Calculatrice et une feuille recto-verso autorisés Lundi 28 avril 2025
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 ZSEFOCKTSDZAK avec la clé GLADOS.

2. Expliquer l'utilité des modes opératoires et le principe de fonctionnement du mode CTR puis préciser les points suivants, en justifiant vos réponses :

- **a.** Le mode CTR nécessite-t-il l'utilisation de bourrage (*padding*) ?
- **b.** permet-il de paralléliser le chiffrement des données ? leur déchiffrement ?
- **c.** est-il malléable ?

3. Charlie a choisit les paramètres suivants pour constituer sa clé RSA : $p = 13$, $q = 17$, $e = 5$.

- **a.** Rappeler le principe de fonctionnement du schéma textbook RSA.
- **b.** Calculer les clés publiques et privées de Charlie.
- **c.** Déchiffrer le message 53 envoyé par Dave.

4. Avez-vous remarqué que dans RSA les paires de clés (n,e) et (n,d) jouent un rôle symétrique ? Pourtant, en pratique, on ne construit pas e et d de la même façon, de sorte qu'on ne doit pas les mélanger. Pourquoi ? Quel est le risque ?

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.

5. 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.

6. 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.

Autour du protocole de Diffie-Hellman (6 points)

7. 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 ?

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

9. Montrons que les sécurités de Diffie-Hellman et El Gamal se réduisent l'une à l'autre. Considérons les deux fonctions suivantes qui décrivent le travail d'un attaquant :
— **CDH**(n, g, x, y) qui à n, g, $x = g^a \pmod n$ et $y = g^b \pmod n$ associe $k = g^{ab} \pmod n$.
— **CEG**(n, g, y, c_1, c_2) qui à n, g, $y = g^s \pmod n$, $c_1 = g^k \pmod n$ et $c_2 = my^k \pmod n$ associe m.

a. Décrire, en pseudo-code, un algorithme polynomial pour **CDH** en supposant qu'on dispose d'une version polynomiale de **CEG** (appeler cette fonction dans le code). Justifier le temps polynomial.

b. Décrire, en pseudo-code, un algorithme polynomial pour **CEG** en supposant qu'on dispose d'une version polynomiale de **CDH** (appeler cette fonction dans le code). Justifier le temps polynomial.

Authentification multifacteurs avec TOTP (4 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 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 TOTP(K) est calculée par l'utilisateur ou lui est transmise par SMS. Expliquer pourquoi la plupart des systèmes bloquent 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.