TD n°2

Exercice 1. (Protocole de Diffie-Hellman)

1) Exécuter le protocole de Diffie-Hellman pour les utilisateurs A et B qui possèdent, respectivement, les clés privées x=113 et y=97 pour g=20 et n=43.
2) Vérifier la validité de la clé partagée.
3) Ré-exécuter le protocole pour trois utilisateurs A, B, et C sachant que l'utilisateur C possède la clé privée z=13.
4) Vérifier la validité de la clé partagée.

Exercice 2. (Chiffrement de RSA)

On souhaite générer une paire de clés RSA à partir de n=1073 et $\Phi(n)=1008$.

1) Calculer les paramètres p et q.
2) Calculer la clé privée correspondante à e=17.
3) Chiffrer M=976, ensuite déchiffrer le résultat.

Exercice 3. (Chiffrement de Rabin)

1) Peut-on créer une paire de clés à partir de p=191 et q=199 ? Expliquer.
2) Calculer la paire de clés.
3) Chiffrer le message M=457, ensuite déchiffrer le résultat.

Exercice 4. (Chiffrement de Merkel-Hellman)

Soit la clé privée (A={1, 3, 5, 11, 25, 53, 101, 205, 512}, n=143, m=960).

1) Calculer la clé publique correspondante.
2) Chiffrer le message M=457, ensuite déchiffrer le résultat.

Exercice 5. (Chiffrement d'ElGamal)

1) Calculer une paire de clés pour p=97, g=13, et a=45.
2) Chiffrer M=81 pour b=35, ensuite déchiffrer le résultat.