IPC – Examen

- **Durée : 1h30.**
- **Documents, calculatrices et dictionnaires autorisés.**
- **Les exercices sont indépendants.**

Exercice 1

Compléter les affirmations suivantes :

1. Pour chiffrer un message, Bertrand utilise la clé de .
2. Pour déchiffrer un message, Arielle utilise la clé de .
3. Pour signer un message, Arielle utilise la clé de sur un hash du message.
4. Pour authentifier un message, Bertrand déchiffre le hash avec la clé de .

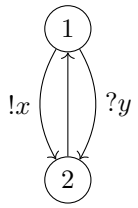
Exercice 2

Arielle et Bertrand utilisent le protocole de Diffie-Hellman. Ils se sont transmis $g = 11$ et $p = 223$, mais Laurent a réussi à infiltrer leur réseau et intercepte leurs messages ultérieurs. Laurent souhaite mettre en place une attaque de l'homme du milieu.

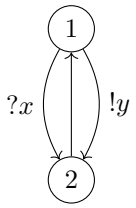
1. Rappeler en quoi consiste une telle attaque.
2. Les valeurs secrètes choisies par Arielle et Laurent sont 17 et 195. De plus, Bertrand envoie 26 sur le canal. Calculer les valeurs échangées entre les trois protagonistes.
3. Quelles sont les valeurs finales d'Arielle et de Bertrand ?

Exercice 3

Le fonctionnement de deux machines est représenté par les automates communicants suivants :



Machine A



Machine B

1. Dessiner les réseaux de Petri représentant le comportement du système
   (a) en utilisant un produit synchrone
   (b) en utilisant un produit asynchrone
2. Ces réseaux sont-ils bornés ? Justifier. Lorsqu'ils le sont, représenter le graphe des marquages accessibles.
3. Ces réseaux sont-il bloquants ? propres ? vivants ?