Calculatrice et une feuille recto-verso autorisés Jeudi 14 décembre 2021
Durée de l'épreuve : 2h

▢>⌟⊐▢▢⊡ ⊐▢ ⌞⌜<⌝>⊏

M1 informatique

Échauffement (10 points)

1. Kwuumvb a'ixxmttm ti uébpwlm lm kpqnnzmumvb cbqtqaém qkq ? Zmkwxqmz tm uwb zibwv-tidmcz acz dwbzm kwxqm.

2. Clobert et Yvonne échangent en utilisant AES-128 en mode CBC. Pour s'éviter de transmettre l'IV, ils décident d'utiliser la clé de chiffrement K comme vecteur d'initialisation :

a. représenter sur un schéma le principe du chiffrement CBC vu en cours ;

b. rappeler les propriétés attendues du vecteur d'initialisation et son rôle dans le mode CBC ;

c. Dans le cas où Eve a la possiblité de faire une attaque à texte clair choisi sur Clobert, expliquer comment Eve peut obtenir facilement la clé K en choisissant astucieusement le message à faire chiffrer.

d. Dans le cas où Eve peut seulement faire déchiffrer autant de messages qu'elle le souhaite à Yvonne, expliquer comment Eve peut ici encore obtenir facilement la clé K.

3. Après avoir rappelé le principe de fonctionnement d'une fonction de hachage cryptographique, expliquer le principe de fonctionnement d'une attaque par extension et comment la construction HMAC met en défaut ce type d'attaque.

4. Alice et Bob échangent suivant le protocole de Diffie-Hellman avec les paramètres $n = 223$ et $g = 11$.

a. Rappeler le principe du protocole de Diffie-Hellman.

b. Alice choisit $a = 84$. Calculer la valeur qu'elle envoie à Bob.

c. Sachant qu'elle reçoit 40, quel est le secret partagé ?

5. Charlie a choisi les paramètres suivants pour constituer sa clé RSA : $p = 11$, $q = 19$, $e = 7$.

a. Rappeler le principe de fonctionnement du schéma textbook RSA.

b. Calculer les clés publiques et privées de Charlie.

c. Déchiffrer le message 131 envoyé par Dave.

Sécurité parfaitement équilibrée (4 points)

Constance a parfaitement compris le cours de cryptographie : la sécurité parfaite n'est atteinte que par le chiffrement du masque jetable.

6. Rappeler le principe de fonctionnement du chiffrement par masque jetable et les conditions nécessaires à la sécurité parfaite.

Malheureusement, d'après Constance, certains choix de masques laissent transparaître une grande partie du message en clair. Elle décide de modifier l'algorithme de génération de clé pour ne garder que les masques qui contiennent autant de bits à 0 que de bits à 1 (les messages sont tous de longueurs paires).

7. Cette manière de chiffrer est-elle parfaitement sûre ? Justifier puis préciser :

a. Formaliser le chiffrement du masque jetable parfaitement parfait ainsi obtenu, en utilisant les notations du cours ($\mathcal{M}$, Gen, Enc, Dec).

b. Démontrer votre affirmation en utilisant la notion de schéma parfaitement indistinguable.

Mise en perspective (6 points)

Pour pratique qu'ils soient, les claviers et souris sans fil sont susceptibles d'être écoutés ou de voir des paquets injectés dans leurs échanges radio avec leur *dongle*. Afin de fournir l'interactivité nécessaire, chaque frappe d'une touche du clavier doit être transmise immédiatement au *dongle* pour que l'utilisateur puisse obtenir un retour sur sa frappe. D'un point de vue réseau, il s'agit donc d'un protocole qui transmet du clavier vers sa base une suite de messages pris dans un ensemble fini (l'ensemble des frappes possible).

Si les premiers claviers sans fils ont pu parfois envoyer leurs messages en clair, de nos jours la plupart des fabricants de claviers sans fils se targuent d'utiliser la meilleure cryptographie (souvent AES !) au service de la sécurité de leurs utilisateurs.

8. Le clavier et son *dongle* doivent se mettre d'accord sur un secret partagé, la clé AES, avant de pouvoir échanger selon un protocole sécurisé. En supposant que ces objets soient remplaçables, l'appairage ne peut être réalisé en usine.

a. Proposer un protocole sans fil pour appairer les objets ;

b. Proposer une attaque de type *homme du milieu* contre ce protocole ;

c. Proposer une alternative fiable qui permette au clavier et au *dongle* de mettre en place cette clé.

9. Les messages échangés sont de très petite taille et le mode opératoire ECB est utilisé. La plupart des fabricants ajoutent une suite d'octets aléatoire en plus de la touche frappée dans les données chiffrées. Expliquer pourquoi.

10. Si les paquets ne contiennent que la touche et le bourrage aléatoire, une attaque par rejeu est possible.

a. Expliquer comment il est possible de se logguer sur une machine qui utilise ce type de clavier à partir d'une écoute et d'un rejeu de paquets ;

b. Proposer une modification du format de paquet qui résout ce problème de rejeu.

Outils divers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Puissances de 2 : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, 2097152, 4194304, 8388608, 16777216, 33554432, 67108864, 134217728, 268435456, 536870912, ...

Premiers premiers : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227.

Suite de carrés successifs modulo 223 (*i.e.* $u_{n+1} = (u_n^2 \mod 223)$) :
11, 121, 146, 131, 213, 100, 188, 110, 58, 19, 138, 89, 116, 76, 201, 38, 106, 86, 37, 31, 69, 78, 63, 178, 18, 101, 166, 127, ...
40, 39, 183, 39, 183, 39, 183, 39, 183, 39, 183, 39, 183, 39, 183, 39, 183, 39, 183, 39, ...
55, 126, 43, 65, 211, 144, 220, 9, 81, 94, 139, 143, 156, 29, 172, 148, 50, 47, 202, 218, 25, 179, ...
84, 143, 156, 29, 172, 148, 50, 47, 202, 218, 25, 179, 152, 135, 162, 153, 217, 36, 181, 203, 177, 109, 62, 53, 133, 72, ...

Suite de carrés successifs modulo 209 (*i.e.* $u_{n+1} = (u_n^2 \mod 209)$) :
7, 49, 102, 163, 26, 49, 102, 163, 26, 49, ...
11, 121, 11, 121, ...
19, 152, 114, 38, 190, 152, 114, ...
103, 159, 201, 64, 125, 159, 201, ...
131, 23, 111, 199, 100, 177, 188, 23, 111, 199, ...

Quelques produits :
$23 \times 131 = 87 \pmod{209}$, $33 \times 110 = 62 \pmod{223}$, $19 \times 62 = 63 \pmod{223}$, $39 \times 183 = 1 \pmod{223}$, $43 \times 177 = 87 \pmod{209}$, $87 \times 177 = 142 \pmod{209}$, $87 \times 188 = 54 \pmod{209}$, $87 \times 111 = 43 \pmod{209}$, $101 \times 188 = 33 \pmod{223}$, $142 \times 188 = 153 \pmod{209}$, $146 \times 213 = 101 \pmod{223}$, $183 \times 183 = 39 \pmod{223}$,