

TD3 — Chiffrement symétrique II

Ex1. Mini AES Dans cet exercice, les messages sont constitués d'une suite d'entiers codés sur 4 bits et notés en hexadécimal. Chaque caractère est codé en ASCII par deux entiers successifs. Ainsi le mot CAKE est codé 43414B45. Les tables en annexe permettent d'adapter l'algorithme Mini AES vu en cours à la notation hexadécimal.

- (a) Chiffrer le message 0k avec la clé cafe.
- (b) Déchiffrer le message 3140 avec la clé 1664.

Ex2. Mode CBC Dans cet exercice les messages sont chiffrés avec Mini AES en mode CBC sans bourrage (pas de *padding*). Des tables sont fournies en fin de fiche pour vous épargner les calculs de chiffrement et déchiffrement avec Mini AES.

- (a) Dessiner le diagramme de chiffrement par bloc avec le mode opératoire CBC.
- (b) Chiffrer le message B, A, BA. Compris. avec la clé b33f et l'IV 1007.
- (c) Dessiner le diagramme de déchiffrement par bloc avec le mode opératoire CBC.
- (d) Expliquer comment déchiffrer le $k^{\text{ième}}$ bloc d'un message chiffré en mode CBC. Appliquer cette méthode pour déchiffrer le 4^{ième} bloc produit à la question précédente.
- (e) Le chiffrement CBC est très malléable : à partir des chiffrés c_i d'un ou plusieurs messages en clair m_i , un adversaire peut produire de nouveaux messages chiffrant des combinaisons et des redécoupages des messages en clair. Expliquer comment il peut procéder.
- (f) Quel est le rôle de l'IV (vecteur d'initialisation) dans le mode CBC ? Pourquoi est-il transmis en clair ?

Ex3. Mode CTR Dans cet exercice les messages sont chiffrés avec Mini AES en mode CTR sans bourrage (pas de *padding*). Ne pas oublier de consulter les tables en fin de fiche.

- (a) Dessiner le diagramme de chiffrement par bloc avec le mode opératoire CTR.
- (b) Déchiffrer le message 5eed 4e5a f05d 915f 572b da66 006d 8326 chiffré en mode CTR avec la clé b33f (le premier bloc est l'entier à usage unique, ou *nonce*).
- (c) Le chiffrement CTR est-il malléable ? Si oui, expliquer comment modifier un message malgré son chiffrement en mode CTR.
- (d) Quel est le rôle du nonce en mode CTR ?

Ex4. Two-time pads Anselme a bien retenu la leçon : il ne faut pas stocker les mots de passe des utilisateurs d'une application en clair dans la base de donnée. Il a donc décidé de chiffrer le champ mot de passe à l'aide de Mini AES en mode CTR. Voici ci-dessous un dump de la table users. Sachant que le mot de passe de l'utilisateur demo est nocake4U, déterminer les mots de passe d'un maximum d'utilisateurs.

```
> select * from users;
demo|affe 164f 2b4d 9462 fb5d
alice|affe 0f0e 3a4d 9d65 a67c
bob|affe 1a10 2a0c ce34 fc3f
charlie|affe 1b48 7c5e ce6e fc72
```

Annexes

► Quelques outils pour Mini AES (défini en cours) en hexadécimal

| \oplus | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|----------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
| 1 | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 | 9 | 8 | b | a | d | c | f | e |
| 2 | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 | a | b | 8 | 9 | e | f | c | d |
| 3 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | b | a | 9 | 8 | f | e | d | c |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | c | d | e | f | 8 | 9 | a | b |
| 5 | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 | d | c | f | e | 9 | 8 | b | a |
| 6 | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 | e | f | c | d | a | b | 8 | 9 |
| 7 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | f | e | d | c | b | a | 9 | 8 |
| 8 | 8 | 9 | a | b | c | d | e | f | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 9 | 8 | b | a | d | c | f | e | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 |
| a | a | b | 8 | 9 | e | f | c | d | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 |
| b | b | a | 9 | 8 | f | e | d | c | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 |
| c | c | d | e | f | 8 | 9 | a | b | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| d | d | c | f | e | 9 | 8 | b | a | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 |
| e | e | f | c | d | a | b | 8 | 9 | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 |
| f | f | e | d | c | b | a | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

| \otimes | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|-----------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
| 2 | 0 | 2 | 4 | 6 | 8 | a | c | e | 3 | 1 | 7 | 5 | b | 9 | f | d |
| 3 | 0 | 3 | 6 | 5 | c | f | a | 9 | b | 8 | d | e | 7 | 4 | 1 | 2 |
| 4 | 0 | 4 | 8 | c | 3 | 7 | b | f | 6 | 2 | e | a | 5 | 1 | d | 9 |
| 5 | 0 | 5 | a | f | 7 | 2 | d | 8 | e | b | 4 | 1 | 9 | c | 3 | 6 |
| 6 | 0 | 6 | c | a | b | d | 7 | 1 | 5 | 3 | 9 | f | e | 8 | 2 | 4 |
| 7 | 0 | 7 | e | 9 | f | 8 | 1 | 6 | d | a | 3 | 4 | 2 | 5 | c | b |
| 8 | 0 | 8 | 3 | b | 6 | e | 5 | d | c | 4 | f | 7 | a | 2 | 9 | 1 |
| 9 | 0 | 9 | 1 | 8 | 2 | b | 3 | a | 4 | d | 5 | c | 6 | f | 7 | e |
| a | 0 | a | 7 | d | e | 4 | 9 | 3 | f | 5 | 8 | 2 | 1 | b | 6 | c |
| b | 0 | b | 5 | e | a | 1 | f | 4 | 7 | c | 2 | 9 | d | 6 | 8 | 3 |
| c | 0 | c | b | 7 | 5 | 9 | e | 2 | a | 6 | 1 | d | f | 3 | 4 | 8 |
| d | 0 | d | 9 | 4 | 1 | c | 8 | 5 | 2 | f | b | 6 | 3 | e | a | 7 |
| e | 0 | e | f | 1 | d | 3 | 2 | c | 9 | 7 | 6 | 8 | 4 | a | b | 5 |
| f | 0 | f | d | 2 | 9 | 6 | 4 | b | 1 | e | c | 3 | 8 | 7 | 5 | a |

| | γ | γ^{-1} |
|---|----------|---------------|
| 0 | e | e |
| 1 | 4 | 3 |
| 2 | d | 4 |
| 3 | 1 | 8 |
| 4 | 2 | 1 |
| 5 | f | c |
| 6 | b | a |
| 7 | 8 | f |
| 8 | 3 | 7 |
| 9 | a | d |
| a | 6 | 9 |
| b | c | 6 |
| c | 5 | b |
| d | 9 | 2 |
| e | 0 | 0 |
| f | 7 | 5 |

► Extrait de la table ASCII

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 20 | 21 | 2C | 2E | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 4A | 4B | 4C |
| SP | ! | , | . | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | G | H | I | J | K | L |
| 4D | 4E | 4F | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 5A | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 6A | 6B | 6C |
| M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | a | b | c | d | e | f | g | h | i | j | k | l |
| 6D | 6E | 6F | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 7A | | | | | | | | | | | | |
| m | n | o | p | q | r | s | t | u | v | w | x | y | z | | | | | | | | | | | | |

► Pour accélérer les calculs en mode CBC et CTR

| | | | | | | | | | | | | | | | | |
|---------------------------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| m | 0393 | 0d17 | 4088 | 522b | 5eed | 5eee | 5eef | 5ef0 | 5ef1 | 5ef2 | 5ef3 | 8114 | 9890 | a7f1 | cb33 | e86e |
| $\mu\text{AES}_{b33f}(m)$ | cb25 | 70bd | aa2f | 87b0 | 0035 | d03e | f034 | 320b | b203 | 7208 | a207 | dbff | a643 | 6ca8 | 7f7e | af34 |

| | | | | | | | | | |
|--------------------------------|------|------|------|------|------|------|------|------|------|
| m | 6ca8 | 70bd | 7f7e | 87b0 | a643 | aa2f | af34 | cb25 | dbff |
| $\mu\text{AES}_{b33f}^{-1}(m)$ | a7f1 | 0d17 | cb33 | 522b | 9890 | 4088 | e86e | 0393 | 8114 |