C[illegible] p[illegible]tre [illegible]

[illegible]ntrod ct[illegible]on[illegible] [illegible] cryptogr p[illegible]e

[illegible].1 Le pro[illegible]è[illegible]e

Cryptage, décryptage, clé.

[illegible]. A [illegible]e[illegible]st[illegible] [illegible] [illegible]r[illegible] Ad[illegible]e[illegible] n)

Le nombre $n = pq$ est un produit de (grands) nombres premiers. Alice choisit c premier avec $\phi(n) = (p-1)(q-1)$. Sa clé publique est (n, c). Elle calcule sa clé secrète d en inversant c modulo $\phi(n)$.

Bob veut envoyer à Alice un message représenté par $m \in \mathbb{Z}/n$ (ou une suite de tels m). Il calcule et envoit $m' = m^c \bmod n$.

Alice calcule $m'^d \bmod n$.

[illegible].3 E[illegible] [illegible] [illegible]

p est un grand nombre premier ; g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Alice choisit sa clé secrète, a et calcule : $A = g^a \bmod p$. Sa clé publique est (p, g, A).

Bob choisit b, calcule $B = g^b \bmod p$. Il encode le message $m \in \mathbb{Z}/p$ avec la formule $m' = mA^b \bmod p$. Il envoit à Alice (B, m').

Alice calcule $m'/B^a = m'B^{p-1-a} \bmod p$.