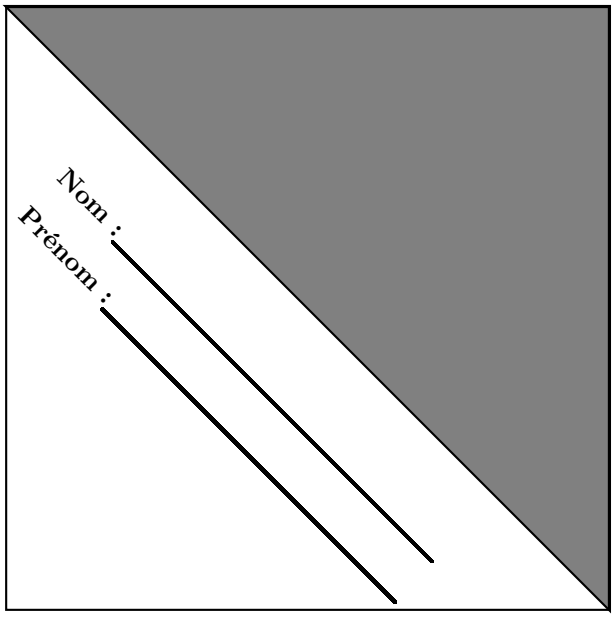
Université Côte d'Azur SI5, parcours Caspar
Cryptographie & Sécurité 2020–2021

Examen novembre 2020

Durée : 2h

Note :



L'examen comporte 4 parties indépendantes. Veuillez répondre sur la copie avec clarté et concision.

1 Quizz sur la sécurité [5 points]

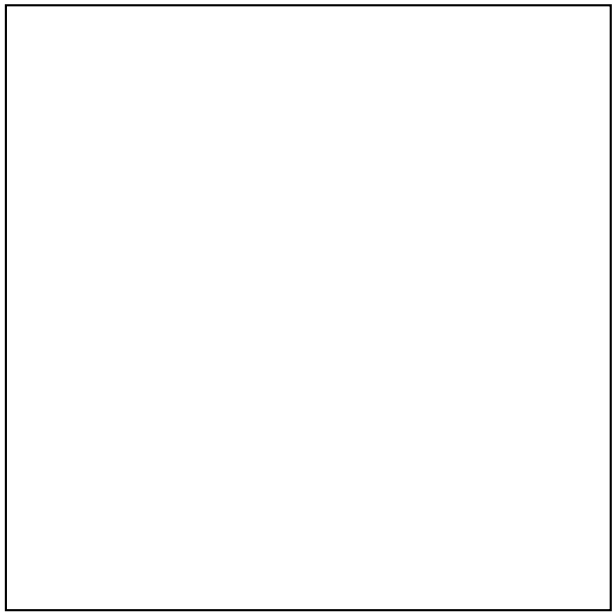
1. Pourquoi le problème de la factorisation reste difficile bien que celui de la primalité soit polynomial ?

2. Rappelez la différence entre la sécurité calculatoire et la sécurité sémantique et expliquez pourquoi la sécurité sémantique est préférable.

3. Quel est l'intérêt d'utiliser un chiffre d'El-Gamal par rapport à RSA ?

4. Pourquoi les opérations élémentaires du chiffrement symétrique (substitution, transposition, action de clé) utilisent-elles des structures algébriques de plus en plus compliquées ?

5. Dans quel cas utilise-t-on des algorithmes de dérivation de clé plutôt qu'une clé maître transportée ?



6. Retrouvez le texte qui a été comprimé au moyen de LZ77 sur les paramètres suivants : taille du tampon de lecture 5 et taille du tampon de recherche 9 : `(0, 0, c), (0, 0,' '), (0, 0, e), (0, 0, s), (0, 0, t), (4, 1, b), (0, 0, o), (0, 0, n), (8, 1, c), (0, 0, a), (3, 2, o), (7, 1, t), (0, 0, i), (3, 1, u), (0, 0, e)`

2 Un mauvais RSA [3 points]

Un mauvais programmeur a oublié de vérifier que les entiers premiers de RSA p et q engendrés aléatoirement sont différents. Alice a obtenu deux fois l'entier p pour construire le module n de RSA.

1. En justifiant votre réponse, dites si cela impacte le reste du fonctionnement du chiffre ?

2. Lorsqu'un autre utilisateur récupère la clé publique d'Alice, comment peut-il se rendre compte de cette erreur ?

3. En justifiant votre réponse, comment un autre utilisateur peut-il tirer parti de cette erreur et retrouver (facilement) la clé privée ?

3 Construction d'une fonction de hachage [5 points]

On considère la fonction de compression g prenant en entrée une lettre minuscule et une valeur initiale (IV) sous la forme d'un entier modulo 100. La sortie de cette fonction est obtenue par la suite d'opérations suivante :

1. On code numériquement la lettre ;
2. on ajoute le code numérique de la lettre à la valeur de chaînage (ou à l'IV pour initialiser) et on réduit modulo 100 ;
3. on multiplie le résultat précédent par 7 modulo 100 ;
4. on échange les chiffres du résultat (65 devient 56) ;
5. on ajoute au résultat précédent la valeur de chaînage modulo 100 pour obtenir la valeur de chaînage suivante.

Chaque lettre est codée numériquement par :

	0	1	2	3	4
+0	a	b	c	d	e
+5	f	g	h	i	j
+10	k	l	m	n	o
+15	p	q	r	s	t
+20	u	v	w	x	y
+25	z				

Exemple de calcul de $g(h, 17)$:

1. codage de `h` :7
2. calculer $17 + 7 = 24$
3. multiplier la valeur obtenue en 2. par 7 modulo 100 : $7 \times 24 = 168 \mod 100 = 68$
4. échanger les chiffres de 68 en 86
5. ajouter à la valeur obtenue en 4. la valeur de chaînage 17 modulo 100 : $17 + 86 = 103 \mod 100 = 3$

1. En ajoutant en bourrage la longueur de la chaîne fournie en entrée, expliquez comment on combine l'usage de la fonction de compression g pour obtenir la fonction de hachage h.

2. En utilisant le paradoxe des anniversaires, donnez le nombre de messages à considérer pour avoir plus d'une chance sur deux de trouver une collision.

3. Alice et Bob partagent le secret commun 20. Alice reçoit `ok,47` de Bob. Que peut-elle en déduire ?

4. Par un argument de dénombrement sur les mots de exactement 2 lettres, estimez le nombre d'antécédents pour une empreinte fixée.

5. Qu'en déduisez-vous sur la sécurité de cette fonction de hachage ? (Justifiez à minima)

4 Chiffrement authentifié [6 points]

On souhaite réaliser un système de chiffrement hybride (message chiffré par une clé secrète, cette dernière est transmise au moyen d'une clé publique). C'est de cette manière que `PGP` ou `GPG` fonctionnent. La clé secrète est rangée dans une enveloppe digitale à laquelle est concaténée le message chiffré, le tout dans une seule transmission.
On souhaite en plus que toutes les opérations de chiffrement soient *authentifiées*, comme dans la librairie `libsodium`.
Le scenario envisagé est que Alice (disposant de sa paire de clés (pka, ska)) veuille écrire à Bob (dont la paire de clés est (pkb, skb)). On supposera que Alice et Bob connaissent au préalable leurs clés publiques respectives et utilisent la même fonction de hachage cryptographique h. On notera MK la clé secrète transportée, K celle utilisée pour chiffrer le clair m et KA la clé utilisée pour l'authentification.
1. Expliquez en détail comment Alice peut transmettre MK à Bob en assurant à la fois la propriété de confidentialité et la propriété d'authentification.

2. Dites pourquoi RSA (dans son mode de fonctionnement "standard") est le meilleur candidat pour assurer ce transport de la clé MK.

Une fois la clé MK transportée, il faut qu'Alice et Bob puissent construire K et KA utilisées respectivement pour le chiffrement et l'authentification.
3. Expliquez comment Alice et Bob peuvent engendrer K et KA à partir de MK.

Une fois les clés K et KA obtenues, m peut être chiffré. Pour assurer le chiffrement authentifié, la méthode préconisée est connue sous le nom *encrypt then MAC*.
4. Expliquez comment réaliser la méthode *encrypt then MAC* pour assurer le chiffrement authentifié.

5. Donnez le formatage final du message en chiffrement authentifié qu'Alice transmet à Bob et expliquez comment Bob peut réaliser l'opération de déchiffrement.

6. Quelles sont les propriétés de sécurité assurées par cette technique de chiffrement et quelle en est la sécurité ?