Master IPS1: Contrôle final du module <<Sécurité informatique>>

Vous devez entrer votre mail institutionnel

*Obligatoire

Adresse e-mail *

Votre adresse e-mail

Une quinzaine Personnes désirent communiquer de façon confidentielle en utilisant un chiffrement symétrique. Combien de clé privées auront –elles besoin ?

- ○ 105 clés
- ⊗ 15 clés

Quelle est la parité des exposants « e » et « d » du système RSA ?

- ☐ Les deux sont pairs
- ☒ Les deux sont impairs
- ☐ « e » est pair, « d » est impair
- ☐ « d » est pair, « e » est impair

Une fonction de hachage assure :

- [ ] La confidentialité
- [x] L'intégrité
- [ ] La non répudiation

L'échange de clés par Diffie-Hellman est vulnérable à :

- [ ] L'attaque par force brute
- [x] L'attaque de « Man in the Middle »
- [ ] L'attaque par dictionnaire
- [ ] L'attaque par indice de coïncidence

Deux certificats différents peuvent ils contenir la même clé publique.

- ( ) Vrai
- (x) Faux

Comment utilise t-on les clés symétriques et asymétriques ensemble ?

- [ ] On utilise la clé asymétrique pour chiffrer la clé symétrique
- [x] Le message est chiffré d'abord par la clé symétrique puis par la clé asymétrique.
- [ ] Le message est chiffré d'abord par la clé asymétrique puis par la clé symétrique.

Lequel des modes opératoires suivants est à ne jamais utiliser :

- [x] ECB
- [ ] CBC
- [ ] OFB
- [ ] CFB
- [ ] CTR

En parlant de la cryptographie asymétrique, lesquelles des phrases suivantes sont fausses ?

- [x] Elle n'assure pas la non-répudiation
- [x] La gestion des clés n'est pas simple
- [ ] Ses algorithmes sont moins rapide que ceux de la cryptographie symétrique
- [x] Les clés utilisées pour chiffrement et déchiffrement sont les mêmes.

Le chiffrement de César est :

- [ ] Un chiffrement affine
- [x] Une substitution mono-alphabétique
- [ ] Une permutation

Etant donné le système RSA with padding avec un modulo « n » et un bourrage de taille « r », quelle est la taille maximale d'un message en clair ?

- [ ] n-r
- [ ] log(n)-log(r)
- [ ] 2^(n)-2^(r)
- [ ] log(n)-r
- [ ] n+r

A l'arrivée quelle clef, Bob doit-il utiliser pour déchiffrer le message ?

- [x] sa clé privée.
- [ ] La clé privée d'Alice

A l'arrivée quelle clef, Bob doit-il utiliser pour vérifier le signature ?

- [x] Sa clé privée
- [ ] La clé publique d'Alice

Quels types d'algorithmes peut-on utiliser pour garantir la confidentialité dans des communications par GSM ?

- [ ] algorithmes asymétriques
- [x] algorithmes de chiffrement par flux
- [ ] algorithmes de chiffrement par blocs

Deux certificats différents peuvent ils avoir une même signature.

- ○ Vrai
- ⊗ Faux

Un chiffrement affine est :

- ☒ Une substitution mono-alphabétique
- ☐ Une substitution poly-alphabétique
- ☐ Une transposition

Quelle est la différence entre les deux techniques de certification des clés publiques S/MIME et PGP ?

- ☐ Les clés sont certifiées par chaque utilisateur dans le cas de S/MIME et par une autorité de certification dans le cas de PGP
- ☐ S/MIME est préférable dans un contexte Linux et PGP est plus adaptée à un environnement Windows ou Mac
- ☒ Les clés sont certifiées par chaque utilisateur dans le cas de PGP et par une autorité de certification dans le cas de S/MIME
- ☐ Pas de différence, les deux sont dédiées à la sécurité de messagerie électronique

La biométrie est un outil pour garantir

- ☐ La confidentialité
- ☐ L'intégrité
- ☒ L'authentification

Alice veut envoyer un message chiffré et signé à Bob, avec quelle clef doit-elle le chiffrer et ensuite le signer ?

- [x] Chiffrer avec la clé publique de Bob et signer avec sa clé privée
- [ ] Chiffrer avec sa clé privée et signer avec la clé publique d'Alice

Lesquels des modes de chiffrement par bloc se comportent comme des chiffrements par flux :

- [ ] ECB
- [ ] CBC
- [x] OFB
- [x] CFB
- [ ] CTR

Une recherche exhaustive sur les 56 bits d'une clef DES nécessite environ 48 heures. Combien de temps faudrait-il approximativement sur une clé de 64 bits ?

- [x] 56 heures
- [ ] 64 heures
- [ ] 64 jours
- [ ] Plus d'un an

Alice chiffre un message avec sa clé privée et l'envoie à Bob. Quelle information obtient Bob à la réception du message ?

- [x] Aucune
- [ ] Une clé

Bob veut envoyer un message à Alice

- [ ] Alice a besoin de la clé privée de Bob
- [ ] Alice a besoin de la clé publique de Bob
- [ ] Bob a besoin de la clé privée d'Alice
- [x] Bob a besoin de la clé publique d'Alice.

La non répudiation est garantie par :`

- [ ] une clé publique
- [x] une signature numérique
- [ ] un certificat

Chiffrement des données avec sa propre clé privée sert à assurer

- [ ] La non répudiation
- [ ] L'intégrité
- [x] La Confidentialité
- [ ] L'authentification

Lequel des inconvénients des systèmes de chiffrement symétriques existe aussi dans les systèmes de chiffrement asymétriques ?

- [ ] Les correspondants doivent se connaître au préalable
- [ ] On a besoin de stocker de façon sécurisée les clés privées pour chaque partie avec qui on communique
- [ ] Il est nécessaire de générer des nombres aléatoires de façon sécurisée
- [x] Les correspondants doivent partager un secret avant d'entrer en communication.

Un certificat X.509 crée un lien entre

- [x] L'identité de l'utilisateur et sa clé publique
- [ ] L'identité de l'utilisateur et sa clé privée
- [ ] Les clés publique et privée de l'utilisateur
- [ ] La clé publique de l'utilisateur et celle de l'autorité de certification

Lorsqu'on utilise un petit exposant publique pour RSA

- [x] Le chiffrement devient rapide
- [ ] Le déchiffrement devient rapide
- [ ] La signature devient rapide
- [x] La vérification de la signature devient rapide

Pour un même message clair M, peut-il y avoir deux signatures différentes par le même crypto-système El Gamal ?

- ○ Vrai
- ⊗ Faux

Une vingtaine de personnes désirent communiquer de façon confidentielle en utilisant un chiffrement asymétrique. De combien de clés privées auront –elles besoin ?

- ⊗ 20 clés
- ○ 40 clés

Peut-on avoir pour un même message clair plusieurs messages chiffrés en utilisant EL Gamal ?

- ○ Vrai
- ☒ Faux

Quel est le rôle d'un GPA dans un chiffrement par flux ?

- ☒ Créer un flux de clé
- ☐ Chiffrer le flux d'entrée

Alice a utilisé le chiffrement de Vernam pour envoyer un message m ∈ {0, 1}^100 à Bob. Ils partageaient tous les deux une clé aléatoire k ∈ {0, 1}^100. Oscar intercepte le chiffré c = m ⊕ k. Quel est le temps nécessaire pour retrouver m ?

- ☐ 100 secondes
- ☐ 100 essais
- ☒ 2^100 essais...

Quelles sont les trois propriétés de base dans la sécurité informatique qui étaient et sont omniprésentes au fil des années

- ☐ Auditabilité
- ☐ Authentification
- ☐ Non répudiation
- ☒ Confidentialité
- ☒ Disponibilité
- ☒ Intégrité

Les certificats délivrés par l'AC sont signés par:

- [ ] Les utilisateurs
- [x] L'autorité de certification
- [ ] Le destinataire

Un certificat devrait être révoqué avant sa date d'expiration si :

- [x] La clé privée de l'autorité est compromise
- [ ] La clé privée de l'utilisateur est compromise
- [ ] Le DN de l'utilisateur est changé

Envoyer Effacer le formulaire