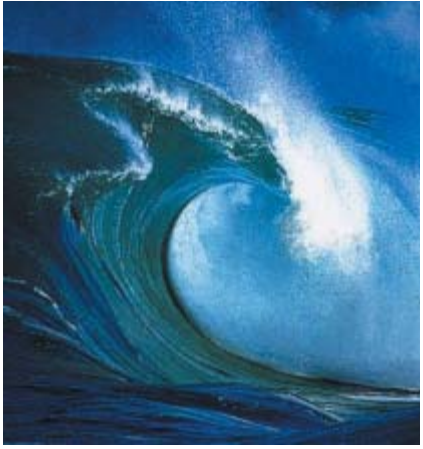


La grande vague

FRANÇOIS CHARRU

La déferlante saisie par le maître japonais est née de quelques rides à la surface de l'océan, à des centaines de kilomètres.

«*Depuis l'âge de cinq ans, j'ai la manie de recopier la forme des choses et depuis près d'un demi-siècle, j'expose beaucoup de dessins ; cependant je n'ai rien peint de notable avant d'avoir soixante-dix ans. À soixante-treize ans, j'ai assimilé légèrement la forme des herbes et des arbres, la structure des oiseaux et d'autres animaux, insectes et poissons ; par conséquent à quatre-vingts ans, j'espère que je me serai amélioré et à quatre-vingt-dix ans que j'aurai perçu l'essence même des choses, de telle sorte qu'à cent ans j'aurai atteint le divin mystère et qu'à cent-dix ans, même un point ou une ligne seront vivants. Je prie pour que l'un de vous vive assez longtemps pour vérifier mes dires.*»

Hokusai, le vieux fou de peinture.

L'estampe *Sous la vague à Kanagawa*, du peintre japonais Katsushika Hokusai (1760-1849), appartient à la série «36 vues du mont Fuji», peintes entre 1831 et 1833. Exposée au Musée Guimet à Paris, elle est l'une des œuvres les plus célèbres de l'art oriental. Elle est signée *Iitsu*, l'un des nombreux noms qu'Hokusai s'est donné au cours de sa longue vie.

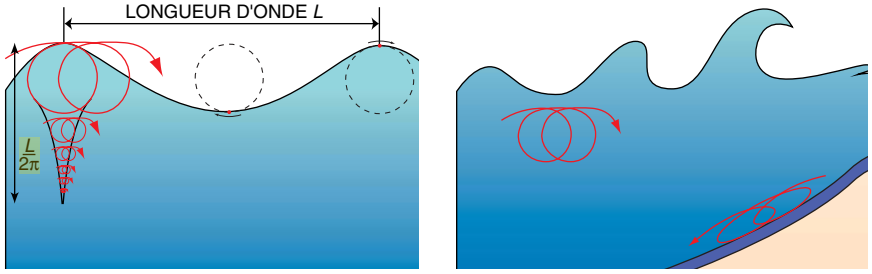
Le tableau suscite d'abord l'effroi, devant cette vague monstrueuse sur le point de s'abattre sur deux embarcations, au fond desquelles se blottissent quelques pêcheurs ou voyageurs. Une telle vague peut-elle vraiment se former? Comment a-t-elle pu atteindre de telles proportions? Imaginons son histoire.

À plusieurs centaines ou milliers de kilomètres de l'archipel nippon, le vent se lève sur une mer calme. De petites fluctuations de vitesse du vent engendrent des variations de pression et de cisaillement sur l'eau, lesquelles soulèvent de petites vaguelettes, ou rides, désordonnées. La longueur d'onde de ces rides – la distance entre deux crêtes – est de l'ordre du centimètre.

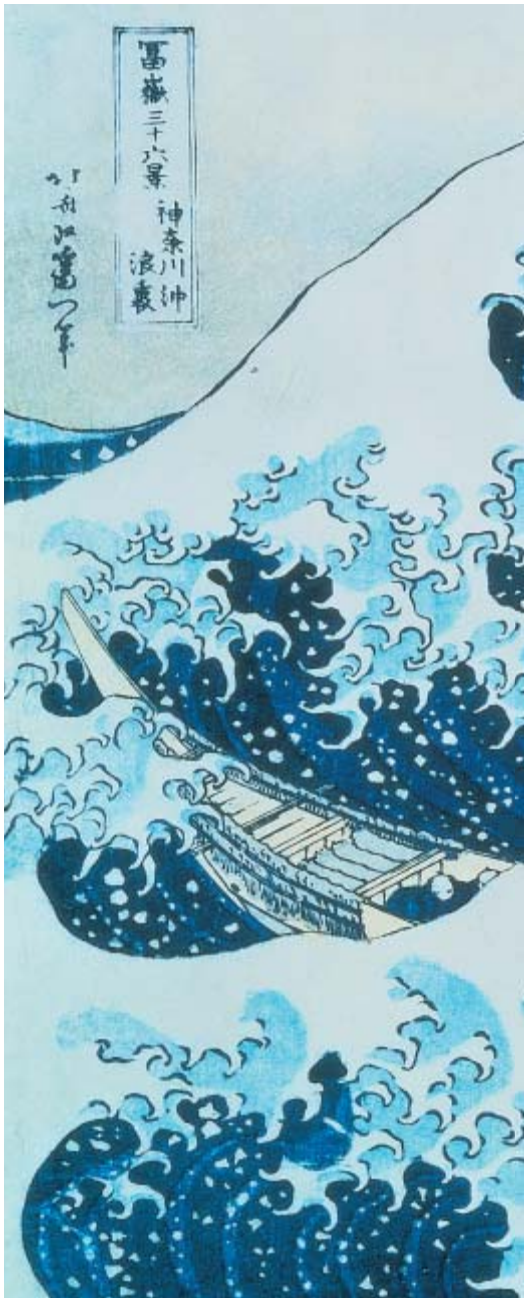
Sans le vent pour les entretenir, ces rides seraient vite amorties par la viscosité, c'est-à-dire la diffusion de la quantité de mouvement dans les interactions moléculaires. Mais le vent continue de souffler, il communique son énergie aux rides qui fusionnent pour en former de plus longues, d'amplitude supérieure : ces vagues mettent en mouvement une masse d'eau plus importante. Du fait de leur plus grande inertie, elles sont moins sensibles à la dissipation par la viscosité, et se propagent donc plus loin.

La tempête rugit maintenant : elle soulève des masses d'eau de différentes tailles sur une mer blanche d'écume (que les peintres décrivent bien mieux que les physiciens!). Bientôt la tempête s'éloigne, le vent tombe. L'agitation à petite échelle, celle qui met en jeu des longueurs inférieures au mètre, disparaît rapidement, dissipée par la viscosité. Les vagues longues se propagent plus vite que les courtes, aussi les rattrapent-elles : elles conjuguent leurs énergies et forment des vagues encore plus longues et plus rapides.

Une belle houle s'est formée, de deux ou trois cents mètres de longueur d'onde, totalement libre de ses mouvements dans le profond océan. Cette houle se propage sur des centaines de kilomètres, à raison de dix ou vingt mètres par seconde, en s'atténuant très peu. Selon les lois de l'hydrodynamique des fluides non vis-



Dans une vague, un petit volume d'eau avance dans le sens de la propagation lorsqu'il est au sommet et dans le sens inverse quand il est dans le creux. Des petits volumes suivent une trajectoire quasi circulaire dont l'amplitude décroît exponentiellement avec la profondeur jusqu'à devenir négligeable quand celle-ci atteint le sixième environ ($L/2\pi$) de la longueur d'onde de la vague *(à gauche, les échelles horizontales et verticales diffèrent)*. Près des côtes, le plateau continental oblige les vagues à s'enfler, à se raidir pour enfin déferler *(à droite)*. Ici, les petits volumes d'eau décrivent non plus des cercle, mais des trajectoires aplaties, car le fond perturbe les mouvements verticaux et crée une «couche limite» *(en violet)* où la viscosité dissipe l'énergie de la vague.



The Brigeman Art Library/Katsushika Hokusai

queux, la vitesse de la houle croît avec sa longueur d'onde, et chaque petit volume d'eau décrit un mouvement quasi circulaire, dont l'amplitude décroît exponentiellement avec la profondeur *(voir la figure)* et disparaît quand celle-ci atteint le sixième environ de la longueur d'onde.

Après un long voyage, la houle arrive sur la côte ; la remontée du plateau continental oblige les trajectoires des petits volumes d'eau à s'aplatir en ellipses, et entraîne un ralentissement de l'onde. Contrainte de contenir son énergie sur une profondeur plus faible, l'onde enfle, se creuse. La profondeur n'est maintenant plus que de quelques mètres. La viscosité, qui jusqu'à présent ne jouait qu'un rôle mineur, intervient maintenant dans une fine couche, de quelques millimètres d'épaisseur, près du fond. Dans cette «couche limite», l'oscillation de l'eau sur le fond sableux ou rocheux crée des tourbillons, de la turbulence, où la vague épuise son énergie.

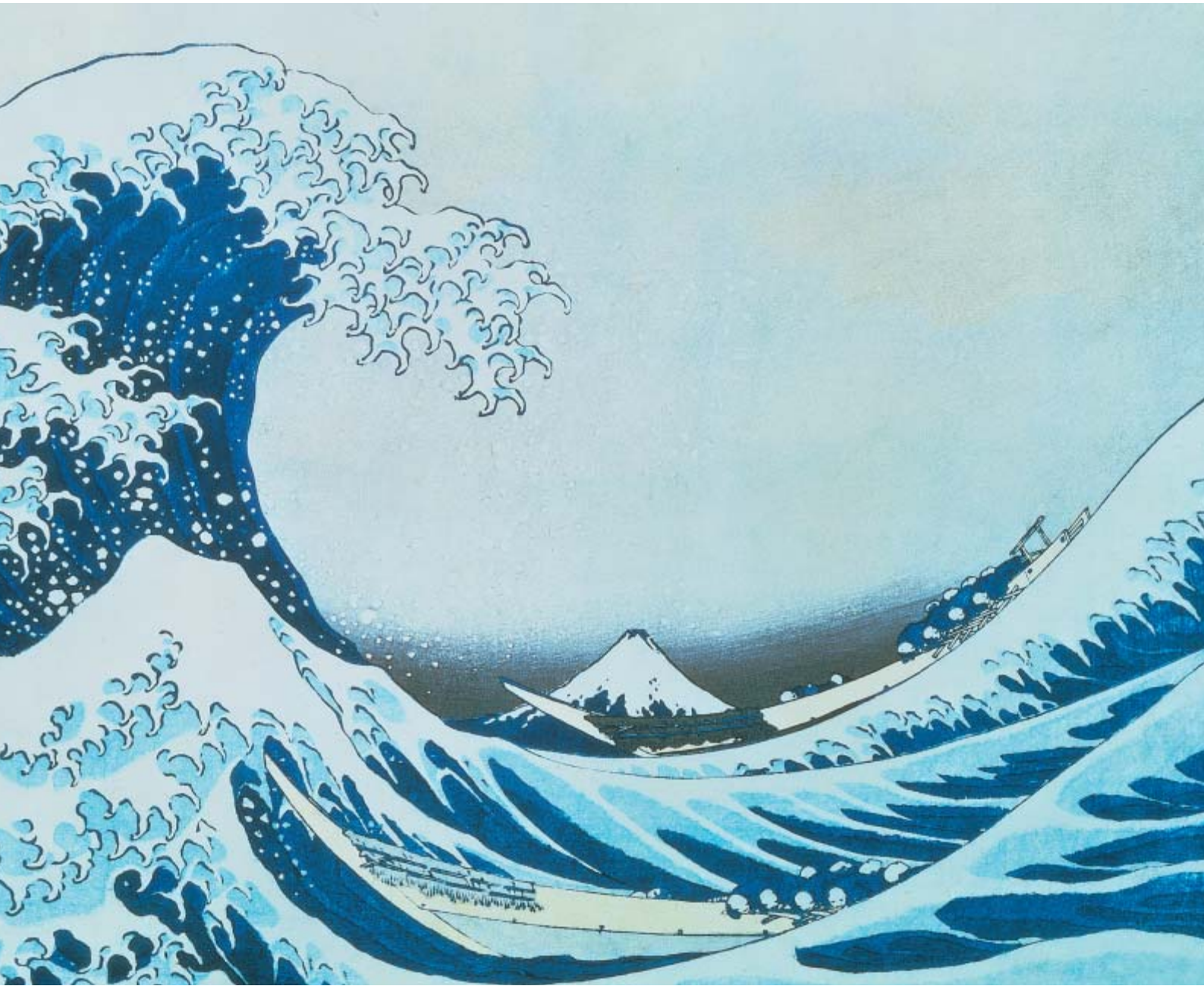
Plus dramatique, la crête tend à rattraper le creux. Cette différence de vitesse résulte de deux phénomènes : d'une part, la hauteur d'eau dans la crête est plus importante que dans le creux, et d'autre part, la vitesse croît avec la profondeur. La vague se déforme alors, son front se raidit, et bientôt la crête surplombe le creux du haut d'une muraille liquide. Emportée par son élan, elle s'étire encore, suspendue au-dessus du vide : elle déferle !

Voici la vague sous le pinceau d'Hokusai. Cédant à la gravité, elle s'incline dans une révérence orgueilleuse, s'enroule, le temps retient son souffle. Là haut, étirée en lames trop fines, déstabilisée par la tension de sa surface, cisaillée par le vent, l'eau perd sa cohésion. Elle se déchire en filaments, se pulvérise en dentelles de gouttelettes.

Mais point d'embruns dans le tableau d'Hokusai, plutôt des doigts menaçants, et de grosses gouttes, tels de lourds flocons de neige. Non, l'heure n'est pas à la légèreté, car quelques hommes se trouvent là, pêcheurs égarés dans le Maelström. Peut-être ces hommes savaient-ils l'endroit dangereux, à cause d'un haut-fond qui «brise la vague», ou de l'affrontement de courants contraires. Mais de là à imaginer ça ! Témoins terrorisés de l'agonie d'une géante, ils ne voient que ses doigts glacés, crochus, les mains gantées de blanc d'une étrangleuse. Pourront-ils échapper à la terrible étreinte ?

Cependant, pas de désespoir dans ce tableau, peut-être pas même la crainte de la mort. Au centre du rond ample que l'onde a dessiné, surgissent les pentes enneigées du mont Fuji, le bienveillant, le protecteur. Seul point fixe du tableau. Avec la sérénité d'un point cardinal, il a tout vu.

François CHARRU,
Université Paul Sabatier, Toulouse



J.-M. Thiriet

L'AGENT SECRET JOUE AUX CARTES

JEAN-PAUL DELAHAYE

Même les plus puissants des ordinateurs ne peuvent rien contre votre jeu de 54 cartes.

Une bombe atomique explose ! Elle est calculée pour ne pas faire de gros dégâts au sol, mais pour produire un éclair électromagnétique, c'est-à-dire un champ magnétique très puissant et très bref. Ce champ magnétique induit des courants électriques très forts dans tous les circuits, grille tous les transistors et met hors service tous les systèmes électroniques ! Que faire contre ce péril ? Comment pourrions-nous vivre dans un monde dont tous les ordinateurs sont brusquement devenus inopérants ? Comment pouvons-nous protéger nos données ?

Dans le cadre de la préparation à un tel événement et aussi pour le défi intellectuel qu'il constitue, le spécialiste de cryptographie Bruce Schneier a conçu un système de codage n'utilisant comme moyen de calcul qu'un simple jeu de 54 cartes. Le niveau de sécurité du système cryptographique de Schneier, qu'il dénomme *Solitaire,* est équivalent à celui des meilleurs algorithmes utilisés aujourd'hui (qui, eux bien sûr, exigent l'utilisation d'ordinateurs). Bien utilisé, il permet de crypter des messages que même les plus puissantes agences spécialisées d'espionnage et d'information ne pourront pas déchiffrer.

La méthode cryptographique de Schneier vous sera utile aussi, si dans votre métier d'agent secret vous souhaitez ne prendre aucun risque de vous faire repérer et que, pour cela, vous désirez ne porter sur vous aucun objet suspect. Elle pourra être utilisée par les hackers qui après s'être faits prendre (comme le fameux Kevin Mitnick) ont été condamnés à ne plus toucher un ordinateur.

La cryptographie moderne par sa compréhension approfondie des méthodes mathématiques pour cacher de l'information a fait progresser même les méthodes manuelles des bons vieux agents secrets des siècles passés. Ils ne pouvaient utiliser les ordinateurs absents et leurs procédés de chiffrement furent craqués par les services ennemis. Avec le *Solitaire* de Schneier ce ne sera plus possible !

Notons que *Solitaire* a été conçu par Schneier parce que dans le roman de Neal Stephenson intitulé *Cryptonomicon* (dont la traduction française par Jean Bonnefoy est en cours) certains personnages utilisent l'idée de la cryptographie avec un jeu de 54 cartes.

LE MASQUE JETABLE

La base de *Solitaire* est la méthode générale de codage par addition d'un message avec une clef (le message et la clef sont deux listes de lettres). Cette méthode est le fondement de nombreux systèmes cryptographiques. Pour coder le message «L'attaque est pour demain», qui comporte 21 lettres, on utilise une clef de 21 lettres, par exemple FUSREBJFYDZMPHYDALDIU, et on procède de la façon indiquée sur la figure 1.

Cette méthode de codage, lorsqu'on l'utilise avec une clef aléatoire qu'on ne réutilisera plus est une méthode absolument sûre qu'on dénomme méthode du masque jetable. C'est la seule méthode de cryptographie mathématique prouvée sûre d'une manière absolue. Le moindre écart dans son utilisation (clef non choisie aléatoirement car tirée d'un texte réel ; clef utilisée plusieurs fois) met la sécurité en péril car les cryptanalistes peuvent exploiter les particularités des clefs lorsqu'elles en possèdent et les usages multiples d'une même clef *(voir la figure 2).*

Le masque jetable, parfait en théorie, possède un grave défaut pratique : il faut que la clef soit aussi longue que le message à crypter. Aussi, n'est-elle que rarement utilisée. Cependant le principe du masque jetable est tellement simple et sa pratique si commode, qu'on l'utilise en remplaçant la clef aléatoire par une clef pseudo-aléatoire. Finalement, concevoir un bon système cryptographique peut se ramener à concevoir un bon procédé de création de suites pseudo-aléatoires. Certaines méthodes utilisées aujourd'hui comme l'algorithme RC4 fonctionne selon cette idée : un générateur pseudo-aléatoire fournit une clef aussi longue qu'on veut, qu'on utilise pour crypter des messages aussi longs qu'on le désire par le procédé de l'addition du message avec une clef pseudo-aléatoire.

La clef pseudo-aléatoire sera appelée *flux de clefs* car elle est produite en continu et peut être aussi longue qu'on le veut. Il ne faut pas la confondre avec les *clefs de base* qui permettront d'engendrer des flux de clefs différents. Les clefs de base servent à configurer le générateur de flux de clefs.

Une façon de procéder, déconseillée car trop simple, est de convenir que la clef de base est un mot (par exemple DTPDGCVA) et de décider que le flux de clefs sera obtenu en répétant indéfiniment la même clef de base : DTPDGCVA DTPDGCVA DTPDGCVA ... Cette méthode de codage où une clef courte est utilisée répétitivement a été inventée au XVI^{e} siècle par Vigenère, et un procédé pour craquer ce code de Vigenère a été mis au point par Charles Babbage au XIX^{e} siècle (il ne publia jamais sa découverte). Ce craquage montre qu'il faut utiliser des suites pseudo-aléatoires plus subtiles que la simple répétition d'un mot.

Les systèmes à flux de clefs appartiennent à la classe des méthodes cryptographiques symétriques : avec une clef de base secrète (qui sert à créer le flux de clefs) l'émetteur code le message original en message crypté et c'est la même clef de base secrète qui en engendrant le même flux de clefs, permet au récepteur du message de décoder le texte secret pour reconstituer le texte original. Dans les méthodes asymétriques (comme le RSA, voir *Pour la Science*, janvier 2000, *La cryptographie RSA vingt ans après*, pages 104-108) une clef, dite publique, sert au codage et une autre, dite privée, sert au décodage.

Avec les méthodes symétriques si l'agent Alice veut communiquer avec