Feuille d'exercices 4.

Exercice 1 Utiliser l'algorithme rho de Pollard pour factoriser 8051 avec $f(x) = x^2 + 1$ et $x_0 = 1$.

Exercice 2 Rappel sur la signature El Gamal: Soit p un nombre premier et soit $\alpha \in \mathbb{F}_p^*$ une racine primitive.
Alice choisit une clé secrète $a \in \{1, ..., p-1\}$.
Alice calcule $\beta = \alpha^a \bmod p$ et rend public (p, α, β).
Alice choisit au hasard et garde secret $k \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$.

Alice envoie le message $x \in \mathbb{F}_p$ à Bob. Sa signature est le couple $(\gamma, \delta) \in \mathbb{F}_p^* \times (\mathbb{Z}/(p-1)\mathbb{Z})$ calculé comme suit:
$\gamma = \alpha^k \bmod p$
$\delta = (x - a\gamma)k^{-1} \bmod p - 1$
1) Quel calcul effectue Bob pour vérifier la signature d'Alice?
2) Application numérique: $p = 467$, $\alpha = 2$, $a = 127$,
a) calculer β.
b) Calculer la signature d'Alice pour le message $x = 100$ avec $k = 213$.
c) Comment vérifie-t-on la signature d'Alice?
3) Supposons qu'Alice utilise la signature El Gamal et signe les messages x_1 et x_2, obtenant (γ, δ_1) et (γ, δ_2) respectivement (avec la même valeur γ dans chaque signature). Supposons que l'on ait $pgcd(\delta_1 - \delta_2, p-1) = 1$.
a) Démontrer que k peut se calculer efficacement avec ces informations.
b) Dans quel cas peut-on alors retrouver a?
c) On suppose que $p = 467$, $\alpha = 2$, et $\beta = 78$, que le message $x_1 = 25$ est envoyé avec la signature $(\gamma, \delta_1) = (245, 292)$ et le message $x_2 = 386$ est envoyé avec la signature $(\gamma, \delta_2) = (245, 347)$. Calculer k et a.

Exercice 3 Soit G le groupe défini par:

$$G = \langle s_1, s_2 | s_1^2 = s_2^3 \rangle$$

Alice et Bob rendent publiques les mots $a_1 = s_1 s_2$; $a_2 = s_1^{-1} s_2$; $b_1 = s_2 s_1$; $b_2 = s_2^{-1} s_1$.
1) Alice choisit le mot $X = a_1$ qu'elle garde secret.
Alice envoie à Bob les données: $(b_1', b_2') = (X^{-1} b_1 X, X^{-1} b_2 X)$. Donner une expression simplifiée de (b_1', b_2').
2) Bob choisit le mot $Y = b_1 b_2^{-1}$ qu'il garde secret aussi.
Bob envoie à Alice les données: $(a_1', a_2') = (Y^{-1} a_1 Y, Y^{-1} a_2 Y)$. Donner une expression simplifiée de (a_1', a_2').
3) Alice calcule $X' = a_1'$ et Bob calcule $Y' = b_1'(b_2')^{-1}$.
Montrer que $K_A = X^{-1} X'$ et $K_B = (Y^{-1} Y')^{-1}$ sont des commutateurs en X et Y et que $K_A = K_B$.
Vérifier cette égalité en faisant les calculs explicites. 4) Quel est le but du protocole (dû à Anshel, Anshel et Goldfeld) décrit dans cet exercice?
Sur quel problème mathématique est-il basé?
5) Alice choisit maintenant que $X = a_1 a_2^{-1}$. Expliquer pourquoi ce nouveau choix de X n'est pas aproprié?

Exercice 4 Le problème du sac à dos est le suivant: on dispose d'un sac à dos vide et de n objets de poids respectifs $a_1, ..., a_n$. Quels objets doit-on mettre dans le sac à dos pour obtenir un poids total égal à k, i.e., existe-t-il une suite $(x_1, ..., x_n)$ de valeurs booléennes telles que $\sum_{i=1}^n x_i a_i = k$?

C'est un problème très difficile à résoudre sauf dans le cas où la suite $(a_1, ..., a_n)$ et supercroissante, i.e., si pour tout entier $1 \leq i \leq n$, on a

$$\sum_{j=1}^{i} a_j < a_i$$

1) Vérifier que la suite $(1, 3, 6, 13, 28, 63, 142, 290, 601, 1231, 2543, 5100)$ est supercroissante.
2) Montrer qu'il y a une unique solution au problème du sac à dos pour $k = 2931$.
3) Montrer qu'il n'y a pas de solution pour $k = 3090$.
4) Donner un algorithme de résolution du problème du sac à dos lorsque $(a_1, ..., a_n)$ est supercroissante.
5) a) Montrer que la suite supercroissante qui ait les plus petits termes a_i est définie par $a_i = 2^{i-1}$.
b) Montrer que si la suite supercroissante $(a_1, ..., a_n)$ est définie par $a_i = 2^{i-1}$, alors le probème du sac-à-dos a une solution pour tout entier $k \leq \sum_{i=1}^{n} a_i$ et que ce n'est plus le cas pour les autres suites supercroissantes.

Le cryptosystème de Merkle et Hellman (1978) est basé sur le problème du sac à dos:
Alice choisit une suite supercroissante $(a_1, ..., a_n)$ et un entier $N > \sum_{i=1}^{n} a_i$,
Alice choisit au hasard un entier d compris entre 1 et $N - 1$ et premier avec $N - 1$,
Alice choisit au hasard une permutation de l'ensemble $\{1, ..., n\}$,
Alice calcule $b_i = a_{\sigma(i)} d \bmod N$ pour tout $i \in \{1, ..., n\}$:
Clé publique d'Alice: $(b_1, ..., b_n)$,
Clé privée d'Alice: $((N, d, \sigma, (a_1, ..., a_n))$.
5) Bob veut envoyer à Alice un message qui est une suite $x_1, ..., x_n$ de n bits. Comment va-t-il s'y prendre pour chiffrer ce message? Pourquoi le message chiffré est-il difficile à déchiffrer?
6) Alice reçoit le message chiffré c. Quels calculs fait-elle pour déchiffrer le message?
7) Application numérique:
$n = 5$, $(a_i) = (2, 5, 11, 23, 55)$, $N = 113$, $k = 27$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}$.

Quelle est la clé publique d'Alice?
Bob veut envoyer le message $m = (10101)$. Calculer c.
Vérifier en faisant les mêmes calculs qu'Alice, qu'elle retrouve bien m.

Le cryptosystème de Merkle et Hellman a été cassé par Shamir en 1982.