Roadmap

DIYPG : do it yourself privacy guard : total 45 points

Module C 28 pts

Phase 1 : génération de clés uint64 (donné+2 pts pour Bézout)

- ◉ calcul de deux nombres premiers
- ◉ calculer N
- ◉ calculer M
- ◉ calculer C et U
- ◉ former la clé publique et la clé privée
- ◉ faire un main.c phase1 qui teste tout ça
- ◎ décomposer un nombre en facteurs premiers (attaque)

Phase 2 : chiffre et déchiffre 4 pts

- ◉ Phase 2.1 : sur des messages utf8 dans des buffers (1 pts)
- ◉ Phase 2.2 : conversion base 64, messages dans des fichiers (revoir) (3 pts)

Phase 3 : interprète de commande et annuaire v1 5 pts

- ◉ générer des paires de clés avec identificateur (table des symboles)
- ◎ chiffrer, déchiffrer avec les clés d'un identificateur
- ◎ supprimer des clés
- ◎ sauver une clé publique en base64
- ◎ retrouver l'identificateur correspondant à une clé publique en b64
- ◎ sauvegarde des clés dans un fichier chiffré

Phase 4 : signature et hash 8 pts

- ◉ générer des clés de signature

- ◉ générer le digest d'un fichier
- ◉ signer le digest en le chiffrant avec la clef privée
- ◎ faire un fichier b64 avec tout ça
- ◎ ajouter un mdp dans l'interprète
- ◎ vérifier une signature
- ◎ signer un message chiffré
- ◎ vérifier et déchiffrer le message signé et chiffré

Phase 5 : annuaire des contacts 4 pts

- ◎ ajouter à l'annuaire la gestion des 2 paires de clés (chiffrement et signature)
- ◎ ajouter fct de manip usuelles pour les signatures
- ◎ ajouter la gestion du fichier de transactions

Phase 6 : blocks et bignum GMP (optionnel) 5 pts

- ◎ 6.1 refaire phase 1 avec GMP
- ◉ 6.2 refaire phase 2.2 avec des blocks de 4 octets
- ◉ 6.3 tester avec les fichiers vérifier b64

Module Java 15 pts points

Phase 1 : Java

- ◉ blockchain de clés publiques (registre)
- ◎ publication d'une clé publique avec signature. Si la clef est nouvelle alors vérification de l'identité
- ◎ sinon la Tx doit être signée avec une clef valide
- ◎ revocation d'une clé avec signature ou vérification d'identité
- ◎ recherche d'une clé pour trouver le propriétaire
- ◎ recherche de toutes les clés de quelqu'un

- savoir si une clé est révoquée
- connaître si la clef est vérifiée et par qui (mail d'ack quand la transaction est traitée)
- Comparrer toutes les clés d'une personn et dire si elle ont étét déclarées pas cette personne
- sauver/importer en JSON
- sauver des clefs
- Outils : sha256, JSON,base64

Doxygen 2 pts