Examen M2 SeCReTS 2011-2012 : "Bases de la cryptographie".

Remarques :

- Pour chacune des questions, on demande de justifier les étapes en mentionnant notamment les algorithmes utilisés.
- Aucun document, calculatrice, téléphone, Ipad etc ne sont admis.
- Les sacs doivent rester à terre et aucune feuille de brouillon n'est admise.
- Un feuille quadrillée recto (A4) avec vos notes est autorisée (écriture sur les lignes).
- La durée de l'examen est de 3 heures.

Partie I : Théorie

Question 1 (5 points)
Expliquer la notion de réduction calculatoire. Détailler vos explication en considérant le logarithme discret. Quelles sont les indicences sur la sécurité de la primitive Diffie-Hellman. Expliquez en détails un algorithme permettant de calculer le logarithme discret façon de efficace.

Question 2 (2 points)
Détailler le RSA en chiffrement et montrez que l'algorithme de chiffrement et de déchiffrement forment une paire de permutation inverse l'une de l'autre.

Question 3 (3 points)
Expliquez quelle est l'utilité des modes en crytographie symétrique. Précisez les caractéristiques importantes auxquelles il faut faire attention et décrivez brièvement les principaux modes utilisés en pratique.

Partie II : Exercices

Question 4 (5 points)
Considérons l'alphabet $\mathcal{A} = \{0, 1\}$. Supposons que l'on choisisse un mot de passe de la façon suivante : on tire d'abord au hasard un nombre t compris 1 et n (fixé). Ensuite, on tire au hasard un mot de passe composé de t caractères de $\mathcal{A}$.

1. Calculez que la probabilité de chaque mot de passe.
2. Calculez l'entropie du mot de passe (en fonction de n). Evaluez la formule obtenue pour $n = 4$.
3. Calculez l'entropie conditionnelle du mot de passe connaissant sa longueur (en fonction de n). Evaluez la formule obtenue pour $n = 4$.
4. Calculez l'information qu'apporte la connaissance de la longueur du mot de passe. En d'autres termes, calculez l'information mutuelle entre le mot de passe et la longueur de celui-ci (en fonction de n). Evaluez la formule obtenue pour $n = 4$.

Remarque : si la question ne vous inspire pas, donner tout de même les formules des concepts mentionnés.

Question 5 (5 points)
Cette question concerne le RSA de Takagi. Il s'agit d'un RSA classique dans lequel le module RSA est le produit d'une puissance d'un nombre premier et d'un autre nombre premier. Considérons les nombres premiers $p = 5$, $q = 7$ et dénotons par $n = p^2 \cdot q$ le module RSA de notre système. Dénotons par Φ la fonction totient d'Euler.

1. Calculer le module RSA n et $\Phi(n)$.
2. Parmi les nombres 12 et 31, déterminer ceux qui satisfont les hypothèses d'exposant de signature et pour ceux-la calculer l'exposant de vérification correspondant.
3. Signer le message 19 pour le(s) exposant(s) retenu(s) au point précédent. Utiliser la méthode la plus efficace que vous connaissez.