01. C : DES en ECB = blocs de 64 bits
02. D : AES en ECD = blocs de 128 bits
03. A : CTS = même longueur (minimum = taille d'un bloc)
04. A : idem
05. A : idem
06. D : idem (bloc AES = 128 bits, 90 < 128)
07. E : un XOR bit à bit
08. B
09. A
10. A
11. B
12. C
13. A
14. D (Réduction modulo m[X])
15. A
16. C ({02}+{01})
17. A ({11}+{11})
18. D (voir plus bas)
19. C (voir plus bas)
20. E ({4F} voir plus bas)
21. B (voir plus bas)
22. E : 2^128 / (8*10^9 / 12)
23. E (log(N))
24. E ($\log^2(N)$)
25. E (log^3(N))
26-30. Je ne sais pas.

Réduction modulo m[X]

m[X] = {01}{1b} = 0000 0001 0001 1011

Pour réduire un résultat modulo m[X], on élimine un à un tous les bits de poids supérieur ou égale au degré de m (deg(m) = 8). Pour cela, il faudra multiplier. (shift + xor)

QUAND ? Lorsque le résultat d'une multiplication a plus de 8 bits (ne tient pas sur un octet).

COMMENT ?

1. Shifter vers la gauche (vers les poids forts) m[X] pour "aligner" le '1' à éliminer avec le premier '1' de m[X]. Soit un shift de [Poids du '1' à éliminer] - [deg(m[X])] rang(s).
2. XOR le nombre trouvé à l'étape précédente avec le résultat à réduire.
3. Recommencer à l'étape 1 tant qu'il y a des bits de poids >= 8.

<u>Exemple</u> :

A la question 14, {11}.{11}, on trouve (en binaire) 0001 0000 0001.

Il faut donc réduire modulo m[X], pour éliminer le bit de poids 8 (= ce putain de '1'), afin de pouvoir écrire le résultat en Héxadécimal avec 2 digits : {XX}.

On shift donc m[X] de 8-8=0 rang vers la gauche. Puis on XOR :
Résultat 0001 0000 0001
m[X] 0000 0001 0001 1011
Réduction 0 0001 1010 = {1A}

Multiplication de deux mots en AES (questions 16 à 21)

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

Terme en X^0 : {02}{01} = {02}
Terme en X^1 : {00}{01} + {2F}{02} = {5E}
Terme en X^2 : {00}{2F} + {01}{01} + {00}{02} = {01}
Terme en X^3 : {11}{01} + {11}{02} + {01}{2F} + {00}{00} = {1C}
Terme en X^4 : {01}{00} + {11}{2F} + {00}{11} = {E9}
Terme en X^5 : {11}{00} + {11}{01} = {11}
Terme en X^6 : {11}{11} = {1A}
Ensuite on fait une :

Réduction modulo X^4+1

Pour faire simple : tous les termes de degré >= 4, on leur fait -4.
Puis on les additionne (xor). (L'exemple vaut mieux qu'un long discours)
Les termes en X^6, X^5, X^4 s'annulent.
Terme en X^0 "récupère" le terme en X^4 : {02}+{E9} = {EB}
Terme en X^1 "récupère" le terme en X^5 : {5E}+{11} = {4F}
Terme en X^2 "récupère" le terme en X^6 : {01}+{1A} = {1B}
Terme en X^3 ne change pas : {1C}
QUAND ? Dès qu'il y a des termes de degré >= 4 (quasiment tout le temps donc).

TIPS :

- Multiplier par {01} = multiplier par 1 en décimal
- Multiplier par {00} = multiplier par 0 en décimal
- Additionner un nombre avec lui-même = 0 ({XY} xor {XY} = {00})
- Additionner {01} = additionner 1 (hé oui !)

--
Questions / Correction d'erreur via Fb.
Bisous.
Maxime Dufay