Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 5.5 (bis)

Exercice 5.5 (bis) APPLICATION DE L'ALGORITHME DE POHLIG-HELLMAN

Appliquer l'algorithme de Pohlig-Hellman pour calculer le logarithme discret de h en base g dans $(\mathbb{Z}/p\mathbb{Z})^*$ où

$$
\begin{aligned}
p &= 3108245349559267029701540311839425705474585176323729835415199 49 \\
g &= 2 \\
h &= 6747174816035556523377570381184709853273515308077860044811648 1
\end{aligned}
$$

Solution : Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est d'ordre

$$p - 1 = 2 \cdot 1342417 \cdot 1424589 \cdot 1512007 \cdot 1523978 \cdot 1721483 \cdot 1812351 \cdot 1833613^4.$$

Notons x le logarithme discret de h en base g. En appliquant l'algorithme de Shanks pour calculer la valeur de x modulo chaque nombre premier qui divise $p - 1$ avec multiplicité 1, nous trouvons

$$\begin{aligned} x &\equiv 1 \bmod 2 \\ x &\equiv 1211151 \bmod 1342417 \\ x &\equiv 714949 \bmod 1424589 \\ x &\equiv 1334025 \bmod 1512007 \\ x &\equiv 710833 \bmod 1523978 \\ x &\equiv 585598 \bmod 1721483 \\ x &\equiv 135787 \bmod 1812351 \end{aligned}$$

En calculant la valeur de x modulo les puissances de 1833613, nous obtenons successivement

$$\begin{aligned} x &\equiv 1110324 \bmod 1833613 \\ x &\equiv 1046231350316 \bmod 1833613^2 \\ x &\equiv 1114582961692111506 \bmod 1833613^3 \\ x &\equiv 109055846061194779667853 30 \bmod 1833613^4 \end{aligned}$$

et finalement, en appliquant le théorème chinois des restes, nous obtenons la valeur de x suivante :

$$x = 2810428814766099466567180485405284948829324730606375276752 42259.$$

□