Université Clermont 1
IUT Info 1A
Codes et Cryptographie
Année 2010-2011

Yannick Do
Malika More
Gisèle Provost
Chafik Samir

Mode d'emploi des TPs de cryptographie

Les feuilles de TD et d'autres documents et informations
sont disponibles sur la page du cours sur l'ENT

Au début du TP

- Démarrer sous WINDOWS
- On vous distribue une copie papier du sujet
- Le fichier Maple que vous devez utiliser pour faire le TP se trouve sur l'ENT (dans le cours Codes et Cryptographie, cliquer sur documents puis sur crypto)
- Vous devez IMPÉRATIVEMENT copier le fichier dans votre compte sur le serveur pédagogique (pour pouvoir sauvegarder votre travail) et le renommer en utilisant vos noms (par exemple Dupond_Dupont.mw) (pour le confort des correcteurs)
- Il est préférable que vous écriviez aussi vos noms et votre groupe au début du fichier (il y a des lignes prévues exprès...)
- Le logiciel est Maple
- N'oubliez pas de sauvegarder régulièrement votre travail, pour limiter les conséquence des accidents qui ne manqueront pas de se produire ici ou là.

À la fin du TP

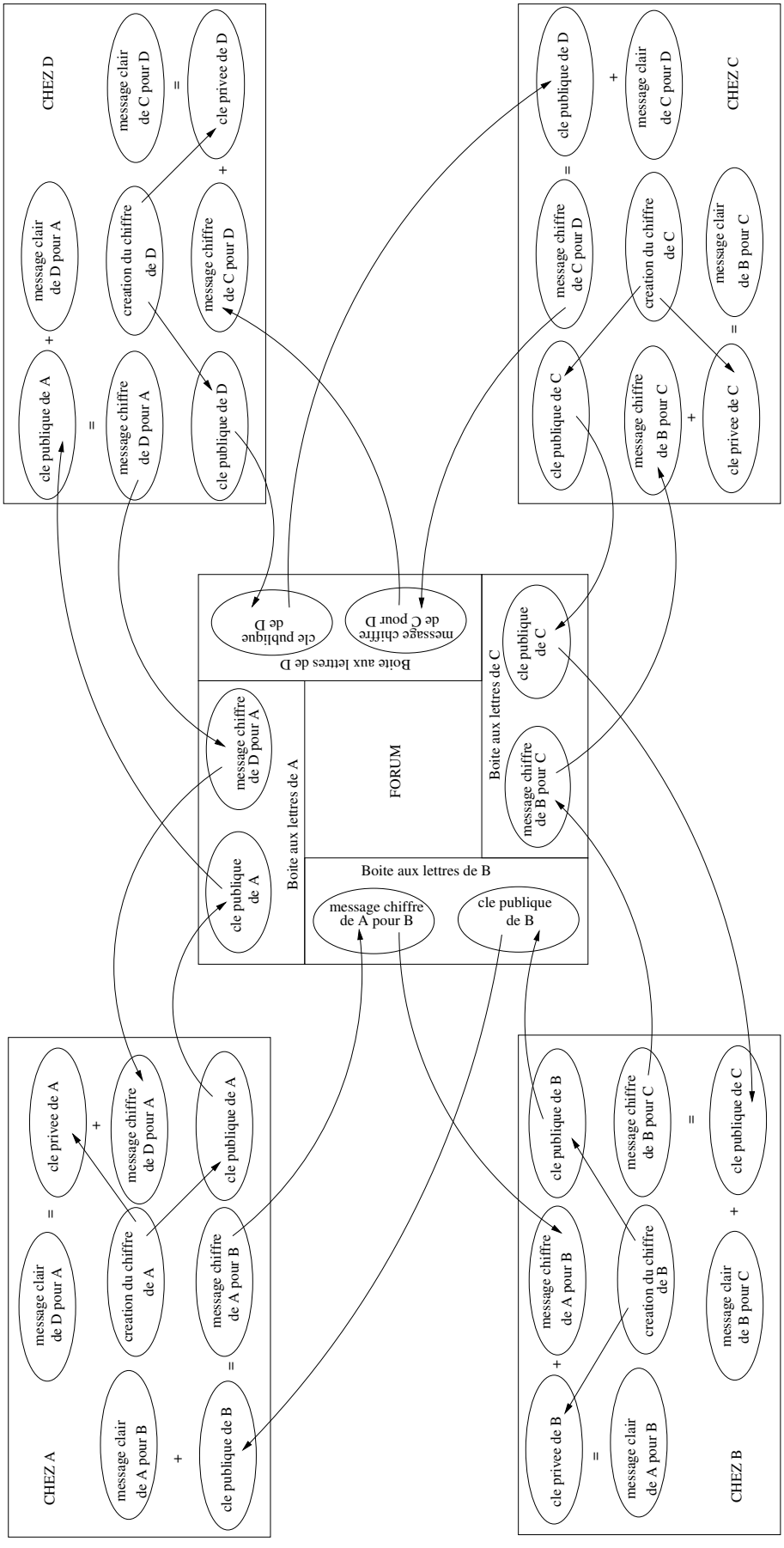
- Vous sauvegardez votre fichier (dans votre compte sur le serveur pédagogique, donc) pour garder une trace de votre travail
- Vous retournez sur l'ENT dans le cours Codes et Cryptographie, onglet Travaux
- Vous ouvrez le travail adéquat (eg. TP1 Groupe 1) et vous postez le fichier final dans ce travail ATTENTION : Il n'est plus possible de poster un fichier après la fin du TP !!!

Pour les TPs 2 et 3

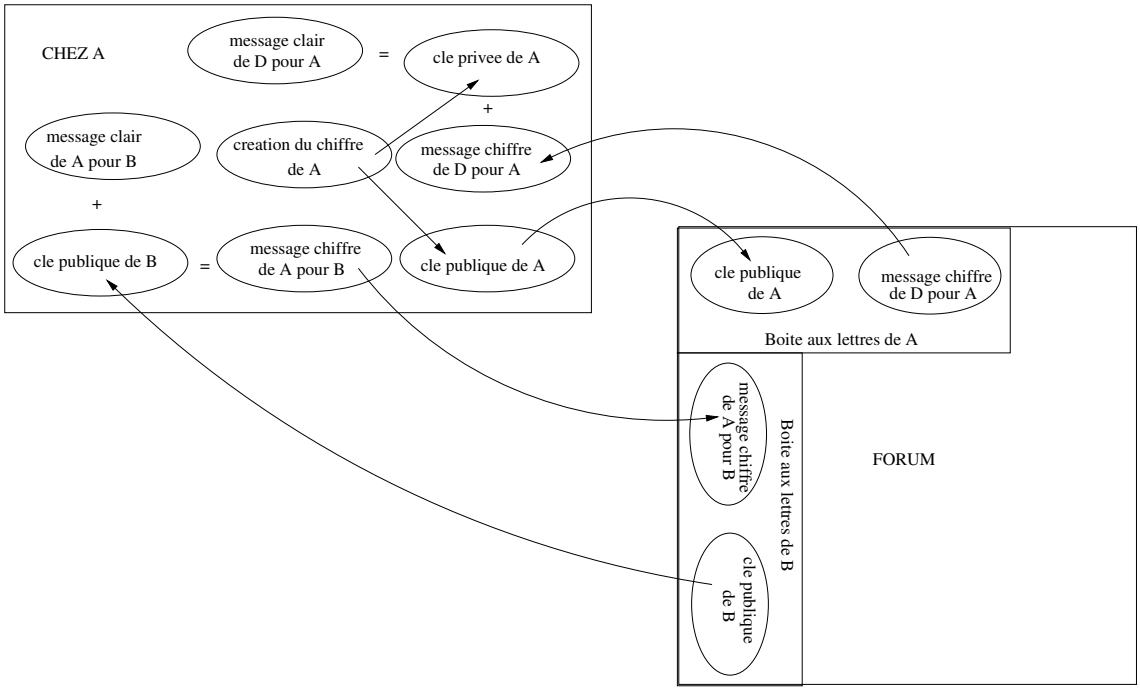
- Le cours sur RSA ou le Sac-À-Dos ne sera pas refait. Il y a sur l'ENT (dans le cours Codes et Cryptographie) des documents intitulés MementoRSA et MementoSacADos qui sont fait exprès pour vous rafraîchir la mémoire. Je vous demande de les étudier avant le TP, et ils sont aussi accessibles pendant le TP si besoin
- Vous utilisez le forum de votre groupe (toujours sur l'ENT et dans le cours Codes et Cryptographie) pour publier votre clé publique en créant un nouveau fil intitulé "Boîte aux lettres RSA de Dupond et Dupont" ou "Boîte aux lettres SAD de Dupond et Dupont"
- Puis chacun publie son message secret dans le fil du destinataire (c.-à-d. son voisin de droite) et récupère le message qui lui est destiné (c.-à-d. envoyé par son voisin de gauche) dans son propre fil.
- ATTENTION : Le TP est terminé pour un binôme lorsqu'il a déchiffré le message qui lui a été envoyé ET que le message qu'il a envoyé a été déchiffré par le destinataire.

Schémas de fonctionnement des TPs 2 et 3

Vue globale

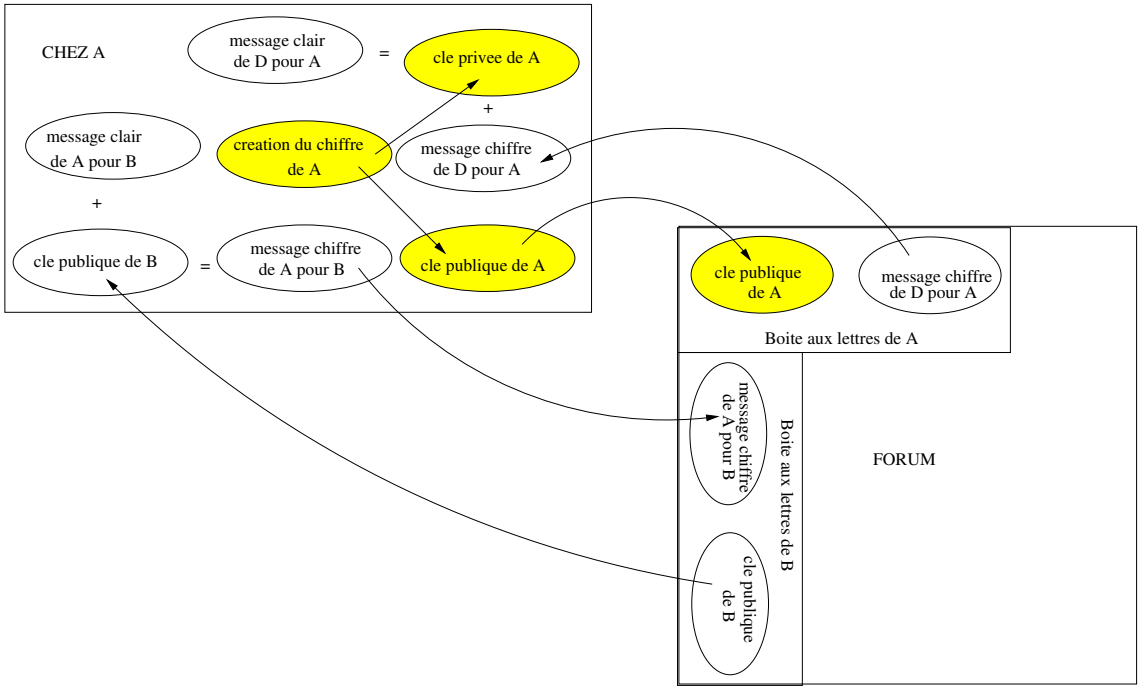


Vue de détail



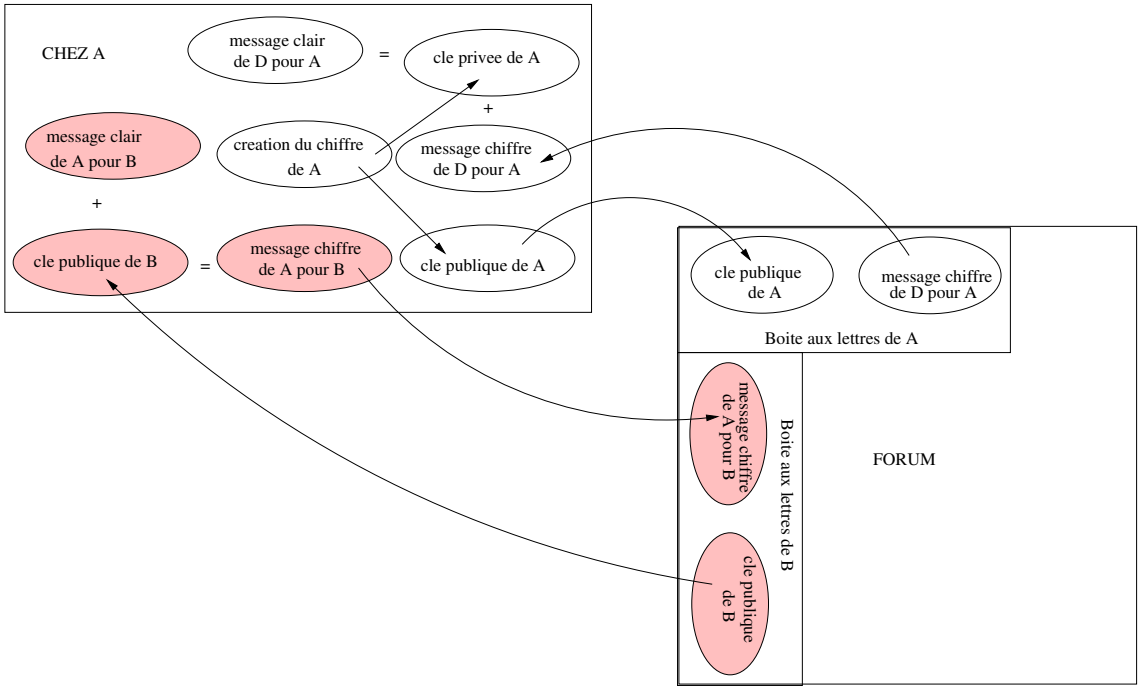
Phase 1 : Création du chiffre

- Maple : Génération de la clé privée et de la clé publique
- ENT : Publication de la clé publique



Phase 2 : Chiffrement d'un message

- ENT : Récupération de la clé publique du destinataire
- Maple : Chiffrement du message
- ENT : Publication du message chiffré



Phase 3 : Déchiffrement d'un message

- ENT : Récupération par le destinataire du message chiffré
- Maple : Déchiffrement du message chiffré