Calculatrice et une feuille recto-verso autorisés Vendredi 16 décembre 2022
Durée de l'épreuve : 2h

□>⌋⊐□□⊡ ⊐□ ⌊⌜<⌝>⊏

M1 informatique

Les questions peuvent être traitées dans le désordre.
Réponses précises et concises attendues. Détailler les calculs.

Échauffement (10 points)

1. En utilisant le chiffre de Vigenère, déchiffrer le message LWVZRBKCFKNDW avec la clé SPRINT.

2. Expliquer le principe de fonctionnement du mode opératoire CBC et dessiner un schéma expliquant le principe de chiffrement. Puis préciser les points suivants en justifiant vos réponses :

- **a.** Ce mode opératoire nécessite-il l'utilisation de bourrage (*padding*) ?
- **b.** Peut-on paralléliser facilement le chiffrement des données ?
- **c.** Ce mode opératoire est-il malléable ?

3. Pour un protocole cryptographique, que signifie la propriété d'authenticité ? Donner un exemple de situation où une telle propriété est désirable. Citer une pritimive cryptographique d'usage courant en 2022 qui permet d'assurer cette propriété. Expliciter les paramètres nécessaires à son bon fonctionnement.

4. Alice et Bob échangent suivant le protocole de Diffie-Hellman avec $n = 199$ et $g = 69$.

- **a.** Alice choisit $a = 21$. Calculer la valeur qu'elle envoie à Bob.
- **b.** Sachant qu'elle reçoit 54, quel est le secret partagé ?

5. Charlie a choisi les paramètres suivants pour constituer sa clé RSA : $p = 43$, $q = 67$ et $e = 17$.

- **a.** Rappeler le principe de fonctionnement du schéma textbook RSA.
- **b.** Calculer les clés publiques et privées de Charlie.
- **c.** Déchiffrer le message 2682 envoyé par Dave.

Autour du protocole de Diffie-Hellman (7 points)

6. Décrire formellement le protocole d'échange de clés de Diffie-Hellman. À quoi sert ce protocole ? Comment est-il utilisé dans les protocoles comme TLS ?

7. Le protocole de Diffie-Hellman permet-il d'authentifier les parties en présence ? Si c'est le cas, expliquer pourquoi. Si ce n'est pas le cas, préciser un scénario dans lequel Eve exploite ce manque d'authentification.

8. Décrire formellement le chiffrement d'El Gamal. Expliquer ses liens avec le protocole de Diffie-Hellman.

9. Le protocole triple Diffie-Hellman (3DH) est la variante suivante du protocole DH. Alice et Bob se mettent d'accord sur un groupe (g, n) et choisissent en amont leurs secrets respectifs a et b à partir desquels ils calculent leurs clés publiques $A = g^a \pmod n$ et $B = g^b \pmod n$ qu'ils diffusent publiquement. Lorsqu'Alice souhaite communiquer avec Bob, elle choisit un secret éphémère x et transmet $X = g^x \pmod n$ à Bob. Bob choisit alors un secret éphémère y et transmet $Y = g^y \pmod n$ à Alice. Chacun calcule alors un secret K grâce à une fonction de dérivation de clé f choisie au préalable, tous les calculs ci-dessous sont effectués modulo n :

$$K = f(Y^x, B^x, Y^a, X, Y, A, B) \qquad K = f(X^y, X^b, A^y, X, Y, A, B)$$

- **a.** Vérifier qu'Alice et Bob disposent bien de tous les éléments pour faire les calculs. Pourquoi trouvent-ils la même valeur de K ?
- **b.** 3DH permet-il d'authentifier les parties en présence ? Justifier.
- **c.** Quel est l'intérêt des paramètres éphémères dans ce protocole ? Assure-t-il la confidentialité persistente ? La répudiabilité des échanges ?

d. La messagerie chiffrée Signal utilise une variante de ce protocole appelée X3DH. Dans le cas d'échanges asynchrones, Bob n'est pas toujours disponible pour générer la paire (y, Y). Comment proposez-vous de contourner ce problème ?

Authentification multifacteurs avec TOTP (3 points)

10. HOTP est un mécanisme standardisé de génération de mots de passe à usage unique, construits à partir de la primitive HMAC, d'un secret partagé K et de la valeur d'un compteur C. Le résultat du calcul $\text{HOTP}(K, C)$ est un nombre décimal à d chiffres dérivé du calcul de HMAC.

a. Expliquer le principe de fonctionnement de HMAC. Quelles sont les propriétés attendues de cette primitive ?

b. Connaissant plusieurs paires (C_i, H_i) où $H_i = \text{HOTP}(K, C_i)$, est-il possible pour un adversaire de retrouver K ?

11. TOTP utilise HOTP avec un compteur qui est dérivé de l'heure courante $C = \left\lfloor \frac{T - T_0}{\Delta} \right\rfloor$. La valeur courante $\text{TOTP}(K)$ est calculée par l'utilisateur ou lui est transmise par SMS. Expliquer pourquoi la plupart des systèmes bloquent-ils l'utilisation de TOTP après 3 erreurs de saisie ? Votre réponse doit traiter de cryptographie.

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.* $u_{n+1} = (u_n^2 \mod 199)$) :
14, 196, 9, 81, 193, 36, 102, 56, 151, 115, 91...
17, 90, 140, 98, 52, 117, 157, 172, 132, 111...
22, 86, 33, 94, 80, 32, 29, 45, 35, 31, 165...
30, 104, 70, 124, 53, 23, 131, 47, 20, 2, 4...
42, 172, 132, 111, 182, 90, 140, 98, 52...
54, 130, 184, 26, 79, 72, 10, 100...
69, 184, 26, 79, 72, 10, 100, 50...
77, 158, 89, 160, 128, 66, 177, 86, 33...
110, 160, 128, 66, 177, 86, 33, 94, 80, 32, 29...

Suite de carrés successifs modulo 2183 (*i.e.* $u_{n+1} = (u_n^2 \mod 2183)$) :
1340, 1174, 803, 824, 63, 1786, 433, 1934, 877, 713, 1913, 861, 1284...

Suite de carrés successifs modulo 2501 (*i.e.* $u_{n+1} = (u_n^2 \mod 2501)$) :
1199, 2027, 2087, 1328, 379, 1084, 2087, 1328, 379, 1084, 2087, 1328, 379, 1084...

Suite de carrés successifs modulo 2881 (*i.e.* $u_{n+1} = (u_n^2 \mod 2881)$) :
2682, 2148, 1423, 2467, 1417, 2713, 2295, 557, 1982, 1521, 2879, 4, 16, 256, 2154...

Quelques produits :
$3 \times 72 = 17 \pmod{199}$, $4 \times 1607 = 666 \pmod{2881}$, $10 \times 11 = 110 \pmod{199}$, $13 \times 47 = 14 \pmod{199}$, $14 \times 102 = 35 \pmod{199}$, $17 \times 98 = 74 \pmod{199}$, $22 \times 29 = 41 \pmod{199}$, $23 \times 139 = 13 \pmod{199}$, $26 \times 54 = 11 \pmod{199}$, $26 \times 69 = 3 \pmod{199}$, $27 \times 128 = 73 \pmod{199}$, $35 \times 56 = 169 \pmod{199}$, $41 \times 45 = 54 \pmod{199}$, $42 \times 172 = 60 \pmod{199}$, $53 \times 104 = 139 \pmod{199}$, $54 \times 184 = 185 \pmod{199}$, $60 \times 182 = 174 \pmod{199}$, $62 \times 86 = 158 \pmod{199}$, $66 \times 73 = 42 \pmod{199}$, $74 \times 157 = 76 \pmod{199}$, $77 \times 158 = 27 \pmod{199}$, $79 \times 185 = 88 \pmod{199}$, $90 \times 174 = 138 \pmod{199}$, $94 \times 158 = 126 \pmod{199}$, $160 \times 177 = 62 \pmod{199}$, $355 \times 2713 = 861 \pmod{2881}$, $379 \times 1199 = 1740 \pmod{2501}$, $406 \times 2087 = 1984 \pmod{2501}$, $433 \times 672 = 637 \pmod{2183}$, $637 \times 1934 = 746 \pmod{2183}$, $713 \times 746 = 1429 \pmod{2183}$, $861 \times 1521 = 1607 \pmod{2881}$, $1084 \times 1740 = 406 \pmod{2501}$, $1340 \times 1786 = 672 \pmod{2183}$, $1417 \times 2682 = 355 \pmod{2881}$