Sécurité des données TD 1-2

November 29, 2024

RSA

Exercise 1 Pour utiliser le système de cryptographie RSA, Alice choisit $p = 5$ et $q = 11$, deux nombres premiers, et la clé publique $(n, e) = (55, 27)$. Utilisez ces informations pour :

- Trouver la clé secrète d'Alice,
- Décrire le protocole de chiffrement RSA.

Exercise 2 Alice publie les données suivantes : $n = pq = 21$ et $e = 5$. Bob reçoit le message $P = 2$ et la signature numérique correspondante $S = 11$.
Question: Vérifiez la signature.

Diffie-Hellman

Exercise 3

- Calculer $2^9 \mod 11$
- Trouver x tel que $2^x = 5 \mod 11$, et y tel que $2^y = 3 \mod 11$

Supposons que deux utilisateurs veulent établir une clé secrète commune sur un canal non sécurisé en utilisant le protocole d'échange de clés Diffie-Hellman. La clé privée de l'utilisateur A est 3 et celle de l'utilisateur B est 5. Nous considérons le nombre premier $p = 11$.
Question:

- Trouvez le plus petit élément primitif (c'est-à-dire générateur) pour $p = 11$.
- Obtenez la clé commune en utilisant l'élément primitif trouvé ci-dessus. Dessinez un diagramme de séquence avec tous les messages échangés entre les deux utilisateurs, en utilisant les valeurs spécifiques données ci-dessus.

Exercise 4 Concevez une extension du protocole Diffie-Hellman qui permet à trois parties – Alice, Bob et Charles – de générer une clé secrète commune. Quels sont les inconvénients ? Proposez une version alternative.

ElGammal

Exercise 5 Décrire le protocole de ElGammal avec :

- le clé publique est $p = 5$, $g = 2$
- la clé secrète de Alice est $a = 2$ et celle de Bob est $b = 3$
- le message secret de Bob est $m = 4$.

Protocole SSS

Exercise 6 Une famille de quatre personnes décide de conserver sa fortune dans un coffre-fort numérique verrouillé. Chaque membre a son propre code PIN. Le coffre-fort s'ouvre si deux personnes parmi les quatre saisissent leur code PIN. Les codes sont :
P1 : 2 P2 : 5 P3 : 8 P4 : 0

- Donnez le polynôme correspondant $f(x)$.
- Calculez le secret $f(0)$.

Toutes les calculs seront effectués modulo 11.

Exercise 7 Un bureau militaire se compose de trois généraux. Ils ne se connaissent pas et doivent lancer une opération importante. Ils ne veulent la lancer que si deux d'entre eux sur trois décident de la lancer. Il y a quatre personnes dans une pièce, et exactement l'une d'elles est un espion, les trois autres étant nos généraux. Les généraux partagent un secret en utilisant le protocole de partage secret de Shamir, et l'espion a choisi aléatoirement sa part. Les parts sont
P1 : 3 P2 : 5 P3 : 7 et P4 : 8.

Trouvez quelle part a été créée par l'espion. Tous les calculs sont effectués sur les entiers.

Fonction de hachage

Exercise 8 (collision pour fonction de hachage) Considérez la distribution uniforme des anniversaires dans une année de 365 jours.
A. Quelle est la probabilité que deux personnes d'un groupe aient leur anniversaire le même jour si le groupe se compose de :

1. 2 personnes;
2. 23 personnes;
3. 97 personnes ?

Réponse : 1. $\approx 3 \cdot 10^{-3}$; 2: ≈ 0.507; 3: ≈ 0.99999992.
On peut observer que bien qu'il soit très improbable que deux personnes aient leur anniversaire le même jour, avec seulement 23 personnes, il y a plus de 50 % de chances qu'il y ait deux personnes avec un anniversaire le même jour. Pour 97 personnes, il est presque certain qu'il y aura une telle paire.
B. Même question si vous exigez que au moins une personne ait un anniversaire particulier (par exemple, le 15 février), si le groupe se compose de :

1. 2 personnes;
2. 23 personnes;
3. 97 personnes
4. 253 personnes ?

Réponse : ≈ 0.0054; 2: ≈ 0.0611; 3: ≈ 0.06115; 4: ≈ 0.50047