Examen ISEC / 18 mars 2021 / durée 2h

— Notes manuscrites et planches des cours ISEC autorisées à l'exclusion de toute autre document.
— L'utilisation de tout matériel électronique (en dehors d'une montre non connectée) est interdite.
— Il y a trois exercices indépendants. Ce sujet est recto-verso.
— Une rédaction claire et concise sera appréciée. Toute affirmation devra être justifiée.

1 Chiffrement symétrique

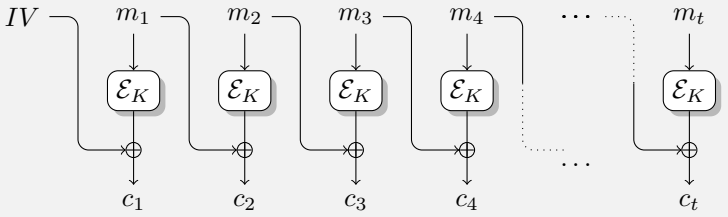
▷ **Question 1:** Pourquoi le gouvernement américain a-t-il renoncé à l'algorithme de chiffrement par bloc DES ?

▷ **Question 2:** Lorsque l'AES a été adopté, trois versions ont été standardisées, avec des clefs de 128, 192 et 256 bits. Pourquoi n'a-t-on pas pris en compte la possibilité d'avoir des clefs de 512 bits ?

▷ **Question 3:** Dans les modes opératoires de chiffrement qui en ont un, à quoi sert le Vecteur d'Initialisation ?

Mode opératoire de chiffrement CBC$^-$

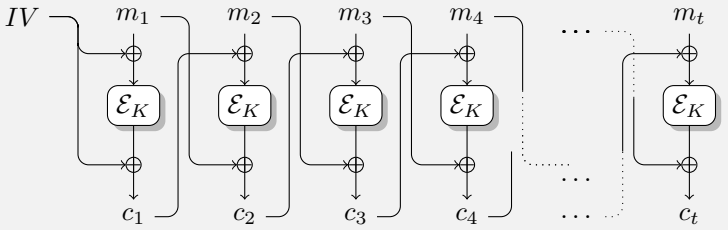
$\mathcal{E}$ désigne un mécanisme de chiffrement par bloc, où le bloc fait n-bits.



▷ **Question 4:** Montrez que le mode CBC$^-$ n'offre pas la sécurité sémantique sous des attaques à clairs choisis (des messages très courts suffisent).

Mode opératoire de chiffrement IGE (Infinite Garble Extension — sic)

$\mathcal{E}$ désigne un mécanisme de chiffrement par bloc, où le bloc fait n-bits.



▷ **Question 5:** Montrez, en vous inspirant de l'attaque correspondante sur le CBC normal, que le mode opératoire IGE n'offre pas la sécurité sémantique sous des attaques à clairs choisis si des messages de taille $2^{n/2}$ sont autorisés.

2 Protocoles d'échange de clef

Cet exercice considère trois protocoles d'échanges de clefs indépendants.

Échange de clef à base de RSA

Ce protocole est censé permettre à Alice et Bob d'établir un secret partagé sur un canal de communication public.
— Alice initie le protocole en générant une paire de clefs RSA (pk, sk). Elle envoie la partie publique (pk) à Bob.
— Bob génère une chaine de 128 bits aléatoires K, puis transmets $E(pk, K)$ à Alice.
— Alice et Bob possèdent alors en commun une chaîne de 128 bits secrète K et peuvent faire du chiffrement symétrique avec.

▷ **Question 6:** Ce protocole est-il sûr face à des adversaires *passifs* (répondre « oui » ou « non » est insuffisant).

▷ **Question 7:** Démontrer qu'il n'est pas sûr face à des adversaires *actifs* en explicitant une attaque « par le milieu »

Échange de clef tripartite

Ce protocole est censé permettre à Alice, Bob et Charlie d'établir un secret partagé entre eux trois sur un canal de communication public.

- Alice, Bob et Charlie choisissent chacun un exposant aléatoire secret, respectivement a, b et c.
- Alice envoie $g^a \bmod p$ aux deux autres ; Bob envoie $g^b \bmod p$ aux deux autres ; Charlie envoie $g^c \bmod p$ aux deux autres.
- Ils calculent tous $g^{a+b+c} \bmod p$.

▷ **Question 8:** Comment font-ils le calcul de la dernière étape ?

▷ **Question 9:** Quel gros problème possède ce protocole ?

Échange de clef Diffie-Hellman avec signature

Ce protocole est censé permettre à Alice et Bob d'établir un secret partagé sur un canal de communication public.

- Alice et Bob choisissent chacun un exposant aléatoire secret, respectivement a et b.
- Alice envoie $g^a \bmod p$ à Bob ; Bob envoie $g^b \bmod p$.
- Ils calculent tous les deux $S := g^{ab} \bmod p$.
- Alice envoie à Bob une signature de S ; Bob envoie à Alice une signature de S.
- Ils vérifient mutuellement leurs signatures. En cas d'erreurs, ils interrompent le protocole.
- Ils utilisent alors $K := H(S)$ comme clé symétrique partagée, où H est une fonction de hachage cryptographique, dont la sortie est tronquée à 128 bits.

▷ **Question 10:** Ce protocole résiste-t-il à l'attaque par le milieu ?

▷ **Question 11:** Quel risque potentiel y a-t-il à échanger des signatures de S ?

3 Signature à base de logarithme discret

(très mauvais) Algorithme de signature numérique

- La clef secrète d'Alice est composée d'un grand entier x.
- La clef publique est composée d'un nombre premier p, d'un générateur g, et de $h = g^x \bmod p$.
- Pour signer un message m, Alice calcule $\textsc{Sig}(x, m) := m + x \bmod p$.
- Pour vérifier une signature σ d'un message m, Bob teste si $g^\sigma \equiv h \cdot g^m \bmod p$.

▷ **Question 12:** Est-ce que la procédure de vérification est correcte ? (c.a.d. réussit systématiquement sur des messages correctement signés)

▷ **Question 13:** Justifier que le schéma de signature est incassable sous une attaque sans messages (UB-KOA).

▷ **Question 14:** Montrer une attaque en bris total (récupération de la clef secrète) sous une attaque à messages connus.