Cryptographie et Sécurité - TD4

guillaume.postic@universite-paris-saclay.fr

Exercice 1 : intégrité des données

1. Pour une taille de bloc de 4 bits, calculer la somme de contrôle du message suivant, en appliquant un remplissage par des zéros : **011011110011**.

2. Le destinataire reçoit ce message avec une somme de contrôle égale à **1010**. Effectuer le calcul nécessaire pour conclure quant à l'intégrité du message.

Exercice 2 : fonction de hachage cryptographique

Pour le message **101100001** et pour une taille de bloc de 4 bits, calculer la valeur de hachage produite par une construction de Merkle-Damgård, dont la fonction de compression est un **XOR**. Vous utiliserez un renforcement de Merkle-Damgård sans encodage de la longueur et le vecteur d'initialisation **0100**.

Exercice 3 : signature numérique

Alice veut envoyer un message M à Bob, en l'authentifiant par DSA.
La valeur de hachage de M est $H(M) = 5$. La clé privée d'Alice est $x = 3$ et elle utilise un *nonce* $k = 4$. Les variables publiques sont les modules $p = 7$ et $q = 11$, ainsi que le générateur $g = 2$.

1. Quelle est la clé publique y d'Alice ?

2. Quelle est la signature envoyée par Alice ?

3. Quel calcul Bob effectue pour valider la signature ?

Exercice 4 : code d'authentification de message

Soit un chiffrement par bloc de 3 bits défini dans la table ci-dessous.

1. Calculer le CBC-MAC de m = `011011011`.
2. Calculer le CBC-MAC de m' = `101101101`.
3. Construisez un message m'', dont le CBC-MAC sera identique à celui de m'.

Entrée	Sortie	Entrée	Sortie
`000`	`001`	`100`	`010`
`001`	`100`	`101`	`110`
`010`	`111`	`110`	`011`
`011`	`000`	`111`	`101`