Fondements mathématiques pour la sécurité informatique

Sujet de contrôle du cours de Jean-Luc Stehlé

Juin 2012

QCM sans aucun document ni ordinateur.
Les calculettes sont autorisées

Total : 30 questions sur 5 pages
Durée : 1h30

Attention, les mauvaises réponses seront pénalisées. Dans la vie professionnelle d'un ingénieur en informatique, il vaut mieux avouer son ignorance que de raconter une bêtise.

Chiffrement par bloc avec chaînage.

Rappels de cours : On rappelle les divers modes de chaînage et/ou d'utilisation des algorithmes par bloc

ECB (Electronic Code Book)
CBC (Cipher Block Chaining)
CTS (Cipher Text Stealing = Vol de texte chiffré)
CTR (CounTeR = CompTeuR)
OFB (Output Feedback)

1. On veut chiffrer un message de 550 bits (sans compression) en utilisant DES en mode ECB. De combien de bits se composera le message chiffré ?
(A) 550 (B) 560 (C) 576 (D) 640 (E) autre valeur

2. On veut chiffrer un message de 550 bits (sans compression) en utilisant AES en mode ECB. De combien de bits se composera le message chiffré ?
(A) 550 (B) 560 (C) 576 (D) 640 (E) autre valeur

3. On veut chiffrer un message de 550 bits (sans compression) en utilisant DES en mode CTS. De combien de bits se composera le message chiffré ?
(A) 550 (B) 560 (C) 576 (D) 640 (E) autre valeur

4. On veut chiffrer un message de 550 bits (sans compression) en utilisant AES en mode CTS. De combien de bits se composera le message chiffré ?
(A) 550 (B) 560 (C) 576 (D) 640 (E) autre valeur

5. On veut chiffrer un message de 90 bits (sans compression) en utilisant DES en mode CTS. De combien de bits se composera le message chiffré ?

(A) 90 (B) 92 (C) 96 (D) 128 (E) autre valeur

6. On veut chiffrer un message de 90 bits (sans compression) en utilisant AES en mode CTS. De combien de bits se composera le message chiffré ?

(A) 90 (B) 92 (C) 96 (D) 128 (E) autre valeur

Rappels de cours sur le système de chiffrement AES

On note Z/2Z [X] l'algèbre des polynômes à une variable sur le corps à deux éléments Z/2Z, et on considère qu'un octet en AES représente un élément du corps quotient de Z/2Z [X] par l'idéal engendré par le polynôme $m[X] = X^8 + X^4 + X^3 + X + 1$. *Ce corps sera noté K dans la suite de ce QCM*

Un élément de K est représenté par la valeur hexadécimale entre accolades de l'octet correspondant.

Par exemple {72} (soit en binaire 0111 0010) représente le polynôme $X^6+X^5+X^4+X$, *modulo m[X] sur le corps Z/2Z*

Dans le corps K les opérations d'addition et de multiplication sont l'addition et la multiplication des polynômes dans Z/2Z [X], modulo le polynôme m[X]. Ces opérations sont respectivement notées $\oplus$ *et* $\bullet$.

En AES, un mot de 32 bits (4 octets) représente un élément du quotient de l'algèbre K[X] des polynômes sur K, quotientée par l'idéal engendré par le polynôme X^4+1 . *Un tel élément est représenté par la suite des 4 octets, par ordre de degré décroissant.*

Par exemple {18}{AC}{62}{2A}représente le polynôme $\{18\}X^3+\{AC\}X^2+\{62\}X+\{2A\}$, *modulo* X^4+1 *sur le corps K*

7. L'addition dans K est équivalente à

(A) L'addition classique
(B) L'addition modulo 64
(C) L'addition modulo 256
(D) L'opération OR bit à bit
(E) Autre chose

8. Combien vaut $\{23\} \bullet \{02\}$ dans K ?

(A) {00} (B) {46} (C) {4B} (D) {81} (E) autre valeur

9. Combien vaut $\{23\} \oplus \{23\}$ dans K ?

(A) {00} (B) {46} (C) {4B} (D) {81} (E) autre valeur

10. Combien vaut $\{23\} \oplus \{03\}$ dans K ?

(A) {20} (B) {26} (C) {2B} (D) {65} (E) autre valeur

11. Combien vaut $\{23\} \bullet \{03\}$ dans K ?

(A) {69} (B) {65} (C) {6B} (D) {81} (E) autre valeur

12. Combien vaut {40} ⊕ {03} dans K ?
(A) {C0} (B) {83} (C) {43} (D) {70} (E) autre valeur

13. Combien vaut {40} • {03} dans K ?
(A) {C0} (B) {83} (C) {43} (D) {1A} (E) autre valeur

14. Combien vaut {11} • {11} dans K ?
(A) {C0} (B) {83} (C) {43} (D) {1A} (E) autre valeur

15. La multiplication par {02} dans K est équivalente à

(A) Un décalage d'un bit dans le sens des poids forts
(B) Un décalage d'un bit dans le sens des poids faible
(C) Une permutation circulaire des bits
(D) Une multiplication par 2 modulo 256
(E) Autre chose

Les quatre question suivantes portent sur l'algèbre des mots de 32 bits utilisée en AES, c'est-à-dire l'algèbre des polynômes sur K , modulo X^4+1, dont on se donne les éléments

```
P = {11}{01}{00}{02}
Q = {11}{00}{2F}{01}
```

16. Quel est l'octet de poids faible de la somme de ces deux éléments P et Q
(A) {00} (B) {02} (C) {03} (D) {1C} (E) autre valeur

17. Quel est l'octet de poids fort de la somme de ces deux éléments P et Q
(A) {00} (B) {02} (C) {03} (D) {1C} (E) autre valeur

18. Quel est l'octet de poids fort du produit de ces deux éléments P et Q
(A) {00} (B) {02} (C) {03} (D) {1C} (E) autre valeur

19. Quel est le terme en X^2 de ce produit
(A) {E9} (B) {1C} (C) {1B} (D) {01} (E) autre valeur

20. Quel est le terme en X de ce produit
(A) {00} (B) {4D} (C) {5E} (D) {5F} (E) autre valeur

21. Quel est l'octet de poids faible de ce produit
(A) {02} (B) {EB} (C) {E9} (D) {5F} (E) autre valeur

22. Étant donné un processeur cadencé à 8 GHz qui génère toutes les clés possibles, en supposant qu'il lui faille 12 tops d'horloge pour générer une clé, quel est l'ordre de grandeur du temps approximatif lui faudra-t-il pour générer toutes les clés possibles d'un système de chiffrement utilisant de l'AES à 128 bits.

(A) 1 an (B) 1 million d'années (C) 1 milliard d'années (D) 940 000 milliards d'années (E) Beaucoup plus

Dans la suite de ce QCM, on suppose qu'on travaille avec un processeur 16 bits, cadencé à 4 GHz. On appellera multiplication élémentaire l'opération consistant à multiplier deux entiers non signés à 16 bits pour fournir un résultat stocké sur deux registres de 16 bits. Dans tous les calculs d'ordre de grandeur des temps de calcul, on ne tiendra compte que du nombre de multiplications élémentaires. On négligera donc les additions (qui en général seront simultanées aux multiplications, car les registres résultats fonctionneront comme des accumulateurs) ainsi que les calculs d'indice, les transferts registre mémoire etc. On admettra qu'une multiplication élémentaire se fait en moyenne en 9 tops d'horloge (y compris les additions dans les registres résultats, calculs d'indices, ...)

Dans toute la suite on considère qu'on travaille en arithmétique modulo N, où N est un entier à n bits.

Pour trois entiers u ,v ,z, on notera $u \equiv v$ [Mod z] pour dire que la différence (u-v) est un multiple entier de z, donc $u-v = \lambda z$ avec $\lambda \in \mathbf{Z}$.

On travaillera toujours en représentation de Montgomery (un entier modulo N est codé en machine par sa représentation de Montgomery, mais les exposants restent stockés en binaire). On estimera que le temps de calcul de la fonction de Montgomery est équivalent à celui d'une multiplication de deux grands nombres (à n bits). En conséquence, on estimera qu'une multiplication modulo N a un temps de calcul équivalent approximativement au double de celui d'une multiplication de deux grands nombres (à n bits).

$\Phi(N)$ représente l'indicateur d'Euler de N.
$\Phi(N)$ est égal au nombre de d'entiers positifs inférieurs à N et premiers à N.

23. Le temps de calcul de l'algorithme de calcul d'une addition modulo N, est, par rapport au nombre de bits de N est

(A) linéaire (B) quadratique (C) subexponentiel (D) exponentiel (E) Autre réponse

24. Le temps de calcul de l'algorithme de calcul d'une multiplication modulo N, est, par rapport au nombre de bits de N est

(A) linéaire (B) quadratique (C) subexponentiel (D) exponentiel (E) Autre réponse

25. Le temps de calcul de l'algorithme de calcul d'une division modulo N, est, par rapport au nombre de bits de N est

(A) linéaire (B) quadratique (C) subexponentiel (D) exponentiel (E) Autre réponse

On utilisera en RSA un exposant public égal à $d=2^{16}+1$ et un exposant privé c de l'ordre de grandeur de N, ayant approximativement autant de bits à 1 que de bits à 0 .

Dans la suite, on supposera toujours que le nombre n de bits de N est égal à 1024 .

Pour les signatures électroniques, on dispose d'un algorithme de hachage calculant des empreintes à 128 bits. On ne tiendra pas compte des temps de calculs de cet algorithme de hachage.

26. On veut mettre en œuvre RSA, en travaillant à 1024 bits. (On travaille modulo N où N est un nombre à n=1024 bits). Quel est approximativement le temps de calcul pour le chiffrement d'un message de 1 Mo (Megaoctet) utilisant la clé publique du destinataire ? (On ne demande pas un résultat précis, mais simplement un ordre de grandeur, à 50% près)

(A) Moins d'une seconde
(B) 2 secondes
(C) 1 minute
(D) 2 minutes
(E) Autre réponse

27. On veut mettre en œuvre RSA, en travaillant à 1024 bits. (On travaille modulo N où N est un nombre à n=1024 bits). Quel est approximativement le temps de calcul pour le déchiffrement d'un message de 1 Mo utilisant la clé privée ? (On ne demande pas un résultat précis, mais simplement un ordre de grandeur, à 50% près)

(A) Moins d'une seconde
(B) 1,2 secondes
(C) 2 minutes
(D) 4 minutes
(E) Autre réponse

28. On veut chiffrer un flux de données par RSA en utilisant la clé publique du destinataire. Quel débit maximal, en Megabits par seconde, peut-on atteindre en supposant que toute la puissance du processeur est dédiée au chiffrement ? (On ne demande pas un résultat précis, mais simplement un ordre de grandeur, à 50% près)

(A) 1 Mbps (B) 2 Mbps (C) 4 Mbps (D) 8 Mbps (E) Plus de 50 Mbps

29. Quel est le temps de calcul d'une signature électronique d'un message de 256 Mo par son expéditeur (utilisant sa clé privée en RSA) ? (On ne demande pas un résultat précis, mais simplement un ordre de grandeur, à 50% près)

(A) moins de 5 millisecondes
(B) 10 millisecondes
(C) 30 milliseconde
(D) 60 millisecondes
(E) Plus d'un dixième de seconde

30. Quel est le temps de vérification par le destinataire de la signature électronique de la question précédente ? (On ne demande pas un résultat précis, mais simplement un ordre de grandeur, à 50% près)

(A) moins de 1 milliseconde
(B) 1.7 millisecondes
(C) 3.2 millisecondes
(D) 6.6 millisecondes
(E) Plus d'un centième de seconde