Feuille TD 2 - RSA

1 Codage et décodage RSA.

On considère la clef publique RSA (11, 319), c'est-à-dire pour $n = 319$ et $e = 11$.
Note : on pourra utiliser les résultats suivants :

- $319 = 11 \times 29$; $10^{11} = 263 \pmod{319}$; $263^2 = 216 \times 319 + 265$;
- $133^3 = 12 \pmod{319}$; $133^{25} = 133 \pmod{319}$;
- $11^2 = 121 \pmod{280}$; $11^4 = 81 \pmod{280}$; $11^8 = 121 \pmod{280}$; $11^{16} = 81 \pmod{280}$;
- $95 = 64 + 31$; $81.11 = 51 \pmod{280}$; $81.121 = 1 \pmod{280}$.

1. Quel est le message correspondant au codage avec cette clé du message $M = 100$?
2. Calculer d la clé privée correspondant à la clé publique e.
3. Décoder le message $M' = 133$.
4. Le message codé 625 peut-il résulter d'un codage avec la clé publique ? Même question avec la clé privée.

2 Cryptographie RSA et authentification

Un professeur envoie ses notes au secrétariat de l'École par mail. La clef publique du professeur est (3,55); celle du secrétariat est (3,33).

1. Vérifier que la clef privée du professeur (supposée connue de lui seul) est 27; et que celle du secrétariat est 7.

2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef RSA du secrétariat. Quel message chiffré correspond à la note 12 ?

3. Pour assurer l'authenticité des messages contenant les notes, le professeur signe ses messages pour le secrétariat aprés les avoir chiffrés. Le secrétariat reçoit le message 23. Quelle est la note correspondante ?

3 Quelques attaques de RSA.

1. Montrer que casser un code RSA de clef publique (n, e) avec $e = 3$ est polynomialement aussi difficile que factoriser n.
Ceci fonde la robustesse de l'algorithme RSA; mais cela ne justifie pas pour autant une confiance aveugle en n'importe quelle implémentation de RSA car de nombreuses attaques sont possibles liées à des mauvais choix d'implémentation ou de protocoles. Les questions suivantes présentent quelques unes de ces attaques.

2. Attaque par diffusion de messages sur un même exposant e petit. William, Jack et Averell ont respectivement les clefs RSA publiques $(n_W, 3)$, $(n_J, 3)$ et $(n_A, 3)$. Joe envoie en secret à chacun d'eux le même message x avec $0 \leq x < \text{Min}(n_W, n_J, n_A)$.
Montrer que Lucky Luke, qui voit passer sur le réseau $x^3 \mod n_W$, $x^3 \mod n_J$ et $x^3 \mod n_A$ peut facilement calculer x.
Indication. On rappelle (ou on admettra !) que pour a et k entier, la méthode de Newton permet de calculer très rapidement $\lfloor a^{1/k} \rfloor$, en temps $O(\log^2 a)$.

3. Attaque par texte chiffré bien choisi. Eve intercepte le message c chiffré envoyé par Bob à Alice : $c = m^{e_A} \mod n_A$. Pour déchiffrer c, Eve procède comme suit :

1. Eve choisit un entier $0 < r < n_A$ au hasard et calcule $x{:=}r^{e_A} \mod n_A$;
2. Eve calcule $y{:=}x.c \mod n_A$;
3. Eve demande à Alice de signer y avec sa clef privée; Alice renvoit à Eve $u = y^{d_A} \mod n_A$.

Montrer que Eve peut alors facilement découvrir le message m émis par Bob (on calculera $u.r^{-1} \mod n_A$). Moralité ?

4. Attaque par modulo commun. Une implémentation de RSA donne à deux personnes (Alice et Bob) le même nombre n (produit de deux nombres premiers) mais des clefs (e_A, d_A) et (e_B, d_B) différentes. On suppose de plus que e_A et e_B sont premiers entre eux (ce qui est le plus général).
Supposons alors que Alice et Bob chiffrent un même message m et que Eve intercepte les deux messages $c_A = m^{e_A} \mod n_A$ et $c_B = m^{e_B} \mod n_B$ qu'elle sait être deux chiffrements du même message m.
Montrer que Eve peut alors très facilement découvrir le message m (on pourra utiliser le calcul des coefficients de Bezout associés à e_A et e_B). Moralité ?

4 Cryptographie à clef publique par résidu quadratique

Soient a et b deux entiers; on dit que $a \neq 0$ est un *carré* (ou *résidu quadratique*) modulo b ssi il existe x tel que $x^2 \equiv a \mod b$.
On dit alors que x est une *racine carrée* de a modulo b.
Dans tout l'exercice, p et q désignent deux nombres premiers différents de 2 et $n = p.q$.

1. Dénombrement des carrés dans $\mathbb{Z}/n\mathbb{Z}^\star$

a. Vérifier que si $x^2 \equiv a \mod b$, alors $(b-x)^2 \equiv a \mod b$.

b. Montrer que si a est un carré modulo n, alors a est aussi un carré modulo p et modulo q.

c. Montrer que tout carré $a \neq 0$ modulo p a exactement 2 racines : x et $y = p - x$.

d. En déduire que tout carré a dans $\mathbb{Z}/n\mathbb{Z}$, tel que a est premier avec p et q, admet exactement quatre racines carrées distinctes x_1, $n - x_1$, x_2 et $n - x_2$. **Indication :** utiliser le théorème chinois des restes.

e. En utilisant que $(\mathbb{Z}/p\mathbb{Z}^\star, \times)$ est cyclique, montrer qu'il y a $\frac{p-1}{2}$ carrés non nuls modulo p.

f. En déduire le nombre de carrés dans $\mathbb{Z}/n\mathbb{Z}^\star$.

2. Difficulté du calcul des racines carrées. Soit $a < n$; le but de cette question est de montrer que calculer les racines carrées x de $a \neq 0$ modulo n est (polynomialement) plus difficile que factoriser n.
On suppose donc dans toute cette question que l'on connaît les 4 racines distinctes x_1, x_2, $(n - x_1)$ et $(n - x_2)$ de a modulo n; on veut montrer qu'il est alors possible de factoriser rapidement n.

a. Soit $u = x_1 - x_2 \mod n$ et $v = x_1 + x_2 \mod n$. Montrer que $u.v \equiv 0 \mod n$.

b. En justifiant que $1 \leq u, v < n$, expliquer comment calculer alors les deux facteurs p et q de n à partir de u et v.

c. Donner une majoration du coût de ce calcul en fonction du nombre de bits de n.

d. En déduire que la fonction *carré* de $\mathbb{Z}/n\mathbb{Z}$ définie par $\mathit{carré}(x) = x^2 \mod n$ peut être considérée comme une fonction à sens unique.

3. Protocole d'identification quadratique. Soit $n = pq$ un nombre de 512 bits, produit de deux nombres premiers; p et q ne sont connus que d'un tiers de confiance TTP, mais pas d'Alice et de Bob.
Pour s'identifier, Alice choisit l'entier $x_A < n$ comme clef secrète unique. Soit $a = x_A^2 \mod n$; TTP délivre alors à Alice un passeport sur lequel figure les entiers publics n et a.

a. On suppose que seule Alice (et peut-être TTP) connaît x_A et que personne en dehors de TTP ne sait calculer les racines carrées modulo n; est-ce raisonnable ?

b. Pour identifier Alice, le douanier Bob qui consulte le passeport d'Alice utilise le protocole suivant (qu'il répète 2 ou 3 fois) :

   1. Alice choisit un nombre r au hasard qu'elle garde secret;
   2. Alice calcule $y = r^2 \mod n$ et $z = x_A.r \mod n$;
   3. Alice envoie y et z à Bob;
   4. Bob teste l'identité d'Alice en vérifiant que $a.y - z^2 = 0 \mod n$.

   Montrer que si un espion, qui ne sait pas calculer des racines carrées, a pu calculer r, c'est nécessairement qu'il connaît la clef secrète x_A de Alice. Qu'en déduisez-vous ?

c. Cependant, avec le protocole précédent, un espion peut se faire passer pour Alice : à la place des étapes 1 et 2, l'espion tire au hasard un nombre z et calcule $y = z^2/a \mod n$.
   Pour éviter cela, le protocole suivant (dit protocole à *zéro-connaissance*) est utilisé :

   1. Alice choisit r au hasard, calcule $y = r^2 \mod n$ et envoie y à Bob;
   2. Bob tire au hasard $b \in \{0, 1\}$; il envoie b à Alice;
   3. Si Alice reçoit 0, elle envoye $z = r$ à Bob (i.e. une racine de y modulo n);
      si elle reçoit 1, elle envoye à Bob $z = x_A.r \mod n$ (i.e. une racine de $y.m \mod n$).
   4. Bob teste l'identité d'Alice en vérifiant que $y.a^b - z^2 = 0 \mod n$.

   Majorer alors la probabilité que l'espion a de répondre correctement à Bob après k passages dans ce protocole.