TD Cryptographie

ENSSAT

Exercice 10

1. $a = 4$ n'engendre pas Z_5^* (car $4^3 = 4 \mod 5$). En revanche, 2 engendre Z_5^* donc est primitif.
2. Bob envoie
$$k_B = a^B \mod p = 3$$
Alice doit calculer $k = (k_B)^A \mod p = 4$ et doit envoyer à Bob ($k_A = a^A \mod p, kx$). Ainsi, Alice envoie le message
$$(4, 1)$$
3. Bob décrypte : tout d'abord, il calcule lui-même k en utilisant $k_A = a^A \mod p$ envoyé par Alice et en calculant $k = k_A^B \mod p$:
$$k = 4^3 \mod 5 = 4$$
Il doit désormais calculer l'inverse de k modulo p, par l'algorithme d'Euclide étendue; il obtient comme inverse $k^{-1} = 4$. Il décrypte alors le message envoyer par Alice ($y = 2$) en calculant $k^{-1}y \mod p$, c'est-à-dire :
$$k^{-1}y = 4 \times 1 \mod 5 = 4$$
Ainsi, Bob a décrypté le message $x = 4$.

Exercice 15

1. (a) On a, pour k grand :
$$N(k) \approx \pi(2^k) - \pi(2^{k-1})$$
soit, en utilisant le théorème des nombres premiers démontrés par Hadamard et la Vallée Poussin :
$$\begin{aligned} N(k) &\approx \frac{2^k}{\ln(2^k)} - \frac{2^{k-1}}{\ln(2^{k-1}} \\ &\approx \frac{2^k}{k\ln(2)} - \frac{2^{k-1}}{(k-1)\ln(2)} \\ &\approx 2^{k-1}\frac{2(k-1)-k}{k(k-1)\ln(2)} \\ &\approx 2^{k-1}\frac{k-2}{k(k-1)\ln(2)} \approx \frac{2^{k-1}}{k\ln(2)} \end{aligned}$$
(b) On choisit aléatoirement un nombre impairs compris entre 2^{k-1} et $2^k - 1$ inclus. Il y a $\frac{2^k - 2^{k-1}}{2}$ nombres impairs. On applique alors la probabilité qu'il soit premier est (pour k grand et en utilisant l'approximation vue précédemment) :
$$\begin{aligned} P &= \frac{N(k)}{\frac{2^k - 2^{k-1}}{2}} \\ &\approx \frac{\frac{2^{k-1}}{k\ln(2)}}{2^{k-1} - 2^{k-2}} \\ &\approx \frac{2}{k\ln(2)} \end{aligned}$$

2. (a) Cf cours.

   (b) On est sûr que le nombre est composé si l'algorithme renvoie faux. En revanche, s'il renvoie vrai, c'est soit que le nombre n est premier, soit qu'il ne l'est pas mais qu'on a tiré l'un des entiers a qui renvoie $f(a,b)$ vrai.

   (c) On suppose que n est composé. Puisqu'on choisit de manière uniforme l'entier a, l'algorithme renvoie vrai si on tombe sur l'un des entiers qui renvoie $f(n,a)$ vrai. Mais alors, par hypothèse de construction de f, on a :

$$\mathrm{P}_{n \text{ composé}}(f(a,n) \text{ renvoie vrai}) \leqslant \frac{\frac{n-1}{4}}{n} \leqslant \frac{1}{4}$$

   (d) On choisit aléatoirement l'entier a, et on effectue m fois la boucle. On a alors, en utilisant la question précédente,

$$\mathrm{P}_{n \text{ composé}}(\text{renvoie vrai}) = \prod_{i=1}^{m} \mathrm{P}_{n \text{ composé}}(f(a,n) \text{ renvoie vrai}) \leqslant \frac{1}{4^m}$$

3. On note C l'événement n est composé, et A l'événement "l'algorithme renvoie vrai". Alors on cherche :

$$\mathrm{P_A(C)}$$

   En utilisant les questions 1)a) et 2)d), on a alors :

$$\begin{aligned} \mathrm{P_A(C)} &= \frac{\mathrm{P(A \cap C)}}{\mathrm{P(A)}} \\ &= \frac{\mathrm{P(C)}}{\mathrm{P(A)}} \mathrm{P_C(A)} \qquad \text{par la formule de Bayes} \\ &\leqslant \frac{k \ln(2)}{2 \times 4^m} \end{aligned}$$

   Par exemple, pour $k = 1024$ et $m = 50$, on obtient

$$\mathrm{P_A(C)} \leqslant 2,5 \times 10^{-28}$$