

Série de TD n°3-2

Questions de compréhension :

1. Quelle est la différence entre un chiffrement de bloc et un chiffrement de flux ?
2. Combien de clés sont nécessaires pour que deux personnes puissent communiquer via un chiffrement ?
3. Quelles sont les deux fonctions de base utilisées dans les algorithmes de cryptage
4. Quelles sont les deux approches générales pour attaquer un chiffrement ?

Exercice 1

Expliquer à l'aide de schémas comment deux utilisateurs peuvent-ils échanger des informations chiffrées et authentifiées (chiffrement et signature). On utilisera par exemple les algorithmes AES, RSA et SHA

Exercice 2 (Chiffrement asymétrique : RSA)

- Déchiffrer le message reçu $M=18$ chiffré avec la clé publique $(35;11)$.
- Chiffrer le message $M = 10$ avec la clé publique $(55;7)$. Calculer p ; q et d . Déchiffrer $C = 35$.