Pierre Wassef, Arithmétique, application aux codes correcteurs et à la cryptographie.

1 Plan

1. Enonce du protocole
2. Preuve du bon fonctionnement du protocole (Wassef 5.11 et 5.12)
3. Complexité (protocole et craquage) (Meunier, p7.)
4. Nombre de clefs de déchiffrement (de tête)
5. Autres failles (selon temps) (bof, plutôt parler de signature et bosser l'idée)

2 Développement

Protocole : Wassef p.83
Alice choisit $q, p \in \mathcal{P}$ et calcule $n = pq$ ainsi que $\varphi(n) = (p-1)(q-1)$
Elle choisit d premier avec $\varphi(n)$ et calcule $e \equiv d^{-1} \mod \varphi(n)$.
Elle publie la clef publique (n, e) et garde la clef secrète $(\varphi(n), d)$.
Encryptage : Bob veut transmettre le message $x \in \mathbb{Z}/n\mathbb{Z}$ à Alice. Il l'encrypte en calculant $y = x^e$ qu'il envoie à Alice
Décryptage : Alice calcule y^d et retrouve le message original x.

Lemme :
Dans le contexte du protocole, Si $t \in \mathbb{N}$ vérifie $t \equiv 1 \mod \varphi(n)$, alors $\forall a \in \mathbb{N}, a^t \equiv a \mod n$.

Preuve :
Soient un tel t, il s'écrit $t = k\varphi(n) + 1$ avec $k \in \mathbb{N}$.
On a $\mathbb{Z}/n\mathbb{Z} \sim \mathbb{F}_q \times \mathbb{F}_p$, il suffit de montrer le résultat sur $\mathbb{F}_p^\times$.
Soit $x \in \mathbb{F}_p^\times$, $x^t = x^{k\varphi(n)+1} = x \times \left(x^{p-1}\right)^{k(q-1)}$.
Or, d'après la congurence d'Euler, $x^{\varphi(q)=1}$ soit $x^{q-1} = 1$.
Donc $x^t \equiv x \mod p$.
(conclure à l'oral)

Corollaire :
Dans le même contexte, $x \in \mathbb{Z}/n\mathbb{Z} \mapsto x^e \in \mathbb{Z}/n\mathbb{Z}$ est une bijection, et sa réciproque est $x \mapsto x^d$.

En effet : $ed \equiv 1 \mod \varphi(n)$.

Complexité : On admet le tableau suivant (Annexe du plan)
La mise en place du protocole est en temps logarithmique : le calcul de n est une multiplication, le calcul de d également en utilisation l'A.E.E.
Les phases de cryptage et d'encryptage sont en temps logarithmique avec le procédé d'exponentiation rapide.

Supposons qu'un individu extérieur ait accès à $\varphi(n)$:
On a alors $\begin{cases} n = pq \\ \varphi(n) = (p-1)(q-1) \end{cases}$ on connaît donc $\begin{cases} m = p+q \\ \Delta = (p-q)^2 \end{cases}$ et on détermine p et q en temps logarithmique.

Clefs de déchiffrements :
On appelle $r \in \mathbb{Z}/n\mathbb{Z}$ clef de déchiffrement si r vérifie : $\forall x \in \mathbb{Z}/n\mathbb{Z}, (x^e)^r = x$.

Proposition: Soit $m = ppcm(q-1, p-1)$ et $u \in \mathbb{Z}$, les conditions suivantes sont équivalentes :

i $\forall x \in \mathbb{Z}/n\mathbb{Z}, x^u = x$

ii $u = 1 \bmod m$

. On en déduit qu'il existe $pgcd(p-1, q-1)$ clefs de déchiffrement.

Preuve :

($ii \to i$ se fait comme le lemme).
Montrons $i \iff p-1|u-1$ et $q-1|u-1$.
D'une part $\mathbb{Z}/n\mathbb{Z} \sim \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ (anneaux) et d'autre part $\mathbb{Z}/p\mathbb{Z}^\times$ est cylique, d'ordre $p-1$ (de même pour q). cqfd.