Calculatrice et une feuille recto-verso autorisés Jeudi 10 janvier 2019
Durée de l'épreuve : 2h

▢>⌋⊐▢▢⊡ ⊐▢ ⌊⌐<⌝>⊏

M1 informatique

Échauffement (12 points)

1. Ijhmnkkwjw qj rjxxflj xznafsy js uwjhnxfsy qf rjymtij ij hmnkkwjrjsy : `ymjwj nx st xutts`.

2. ɯɑɑpɔhɕdɣɣɗɑɑɗ ɕɯɑ qɑɑɗɗpɔɑɑ ɗɯɕɗɑppɷhɔ ɑɑpɷ ɑɋɗɑɑpɔɕɗɗpɷhɔ ɕɯp qɑɑhɔhɕqɯɑɑ ɯɑɑ pɔhɕdɣɣɗɑɑqɑɑpɷhɔ : ɔɔhɑɑ ɗɑɑɕqɕqɷpɷ ɕɗɗ p ɕɯɕɗɑɑ.

3. Expliquer l'utilité des modes opératoires et le principe de fonctionnement du mode CBC. Peut-on utiliser une fonction de bibliothèque de chiffrement en mode CBC pour calculer un code CBC-MAC ? Justifier.

4. Alice et Bob échangent suivant le protocole de Diffie-Hellman avec les paramètres $n = 199$ et $g = 54$.
a. Rappeler le principe du protocole de Diffie-Hellman.
b. Alice choisit $a = 73$. Calculer la valeur qu'elle envoie à Bob.
c. Sachant qu'elle reçoit 152, quel est le secret partagé ?

5. Charlie a choisit les paramètres suivants pour constituer sa clé RSA : $p = 11$, $q = 19$, $e = 17$.
a. Rappeler le principe de fonctionnement du schéma textbook RSA.
b. Calculer les clés publiques et privées de Charlie.
c. Déchiffrer le message 120 envoyé par Dave.

Chiffrement par flaw (6 points)

Alice et Bob souhaitent discuter en toute confidentialité de leur dernier plan de conquête du monde sur un réseau non sécurisé. En effet, Eve est sur le qui-vive, prête à dénoncer leur complot.

6. Dans un premier temps Alice et Bob souhaitent choisir un secret partagé r de 1024 bits. Ils ne se soucient pas d'authentification. Proposer successivement **deux** protocoles simples et **distincts** pour établir un tel secret partagé, en utilisant **deux** primitives différentes vue en cours. Discuter de la taille des paramètres.

7. Pour transmettre un message M à Bob, Alice commence par calculer, à partir du secret r, la séquence clé $K = F(r).F(2r).F(3r)\ldots$ obtenue en concaténant les valeurs successives de $F(kr)$ où F est une fonction qui transforme un bloc de 1024 bits en un bloc de même taille. Alice envoie alors $M \oplus K$ à Bob.

a. Supposons que $F(x) = x^e \pmod n$. Montrer que si Eve connaît (n, e), C et les 1024 premiers bits de M alors Eve peut retrouver M tout entier.

b. Supposons maintenant que $F(x) = g^x \pmod n$. Montrer que si Eve connaît (g, n), C et les 1024 premiers bits de M alors Eve peut retrouver M tout entier.

c. Proposer une ou plusieurs méthodes plus raisonnables, vues en cours, pour générer une telle séquence K à partir d'un secret r.

Mise en perspective (6 points)

Son diplôme de l'école 54 en poche, Ignace se lance dans le développement d'une solution de messagerie sécurisée pour le milieu médical baptisée 2SADcrypt. Les données médicales étant extrêmement sensibles, hors de question de s'appuyer sur des méthodes de chiffrement qui ne résisteraient pas au moins 200 ans. Aussi, le logiciel s'appuie sur la seule méthode parfaitement sûre : le masque jetable. Chaque usager A reçoit tous les 6 mois par coursier une carte SD contenant un masque personnel K_A de 5 Mo et un masque maître K_0 de même taille partagé par tous les usagers. Le logiciel de messagerie échange ses messages avec un serveur centralisé à l'aide des protocoles SMTP et POP. L'envoi d'un message M de l'usager A vers l'usager B se passe comme suit : A chiffre le message à l'aide des deux masques pour obtenir $C = M \oplus K_A \oplus K_0$ et transmet C au serveur ; puis le serveur calcule $C' = C \oplus K_A \oplus K_B$ et le transmet à B ; enfin B déchiffre le message à l'aide des deux masques en calculant $M = C' \oplus K_B \oplus K_0$. La partie du masque utilisée est consommée et ne sera plus réutilisée.

8. Malgré le succès commercial de 2SADcrypt, on peut s'interroger sur sa réelle sécurité :

a. Rappeler le principe de fonctionnement du schéma de chiffrement par masque jetable et les conditions nécessaires à l'obtention d'un secret parfait.

b. Les algorithmes cryptographiques les plus courants (AES, RSA, ...) permettent-ils d'assurer une confidentialité des données pour les 200 prochaines années ?

c. Le serveur central est géré par la société qui génère les masques jetables. Le protocole utilisé assure-t-il la confidentialité des données de bout en bout ? Une compromission du serveur central met-elle en péril la confidentialité des données échangées ? Justifier.

d. Les usagers échangent des messages contenant parfois des pièces-jointes. La taille des masques est-elle adaptée à 6 mois d'utilisation ? Sachant qu'aucune procédure de régénération de masque n'est prévue et que le logiciel continue de fonctionner, la sécurité parfaite est-elle assurée ? Justifier.

e. Oscar est un usager malveillant capable d'écouter les échanges entre Alice et le serveur central. Expliquer comment Oscar peut récupérer le masque K_A d'Alice. Comment éviter ce problème ?

f. Le protocole n'utilise aucun mécanisme de contrôle d'intégrité. En quoi cela pose-t-il problème ? Discuter.

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 199 (*i.e.* $u_{n+1} = (u_n^2 \mod 199)$) :
54, 130, 184, 26, 79, 72, 10, 100, 50, 112, 7, 49, 13, 169, 104, 70, 124, 53, 23, 131, 47, 20, 2, 4, 16, 57, 65, 46, 126, 155, 145, 130, ...
73, 155, 145, 130, 184, 26, 79, 72, 10, 100, 50, 112, 7, 49, 13, 169, 104, 70, 124, 53, 23, 131, 47, 20, 2, 4, 16, 57, 65, 46, 126, 155, 145, 1
110, 160, 128, 66, 177, 86, 33, 94, 80, 32, 29, 45, 35, 31, 165, 161, 51, 14, 196, 9, 81, 193, 36, 102, 56, 151, 115, 91, 122, 158, 89, 160, .
152, 20, 2, 4, 16, 57, 65, 46, 126, 155, 145, 130, 184, 26, 79, 72, 10, 100, 50, 112, 7, 49, 13, 169, 104, 70, 124, 53, 23, 131, 47, 20, ...

Suite de carrés successifs modulo 209 (*i.e.* $u_{n+1} = (u_n^2 \mod 209)$) :
11, 121, 11, ...
17, 80, 130, 180, 5, 25, 207, 4, 16, 47, 119, 158, 93, 80, ...
19, 152, 114, 38, 190, 152, ...
120, 188, 23, 111, 199, 100, 177, 188, ...

Quelques produits :
$4 \times 152 = 11 \pmod{199}$, $11 \times 65 = 118 \pmod{199}$, $23 \times 120 = 43 \pmod{209}$, $26 \times 54 = 11 \pmod{199}$, $43 \times 199 = 197 \pmod{209}$, $46 \times 64 = 158 \pmod{199}$, $73 \times 130 = 137 \pmod{199}$, $79 \times 137 = 77 \pmod{199}$, $100 \times 197 = 54 \pmod{209}$.