La catastrophe d'octobre 1979 est survenue au troisième jour de forte crue du Var. La charge sédimentaire en suspension a peut-être suffit à donner à l'eau douce chargée une densité supérieure à celle de l'eau de mer : le cours du fleuve se serait alors poursuivi au fond de la mer et aurait érodé les flancs instables du canyon du Var.

P. COUPRIE, Paris

Réponse de Philippe Heinrich

Je ne suis pas opposé a la thèse qu'un tsunami engendré au large aurait précédé l'effondrement de la digue et des sédiments sous-jacents, et de ce fait serait à l'origine de l'effondrement. Toutefois, elle ne fait pas l'unanimité, précisément en raison des contradictions entre les témoignages sur la chronologie des observations des vagues en différents points de la côte.

Les simulations numériques révèlent que l'effondrement de dix millions de mètres cubes de sédiments situés à proximité de la surface de l'eau engendre une vague de quelques mètres de hauteur localement, suffisante pour inonder les terrains situés en face de l'aéroport. Il n'a jamais été conclu que cet effondrement est à l'origine d'un tsunami. Bien au contraire, les simulations ont montré aussi que les vagues engendrées par cet effondrement n'expliquent pas le tsunami observé dans la Baie des Anges. Les modélisations que nous avons effectuées simulent des phénomènes hydrodynamiques, tels le déplacement d'un fluide par le mouvement d'une masse et la propagation d'ondes à la surface de l'eau. Elles ne permettent pas de conclure sur l'antériorité ou non de l'effondrement de la digue, ni sur la cause de cet effondrement.

L'origine de la vie

Pourquoi la vie a-t-elle plus de chances de venir d'une autre planète du Système solaire que de la Terre, alors qu'elles ont toutes à peu près le même âge (voir *Origine extraterrestre ?*, par C.-A. Roten, *Pour la Science*, juillet 1999)? Si elle vient d'un autre système planétaire, c'est un autre problème...

Frédéric MALHER, Paris

Réponse de C.-A. Roten

L'émergence de la vie est associée à l'existence d'une croûte planétaire solide. En son sein ou dans un océan, des molécules peuvent s'auto-organiser pour permettre l'apparition d'une première cellule. Tout corps orbitant autour du Soleil s'est formé il y a 4,6 milliards d'années. Suite au bombardement météoritique intense de l'accrétion et à la chaleur émise par la fission des atomes radioactifs, les constituants de Mars et de la Terre se sont séparés pour former un noyau et un manteau. Par la suite, seule la chaleur émise par la fission nucléaire était suffisante pour empêcher la solidification d'une croûte planétaire. Comme Mars et la Terre ont une concentration d'atomes radioactifs similaire, Mars, plus petite, s'est refroidie plus rapidement car le rapport de sa surface à son volume est plus important que celui de notre planète. Mars, dont la surface s'est solidifiée avant celle de la Terre, a donc pu abriter les plus anciennes formes de vie du Système solaire.

Gingko costaud

Le *Ginkgo biloba* résiste à de nombreuses agressions (voir *La résistance des ginkgos*, *Pour la Science*, mai 1999) : il aurait même survécu à l'explosion atomique d'Hiroshima. Toutefois, ce n'est qu'à Kyoto que j'ai vu beaucoup de ginkgos le long des avenues. À Paris, malheureusement, je ne connais que celui du Jardin des Plantes.

Claude CARDOT, Gif sur Yvette

Réponse de T. T. Nguyen Tu et H. Bocherens

À Hiroshima, un *Ginkgo biloba* a effectivement survécu à la bombe atomique : ses feuilles ont repoussé au printemps suivant l'explosion bien que son appareil végétatif ait entièrement brûlé. L'implantation des ginkgos dans les villes est de plus en plus importante, non seulement au Japon, mais aussi en Europe. De nombreux boulevards et parcs de Tokyo sont plantés de ginkgos. À Paris, son implantation est plus récente : tous les marronniers bordant les avenues n'ont pas été remplacés par des ginkgos! Mais dès que des arbres sont à planter le choix est le plus souvent porté sur le ginkgo, par exemple au Musée de sculpture en plein air, sur le quai Saint Bernard.

Lettre codée

Dans l'article *Paiements sur l'Internet* (voir *Pour la Science*, juin 1999), Octavian Ureche et Réjean Plamondon écrivent : «Ce système est relativement sûr : en Europe, le protocole SSL chiffre les données avec des clés de 40 bits. Autrement dit, pour percer le code de chiffrement, il faudrait trouver les facteurs premiers d'un nombre de 40 bits (ou 10 chiffres), ce qui prendrait des jours à un ordinateur de bureau.» Je pense qu'il y a ici une confusion : la clé de 40 bits utilisée est la clé d'encryptage symétrique (plus précisément, la partie secrète de cette clé, l'algorithme utilisé (RC4) étant de type «stream cipher», chaque message a une clé différente). Cette clé est encodée au moyen d'un algorithme à clé publique, utilisant une clé beaucoup plus grande. La factorisation d'un nombre de 40 bits (12 chiffres) prend moins d'une seconde...

Jacques WILLEKENS, Bruxelles

Réponse d'Octavian Ureche et Réjean Plamondon

Le protocole SSL implique plusieurs phases. Une première phase consiste en l'établissement du lien encrypté de communication entre le client et le serveur. Cette phase est elle-même formée de deux étapes: l'authentification du serveur et l'authentification (optionnelle) du client. La deuxième phase consiste en l'envoi proprement dit des données. Si la première phase utilise effectivement un chiffre asymétrique, notamment le chiffre RSA, la deuxième phase utilise un chiffre symétrique. Lors de la première étape de la première phase, en répondant à la demande du client, le serveur envoie son certificat et ses préférences d'encryptage (le chiffre à utiliser, etc.). Le client crée une clé de session (chaque session, et non pas chaque message lors d'une même session, ayant une clé différente) et l'envoie au serveur, encryptée avec la clé publique de ce dernier. Le serveur décrypte la clé de session et s'identifie en retournant un message authentifié avec la clé de session. Toutes les données seront par la suite encryptées et authentifiées avec cette clé de session. La clé de session utilisée par un algorithme d'encryptage symétrique tel que RC4 a une longueur de quelques dizaines de bits, 40 jusqu'à tout récemment, 128 depuis peu de temps. Même s'il n'est pas trop difficile de craquer des clés très courtes, la cryptanalyse n'est pas à la portée de tout le monde. Toutefois, ceci est en train de changer avec la puissance croissante des ordinateurs personnels accessibles à des prix dérisoires. C'est pour de telles raisons que de plus en plus de gouvernements allègent leurs politiques en matière de cryptographie pour passer à des clés plus longues, donc plus sûres.

Écrivez à *Pour la Science* vos réactions, vos commentaires et vos réflexions sur l'actualité scientifique et vos relations avec la science. L'adresse de *Pour la Science* sur Internet est : tribune@pourlascience.fr. D'autres contributions de lecteurs sont sur le site Web à http://www.pourlascience.com.