

Travaux pratiques de cryptographie

Table des matières

TP A	Authentification artisanale d'emails	1
A.1	Production d'un HMAC à la main	1
A.2	Calculs de HMAC (en C ou en Java)	2
A.3	Vérification du HMAC	2
A.4	Calcul d'un HMAC conforme à la RFC 2104	2
TP B	Fabrique de clefs symétriques longues	4
B.1	Chiffrement et déchiffrement de Vernam	4
B.2	Un exemple sur le papier	9
B.3	Extension de la clef de K à W	9
TP C	Implémentation de l'AES	11
C.1	Chiffrement d'un bloc	14
C.2	Déchiffrement d'un bloc	14
TP D	Fabrique de grands nombres premiers	17
D.1	Premier ou pas ?	17
D.2	Mon premier grand nombre premier	17
D.3	Nombres premiers de Sophie Germain	18
D.4	Vérification expérimentale de la proportion de nombres premiers	18
D.5	Vérification expérimentale de la proportion de témoins de Miller	18
TP E	Implémentation du système RSA	21
E.1	Fabrique d'une paire de clefs	21
E.2	Encodage d'un texte	23
E.3	Décodage d'un texte	23
E.4	Vérification expérimentale du nombre de clefs pour un module donné	24
TP F	Bourrages	25
F.1	Bourrage standard selon le PKCS#5	25
F.2	Mode opératoire CBC	25
F.3	Bourrage OAEP du PKCS#1	26
TP G	Prise en main de la JCE	29
G.1	Déchiffrement AES dans le mode CBC	29
G.2	Vérification de l'implémentation de l'AES réalisée	29
G.3	Déchiffrement d'une clef de session avec un magasin de clefs RSA volumineux	29
G.4	Déchiffrement hybride AES avec mode opératoire inconnu	30
G.5	Vérification du format du fichier décrypté	30



Un exercice à faire absolument en TP.



Une question à finir chez soi, si nécessaire.



Une question facile pour commencer.



Exercice extrait des annales d'examens et de projets.



Un indice pour ne pas se tromper.



Un exercice facultatif.



Une question pour réfléchir un peu.



Exercice à rendre par email.