bien.
- Utiliser ElGamal pour chiffrer les données : pas bien, ce n'est pas l'objectif de la cryptographie à clé publique. Il faut utiliser la cryptographie à clé secrète pour s'échanger de grandes quantités de données.
- Utiliser ElGamal avec des clés de 200 bits : c'est bien.

1.1 Protocole Diffie-Hellman

Soit $\mathbb{G}$ un groupe d'ordre premier p, et soit $g \in \mathbb{G}$. Alice et Bob veulent s'échanger une clé de façon sécurisée. Pour cela, Alice va choisir $a \in \mathbb{Z}_p^*$ pour calculer $A = g^a$ et Bob va choisir $b \in \mathbb{Z}_p^*$ pour calculer $B = g^b$.

Question.

- Si Alice envoie A à Bob et Bob envoie B à Alice, quelle sera la clé finalement partagée ? Quels seront les calculs effectués par Alice et Bob pour calculer cette clé ?
- Si Alice veut s'assurer que B provient bien de Bob, que faut-il rajouter à ce protocole ?

- Si maintenant Alice et Bob veulent utiliser cette clé pour s'échanger des données de façon confidentielle et intègre, pourquoi ne doivent-ils pas utiliser directement cette clé ? Que doivent-ils faire à la place ?

Réponse.

- Alice va calculer $K = B^a$ et Bob va calculer $K = A^b$. Comme $B^a = (g^b)^a = g^{ab} = (g^a)^b = A^b$, ils vont bien partager la même clé.
- Il faut que Bob signe la valeur B avant de l'envoyer à Bob. Il faut aussi rajouter un certificat numérique (provenant d'une autorité de certification) qui va permettre de faire de faire le lien entre la clé publique de signature et l'identité de Bob.
- Ils ne peuvent pas utiliser cette clé pour des problématiques d'usure de clé. Il ne faut jamais utiliser une clé cryptographique pour plusieurs besoins (ici confidentialité et intégrité). Il faut diversifier la clé K ainsi obtenue à l'aide de l'algorithme HKDF, qui va prendre en entrée la clé K et un contexte (tel que "confidentialité" et "intégrité").