Cryptographie, HE-Arc, Automne 2025

Devoir 7 – modes opératoires et fonctions de hachage

Exercice 1

On considère la fonction de chiffrement jouet $E_K(X) = (X + K) \pmod{256}$ pour laquelle X est un octet du message et la clé K est un entier entre 0 et 255.

1. Expliquez pourquoi cette fonction fuite de l'information, même sans connaître la clé.
2. Un adversaire observe le chiffré $C_{\text{inconnu}} = 250$ d'un message X inconnu. Il soupçonne que le message pourrait être l'un des trois suivants :
   - $m_1 = 10$
   - $m_2 = 100$
   - $m_3 = 200$

   Montrez comment l'adversaire peut tester ces hypothèses et identifier le bon message.
3. Dans un chiffrement réel (CBC, CTR...), on utilise un IV ou un nonce. Est-ce que la fonction de chiffrement $E_{IV}(X) = (X + IV) \pmod{256}$ règle le problème précédent?

Exercice 2

Considérez les modes opératoires ECB, CBC et CTR.

1. Quels modes sont déterministes ?
2. Quels modes masquent correctement les répétitions du message lorsque l'IV ou le nonce est bien choisi ?
3. Pourquoi une mauvaise gestion du IV (CBC) ou du nonce (CTR) annule-t-elle cette propriété ?
4. Donnez un exemple concret où ECB fuit la structure d'un message.

Exercice 3

Pour une fonction de hachage, que veut dire

1. Résistance aux collisions?
2. Résistance à la préimage?
3. Résistance à la seconde préimage?

Exercice 4

Pourquoi signer $H(m)$ plutôt que le message m ? Donnez deux avantages pour la sécurité et l'efficacité.

Exercice 5

GCM est catastrophiquement insécure si le nonce est réutilisé. Pourquoi? Soyez précis.

Exercice 6

Considérer la fonction de hachage $H_{\text{pub}}(x) = (1103515245x + 12345) \pmod{327680}$. Les valeurs à hacher sont des entiers positifs.

```
A = 1103515245
B = 12345
m = 327680

def H_pub(x):
    return (A*x + B) % m
```

1. Hachez $x = 47572947294858218452$. Quelle est la taille approximative des hash en bits?
2. Les cinq valeurs suivantes ont été produites à partir d'entrées inconnues :

   ```
   h1 = 118290
   h2 = 215350
   h3 = 311620
   h4 = 118975
   h5 = 54830
   ```

   Pour chaque h_i, trouvez deux entrées distinctes $x_i \neq y_i$ telles que $H_{\text{pub}}(x_i) = H_{\text{pub}}(y_i) = h_i$ par brute force.
3. Nous pourrions rendre le brute force essentiellement impossible en augmentant la taille des paramètres et des outputs hachés. Ceci dit, montrez que ce n'est pas suffisant et que la fonction H_{pub} dans sa forme actuelle est désepérément cassée. Sachant cela, refaites l'exercice précédent sans brute force.