TD sur la cryptographie

Igor Stéphan

7 avril 1999

Références

[Sti96] D. Stinson. *Cryptographie, Théorie et Pratique.* International Thomson Publishing, 1996.

Exemple sur le système RSA

Bob a conservé les clés privées $p = 23$ et $q = 19$ (donc $n = 437$ et $\Phi(n) = 22 * 18 = 396 = (3^2 * 11 * 2^2))$ et a choisi un $b = 5$ premier avec $\Phi(n)$. Bob a calculé sa clé privée $a = b^{-1} \mod 396$ avec l'algorithme *inverse* qui calcul l'inverse dans un corps :

$$\begin{aligned}
a &= 5^{-1} \mod 396 \\
&= inverse(5, 396, 0, 1, 396) \\
&= inverse(1, 5, 1, (0 - ((396/5) * 1)) \mod 396, 396) \\
&= -79 \mod 396 \\
&= 317
\end{aligned}$$

Bob a publié les clés publiques $n = 437$ et $b = 5$.

Alice veut envoyé le message 20 à Bob, elle calcule donc $20^5 \mod 437$ par l'algorithme $square - and - multiply$:

$$\begin{aligned}
20^5 \mod 437 &= sm(20, 5, 437, 3, 1) \\
&= sm(20, 5, 437, 2, (1^2 \mod 437) * 20 \mod 437) \\
&= sm(20, 5, 437, 1, 400) \\
&= sm(20, 5, 437, 0, (400^2 \mod 437) * 20 \mod 437) \\
&= 286
\end{aligned}$$

Alice expédie 286 à Bob.

Pour décrypter le message Bob calcule $286^{317} \mod 437$:

$$
\begin{aligned}
286^{317} \mod 437 &= sm(286, 317, 437, 9, 1) \\
&= sm(286, 317, 437, 8, (1^2 \mod 437) * 286 \mod 437) \\
&= sm(286, 317, 437, 7, 286^2 \mod 437) \\
&= sm(286, 317, 437, 6, 77^2 \mod 437) \\
&= sm(286, 317, 437, 5, (248^2 \mod 437) * 286 \mod 437) \\
&= sm(286, 317, 437, 4, (20^2 \mod 437) * 286 \mod 437) \\
&= sm(286, 317, 437, 3, (343^2 \mod 437) * 286 \mod 437) \\
&= sm(286, 317, 437, 2, (362^2 \mod 437) * 286 \mod 437) \\
&= sm(286, 317, 437, 1, 153^2 \mod 437) \\
&= sm(286, 317, 437, 0, (248^2 \mod 437) * 286 \mod 437) \\
&= 20
\end{aligned}
$$

Bob sait maintenant que Alice lui a envoyé le message 20.