Cryptologie

Durée : 2h.
Notes de cours et de TD autorisées.

Exercice 1 Candide affirme connaître un secret : il saît décomposer un grand entier n en ses deux facteurs premiers p et q ($n = p \cdot q$). Ne souhaitant pas divulguer ce secret à Oscar, il se refuse à fournir ces deux entiers p et q à Oscar mais se propose de calculer rapidement une racine carrée modulaire modulo n de tout nombre entier que lui fournirait Oscar. Que pensez-vous de Candide ? Justifiez votre réponse.

Exercice 2 Considérons le protocole de signature suivant qui permet à Alice de signer un message m authentifié par Bob. Dans ce protocole H désigne une fonction associant à tout message m et à tout entier $K \in [1, n-1]$ un entier dans $[0, n-1]$. [illegible]

```
%Protocole de génération et diffusion des clefs par Alice

Alice calcule deux entiers premiers aléatoires p et q;
      calcule n ← p·q ;
      calcule un entier e ∈ [2,n−1] premier avec φ(n) = (p−1)·(q−1) ;
      calcule un entier a ∈ [2,n−1] tel que A := a^(−e)mod(n) est premier avec n;
      publie (n,e,A) ;

%Protocole de signature d'un message m par Alice

Alice choisit aléatoirement un entier k ∈ [1,n−1] ;
      calcule h ← H(m, k^e mod(n)) ;
      calcule s ← (k·a^h)mod(n) ;
      envoie (h,s) ;

%Authentification de la signature (h,s) du message m par Bob

Bob   vérifie l'égalité h = H(m,(s^e A^h)mod(n)) ;
```

1. Prouver qu'il s'agit bien d'un protocole de signature.
2. Calculer les expressions $a^{-1}\mathrm{mod}(p \cdot q)$ et $a^{-e}\mathrm{mod}(p \cdot q)$ pour les entiers $(a, e, p, q) = (23, 6, 5, 9)$.
3. Indiquer le détail des calculs nécessaires pour évaluer l'expression $s \leftarrow (k \cdot a^h)\mathrm{mod}(n)$ selon une complexité en temps polynomial.
4. Présenter et nommer un (premier) problème sur lequel repose la sécurité de ce protocole.

5. Une méthode pour réaliser l'instruction

   `calcule un entier a` $\in [2, n-1]$ `tel que` $A := a^{-e}\text{mod}(n)$ `est premier avec n;`

   consiste à choisir un entier $A \in [2, n-1]$ premier avec n puis à calculer un entier $a \in [2, n-1]$ égal à $(A^{-1}\text{mod}(n))^{(\frac{1}{e}\text{mod}(\varphi(n)))}\text{mod}(n)$. Démontrer qu'une telle valeur a vérifie l'équation souhaitée.

6. Un observateur remarque qu'en utilisant l'expression $(A^{-1}\text{mod}(n))^{(\frac{1}{e}\text{mod}(\varphi(n)))}\text{mod}(n)$, Oscar pourrait porter tort à Alice car :

   (a) la connaissance par Oscar de a lui permet de contrefaire de la signature de Alice.

   (b) l'évaluation de cette expression est facile car

   (c) le calcul $(x, m) \mapsto x^{-1}\text{mod}(m)$ est facile.

   (d) le calcul $(x, y, m) \mapsto x^{y}\text{mod}(m)$ est facile.

   Que pensez-vous de la véracité de chacun des points précédents ?

7. Considérons le problème suivant :

   `Auxiliaire`
   `E: la clef publique de Alice (n,e,A) et un message m`
   `S: deux entiers h et t tels que :` $h = H(m, A^t)$ `et` $h \equiv t$ `mod`(e)

   (a) En supposant que auxiliaire résolve le problème de même nom et qu'il s'éxécute en temps polynomial, que pensez-vous de l'algorithme suivant ? Prouver en quelques lignes votre réponse.

   ```
   fonction kesako((n,e,A):clef ; m : message):couple d'entiers
   (h,t) ← auxiliaire((n,e,A),m) ;
   x ← (t-h)/e ;
   retourner (h,A^x mod(n)) ;
   ```

   (b) Evaluez la correction et la complexité en fonction notamment de e de l'algorithme suivant :

   ```
   fonction auxiliaire((n,e,A):clef ; m : message):couple d'entiers
       faire
           choisir t aléatoirement dans [1,n-1] ;
           calculer h ← H(m,A^t) ;
       jusqu'à  h ≡ t mod(e)

       retourner (h,t)
   ```

   (c) Quelle préconisation proposez-vous en ce qui concerne l'entier e ?

8. Proposez une définition de la fonction H.