NOM : **Prénom :**

Modèles pour la sécurité **Master INPG-UJF SCCI**

TD - Générateur pseudo-aléatoire cryptographiquement sûr

Le générateur BBS (Blum Blum Shub) est un générateur crytographiquement sûr qui fonctionne comme suit:

- On choisit deux nombres premiers $p = 4.k_1 + 3$ et $q = 4.k_2 + 3$. On calcule l'entier de Blum $n = pq$.
- On choisit un entier $x < n$ aléatoire et premier avec n.
- On pose $x_0 = x^2 \mod n$ et, pour $i \geq 1$, $x_i = x_{i-1}^2 \mod n$.

Le $i^{\text{ème}}$ bit b_i pseudo-aléatoire est alors le bit de poids faible de x_i, i.e. $b_i = x_i \mod 2$.
Ce générateur est cryptographiquement sûr: sa sécurité (admise) repose sur la difficulté de factoriser n. Ce générateur est conjecturé sûr à gauche et à droite.

Question 1. On suppose que Bob, qui connait p et q, a choisi x_0 et veut calculer efficacement x_i.

1. Soit $u_i = 2^i \mod (p-1)(q-1)$; montrer que $x_i = x_0^{u_i} \mod n$.
2. En déduire un algorithme qui prend en entrée i, x_0, p, q et n et qui génère en sortie le bit b_i. Donner le coût de cet algorithme.
3. Quel est l'intérêt de cette propriété ?

Question 2. On suppose que Bob, qui connait p et q, connait x_i mais pas x_0.

1. Montrer que $u_i = 2^i \mod (p-1)$ est premier avec l'entier $\frac{p-1}{2}$.
2. $\star$ Soit v_i l'inverse de u_i modulo $\frac{p-1}{2}$. Donner un algorithme permettant de calculer $x_0 \mod p$ à partir de $x_i \mod p$ et en utilisant v_i.
3. En déduire un algorithme qui prend en entrée i, x_i, p, q et n et qui génère en sortie x_0.

Question 3. Le protocole de chiffrement de Blum-Goldwasser fonctionne comme suit. Pour envoyer un message $M = [M_1, \ldots, M_t]$ de t bits à Bob, Alice procède comme suit. Alice choisit une valeur x_0 aléatoire secrète; à partir de x_0, elle génère avec le générateur BBS et la clef publique n de Bob une suite de t bits $B = [b_1, \ldots, b_t]$ pseudo-aléatoires et elle envoie à Bob le message chiffré $[M', x_t]$ où :

- $M' = [M_1 \oplus b_1, \ldots, M_t \oplus b_t]$ est le ou exclusif de M et B;
- x_t est le t^{ime} itéré de la suite (x_i) générée

Justifier que cet algorithme est sûr. En utilisant les questions précédentes, donner l'algorithme qui permet à Bob de déchiffrer efficacement le message reçu.