



ENSI BOURGES MASTER "SÉCURITÉ INFORMATIQUE"

Systemes cryptographiques : contrôle de connaissances

Mercredi 19 décembre 2001

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

- 56 heures 64 heures 64 jours plus d'un an

2. Alice a utilisé le chiffrement de Vernam pour envoyer un message $m \in \{0, 1\}^{100}$ à Bob. Ils partageaient tous deux une clé aléatoire $k \in \{0, 1\}^{100}$. Charlie intercepte le chiffré $c = m \oplus k$.

Quelle est le temps nécessaire pour retrouver m ?

- instantané 100 essais 2^{100} essais impossible

3. Combien y a-t-il d'éléments dans \mathbb{Z}_{28}^* ?

- 0 10 12 20 27 28

4. Quelle est la valeur du symbole de Legendre $(\frac{8}{29})$?

- 0 -1 1 -2 2 8

5. Une implémentation de RSA, utilisant des exposants public et privé aléatoires de la taille du module, annonce le temps de calcul suivant : 1 milliseconde pour chiffrer un message de 512 bits avec une clef de 512 bits. Sachant que cette implémentation utilise l'algorithme d'exponentiation vu en cours, quel temps nécessiterait le chiffrement RSA d'un message de 2048 bits avec une clef de 2048 bits (en millisecondes) ?

- 1 8 16 32 64 128

6. Afin de pouvoir distinguer ses communications personnelles de ses communications professionnelles, Alice utilise deux clefs publiques RSA, ses correspondants utilisant l'une ou l'autre selon le type de communication. Afin d'accélérer la génération de clefs, Alice ne choisit que trois grands nombres premiers p, q et r de 512 bits, qu'elle garde secrets. Ses deux modules RSA publics sont alors $N_1 = pq$ et $N_2 = qr$. Alice choisit aléatoirement deux couples d'exposants privés et publics (d_1, e_1) et (d_2, e_2) , vérifiant donc $e_1 d_1 \equiv 1 \pmod{\varphi(N_1)}$ et $e_2 d_2 \equiv 1 \pmod{\varphi(N_2)}$. Quelle est la sécurité obtenue ?

- impossible à déterminer identique au RSA traditionnel aucune sécurité

7. Une technique classique d'identification est ■ le mot de passe ■. Si on a confiance dans le serveur, cette technique

- est sûre une fois résiste aux attaques passives est zero-knowledge

8. Pour prouver son identité, Alice veut utiliser la renommée de RSA. Pour cela, elle choisit un nombre premier p , un exposant e ainsi que $x \in \mathbb{Z}_p^*$. Elle publie le module p ,

l'exposant e et $y = x^e \bmod p$. Pour s'authentifier, elle utilise le protocole de Guillou-Quisquater qui lui permet de prouver sa connaissance de la racine e -ième de y modulo p , de façon zero-knowledge. Ce système d'authentification résiste

- à rien aux attaques passives aux attaques actives

9. Lors de l'utilisation de la signature DSA, Alice laisse échapper le nombre aléatoire r utilisé pour la signature. Dès lors, que peut faire Charlie, en connaissant r et la signature d'Alice qui utilise r :

- rien forger existentiellement retrouver la clé de signature

10. Pour la signature RSA, la longueur recommandée est le plus souvent 1024 bits. Quel est le principal intérêt du standard de signature DSA, utilisé avec p de 1024 bits et q de 160 bits? La signature est :

- longue de 320 bits ... de 1024 bits ... de 160 bits + rapide

11. Un problème du mode CBC est qu'aucun parallélisme n'est possible. Il me faut connaître le chiffré du bloc précédent. Une proposition est de séparer l'ensemble des blocs en par exemple deux groupes : ceux de numéro pair et ceux de numéro impair. On fait donc deux CBC en parallèle, l'un avec la clef k_1 et l'initialisation IV_1 , l'autre avec k_2 et IV_2 . Comment garder la sécurité de CBC ?

- Je peux utiliser la même clef et le même IV
 Je peux utiliser la même clef mais pas le même IV
 Les clefs doivent être différentes et les IV aussi
 Je ne peux pas avoir la sécurité d'un unique CBC

12. J'ai peur que les services secrets aient mis des faiblesses dans les algorithmes publiés et je veux utiliser simultanément IDEA et Skipjack. Je choisis une clef de 128 bits, qui sera la clef pour IDEA et dont les 80 bits de poids faibles seront la clef pour SkipJack. Je chiffre chaque bloc successivement avec IDEA puis Skipjack. Quelle est la sécurité de mon système ?

- On peut prouver que c'est au moins la sécurité du meilleur des deux
 On peut prouver que c'est au moins la sécurité du pire des deux
 Il est vraisemblable que c'est au moins la sécurité du meilleur des deux
 Il est vraisemblable que c'est au moins la sécurité du pire des deux
 On n'en sait rien

13. J'utilise un système de chiffrement de flot qui, à partir d'une clef k , fabrique une séquence de bits $k' = f(k)$. Je veux améliorer la sécurité de mon système. Pour cela j'utilise la séquence de bits k'' obtenue en supprimant les 128 premiers bits de k' . Après avoir chiffré le message en calculant $c_0 = m \oplus k'$, je le surchiffre en calculant $c = c_0 \oplus k''$. La sécurité de ce nouveau système est :

- meilleure identique pire sans rapport avec celle de f

14. Je modifie RC4 en faisant à chaque fois $i = i + 2$ au lieu de $i = i + 1$. La sécurité de ce nouveau système est :

- meilleure identique pire sans rapport avec celle de RC4