Master CSI 2 2013-2014

Crypto avancée : feuille de TD 3

– Exercice 1. Soit le langage L constitué des entiers n tels que pour tout a premier avec n, $a^n = 1 \mod n$.

a) Montrer, en exhibant un algorithme probabiliste approprié que, $\overline{L} = \mathbb{N} \setminus L$ est dans RP.

b) L est-il dans BPP ?

– Exercice 2. Rappelons que BPP est l'ensemble des langages L pour lesquels il existe un algorithme polynomial qui
– accepte $x \in L$ avec probabilité $\geqslant 2/3$
– rejette $x \notin L$ avec probabilité $\geqslant 2/3$.
Combien de fois faut-il appliquer l'algorithme pour ne se tromper sur la réponse qu'avec une probabilité $1/2^{20}$?

– Exercice 3. On considère le langage DH (Diffie-Hellman) constitué des quintuplets $(p, g, g^a \bmod p, g^b \bmod p, b^{ab} \bmod p)$ où p est premier et g primitif modulo p.

a) Montrer que DH est aussi l'ensemble des quintuplets

$$\{(p, g, h, y_1, y_2) \mid \exists x,\ y_1 = g^x \bmod p\ y_2 = h^x \bmod p\}.$$

b) Mimer le protocole sans divulgation de connaissance d'un logarithme en base g modulo p, pour proposer un candidat protocole sans divulgation d'appartenance à DH.

c) Démontrer, sa complétude, correction (ou validité), et caractère sans divulgation.

– Exercice 4. Soient p un nombre premier, q un nombre premier divisant $p-1$, et g un élément d'ordre q du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Soit $x \in \{0, 1, \dots, q-1\}$ et soit $y = g^x \mod p$. L'entier y est rendu public, l'entier x est maintenu secret. On considère le protocole suivant, censé démontrer la connaissance du secret x.

– Le prouveur donne un entier t modulo q au vérificateur.
– Le vérificateur choisit aléatoirement et uniformément un entier

$$c \in \{0, 1, \dots, q-1\}$$

et le donne au prouveur.
– Le prouveur donne au vérificateur un entier z modulo q et le véricateur vérifie l'égalité

$$\alpha^z = ty^c \mod p.$$

S'il y a égalité il accepte que le prouveur connaît x : sinon il rejette.

Démontrer que ce protocole est complet, valide, et sans divulgation.

– Exercice 5. Protocole de Guillou-Quisquater.

On considère un entier RSA n et un exposant public e associé à l'exposant secret d. Soit J une donnée publique et $S = J^{-d}$ une quantité secrête associée. On supposera e petit devant n et on fait l'hypothèse cryptographique suivante : il est algorithmiquement difficile, sans connaître la factorisation de n, de déterminer un quelconque élément de l'ensemble

$$E = \{S, S^2, \ldots, S^{e-1}\}.$$

On considère le protocole suivant, destiné à démontrer la connaissance de S.
– P choisit aléatoirement un entier r modulo n, calcule $x = r^e \bmod n$ et le transmet à V.
– V choisit aléatoirement et uniformément un entier $i \in \{1, \ldots, e\}$ et le transmet à P.
– P calcule et transmet à V la quantité $y = rS^i \bmod n$.
Le vérificateur V calcule $J^i y^e \bmod n$ et accepte si cette quantité égale x. Il refuse le protocole sinon.

Démontrer que ce protocole prouve la connaissance de S : détailler la complétude, validité et caractère sans divulgation.

– Exercice 6. Soit $n = pq$ un entier RSA, e un exposant de chiffrement, d l'exposant secret de déchiffrement associé. Le protocole suivant a pour but de prouver au vérificateur V que le prouveur P connaît l'exposant secret $d \mod \phi(n)$.

– V choisit un entier x aléatoire et le donne à P
– P calcule $y = x^d \mod n$ et le donne à V
– V vérifie que $y^e = x \mod n$.

Ce protocole est-il sans divulgation ? Pourquoi ?

– Exercice 7. Le protocole suivant était proposé sur wikipédia pour illustrer la notion de protocole sans divulgation. Il s'agit de démontrer qu'un graphe G est hamiltonien.
– P commence par fabriquer un graphe H isomorphe à G en permutant aléatoirement les sommets de G. Puis il donne H à V.
– V tire à pile ou face. Il donne le résultat à P.
– Si c'est pile, P donne à V l'isomorphisme entre G et H.
– Si c'est face P montre à V un circuit hamiltonien de H.
A-t-on bien affaire à un protocole sans divulgation ?