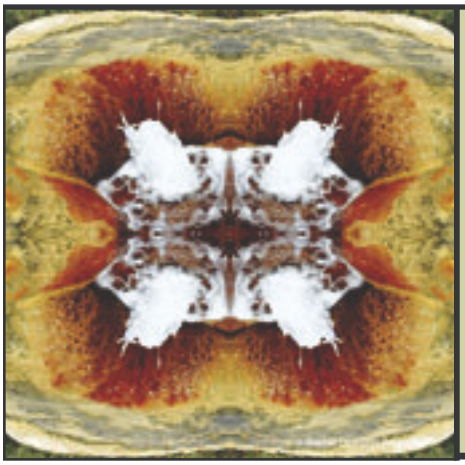


Le Sourcier

revue du Cercle des Sources

numéro 5, juin 2016

Éditorial

Grâce aux talents conjugués et complémentaires de Monique Bornstein (au pinceau et au micro) et de Jacques-Henri Vernier (au piano), notre soirée Jazz du 2 avril a été un succès. Et pourtant, elle avait mal commencé en raison d'une incompatibilité entre l'ordinateur Mac de Monique et notre système de projection. Après de vaines tentatives pour lire le film de Monique, et l'intervention de plusieurs geeks de notre assemblée, notre plus jeune participant, Rémi, a heureusement réussi en un tour de main à régler le problème : nous lui disons un grand merci !

Pour notre prochaine soirée, le 3 juin, nous donnons la vedette à notre Président, Hervé Lehning, normalien, agrégé de Mathématiques, journaliste et écrivain scientifique, auteur de nombreux ouvrages scientifiques et de vulgarisation scientifique.
Hervé nous parlera de « l'Art du secret », autrement dit de la cryptologie, l'art de cacher les messages. Messages amoureux, messages diplomatiques ou messages militaires, cette science existe depuis l'Antiquité et connaît actuellement une explosion historique en raison des impératifs de sécurité sur internet, à l'heure des révélations d'Edward Snowden sur les activités de la NSA. Il nous dédicacera ses derniers livres.

Mais Hervé est également artiste et sait transcender sa vision mathématique du monde dans ses tableaux, ses photographies, ses lampes à la gloire des Mathématiques, avec notamment son « équation du cœur », la cardioïde. C'est donc dans le cadre d'une exposition de ses créations artistiques inspirées par les mathématiques qu'Hervé nous parlera de sa triple passion pour les maths, l'histoire et la cryptologie. Même si vous n'y connaissez rien, et que les maths vous rebutent, n'ayez pas peur : Hervé sait rendre simples et accessibles à tous les notions les plus complexes… le mérite d'une vie consacrée à l'enseignement.

Vendredi 3 juin à partir de 18 h «Soirée secrète»

Conférence et dédicaces d'Hervé Lehning.
Cocktail (gratuit pour les membres du Cercle)
Participation limitée à 45 personnes

Sommaire

Nous vous attendrons ensuite le 13 juillet à partir de 18 h pour notre garden-party et remise des prix du Concours de photo de chats. Parmi les premiers prix : un séjour d'un we à Paris, d'une semaine à Antibes et/ou sur la côte normande et bien sûr des livres. Amoureux des chats : envoyez-nous vite vos photos : le règlement est sur le site. Voir page 3 pour plus de détails.

Les Sources entreront ensuite dans leur période estivale, et la conférence suivante se déroulera le vendredi 16 septembre : «A la découverte du secret des étoiles, quand l 'Astronomie rejoint l 'Espace» par Jean-Pierre Rozelot, Ingénieur INPG, Astronome émérite, université de Nice Sophia Antipolis, Président de Planète Sciences Méditerranée, Membre élu non résident de l'Accademia delle Scienza (Catania,I), Fellow of the Royal Astronomical Society, London (UK). Tous les détails dans le Sourcier n°6 !

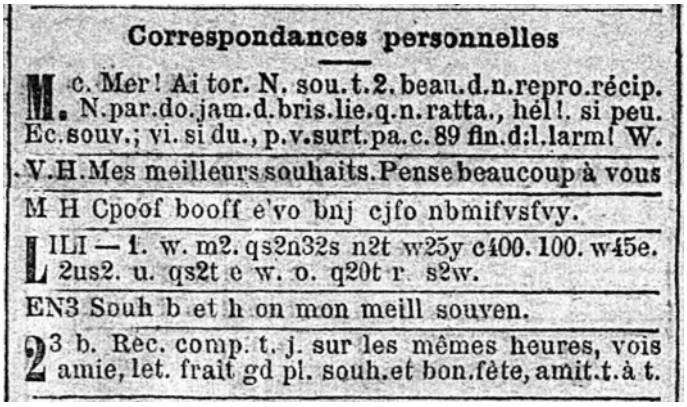
Nouvelles du Cercle

L'Association est constituée, les adhérents ont reçu ou vont recevoir leur justificatif de paiement et nous amorçons à présent une recherche active de sponsors. Rappelons déjà que nous devons toutes nos éditions à Century 21. Nous recherchons maintenant une aide pour nos cocktails et avons engagé des contacts avec des banques. Mais toute idée, suggestion, ou mieux tout contact que vous pourrez nous apporter nous sera précieux. Autre appel au peuple : le Blog. Nous attendons vos articles, papiers ou même « coups de gueule » pour le faire vivre.

DB

La cryptologie, science du secret

À la fin du XIXe siècle, les journaux étaient utilisés pour la communication entre particuliers. Ainsi, voici un extrait de la rubrique « correspondances personnelles » du *Figaro* du premier janvier 1890 :



Correspondances personnelles

M. c. Mer! Ai tor. N. sou.t.2.beau.d.n.repro.récip.
M. N.par.do.jam.d.bris.lie.q.n.ratta., hél!. si peu.
Ec.souv.; vi. si du., p.v.surt.pa.c. 89 fin.d:l.larm! W.
V.H.Mes meilleurs souhaits.Pense beaucoup à vous
M H Cpoof booff e'vo bnj cjfo nbmifvsfvy.
L ILI — 1. w. m2. qs2n32s n2t w25y c400. 100. w45e.
2us2. u. qs2t e w. o. q20t r. s2w.
EN3 Souh b et h on mon meill souven.
2 3 b. Rec. comp. t. j. sur les mêmes heures, vois amie, let. frait gd pl. souh.et bon.fête, amit.t.à t.

Deux messages y sont chiffrés. Le premier (le troisième de le liste) est limpide, il correspond à un décalage d'une lettre et signifie : « bonne année d'un ami bien malheureux ». Le second est un peu plus compliqué à décrypter. Aussi étrange que cela puisse paraître, ces décryptements ont eu un rôle dans l'histoire de la cryptologie. En effet, Étienne Bazeries (1846 – 1931) s'amusait à les lire et, au mess des officiers de sa garnison, régalait ses collègues des histoires scabreuses qu'il lisait sans peine jusqu'au jour où il annonça qu'il pouvait également lire les messages chiffrés de l'armée. Son général prit cette remarque au sérieux et lui demanda de décrypter quelques dépêches du ministère, ce que Bazeries fit sans peine. C'est ainsi qu'il devint l'un des grands cryptologues de l'armée française. L'autre grand nom de la cryptographie de la fin du XIXe siècle est Auguste Kerckhoffs (1835 – 1903) qui fut le premier à énoncer le principe de base de la cryptographie moderne : un système de chiffrement ne doit pas reposer sur son secret mais sur celui d'une clef qu'on change périodiquement.

Comme l'origine de la vocation d'Étienne Bazeries, ce principe a de quoi étonner. Pourtant, la supériorité cryptologique française pendant la Première Guerre mondiale doit beaucoup à ces deux personnages. La suite de l'histoire de la cryptologie n'est pas moins étonnante et mène jusqu'à l'époque actuelle où chaque état a compris l'importance de protéger ses secrets et décrypter ceux des autres. Malheureusement, les États-Unis ont adopté une politique dangereuse pour cela. En effet, selon Edward Snowden, la *National Security Agency* (NSA) pour lire les messages d'autrui a demandé aux fournisseurs de logiciels américains de créer des portes dérobées permettant de contourner leurs algorithmes de chiffrement. Le pire ennui de cette méthode est que, si une porte dérobée existe pour pénétrer dans une citadelle, tout le monde peut la découvrir et l'utiliser. La NSA a ainsi créé une faiblesse dans tous les systèmes de chiffrements qu'elle contrôle, et pourquoi les hackers se priveraient-ils de les utiliser ?

Hervé Lehning nous entretiendra de ces questions aussi bien historiques qu'actuelles au cours de sa conférence du 3 juin 2016.

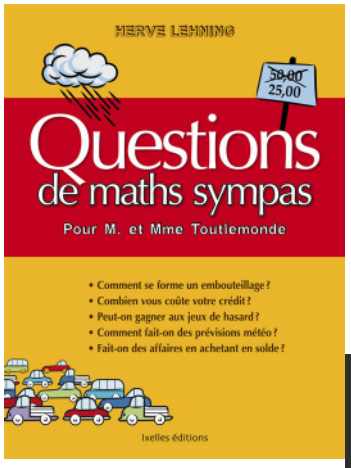
Dédicaces

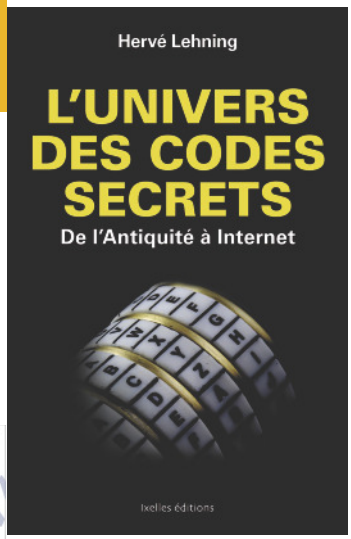
Hervé Lehning dédicacera également ses trois derniers livres, parus chez Ixelles :

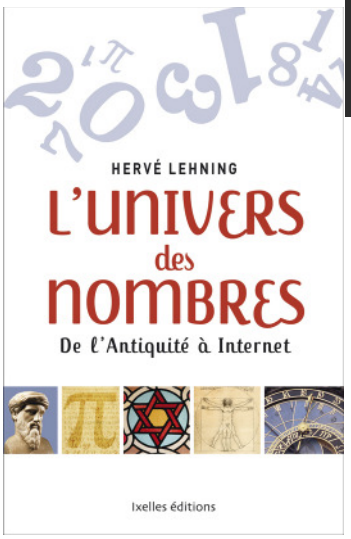
Questions de maths sympas pour M. et Mme Toutlemonde.

L'univers des codes secrets de l'Antiquité à internet.

L'univers des nombres de l'Antiquité à internet.







L'artiste invité : Hervé Lehning

Hervé Lehning nous présentera le même jour ses œuvres inspirées des mathématiques : photographies, toiles, lampes en verre gravé et mugs.

Une grotte en Croatie

1 + 3 + 5

Mugs pythagore

Lampe en hommage à Euler

Des nouvelles du concours photos

Rappelons le thème de notre concours :

Les chats, ces grands félins ... apprivoisés

Peluche, la petite voleuse en gants blancs les nettoie après ses méfaits.

Précisions et le règlement du concours : http://cercledessources.org/concours-de-photos-de-chats/

Envoyez vos photos avant le 20 juin à contact@cercledessources.org.
Remise des prix lors de la garden-party « du 14 juillet » (le 13 au soir à la Villa)

Solutions du «ce n'est pas sorcier» du numéro 4

Trois de suite :

Quel est le plus petit nombre ayant trois diviseurs premiers consécutifs ?

30 (2 x 3 x 5)

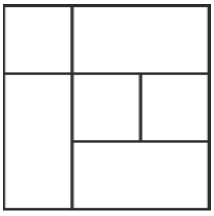
Jeter l'argent par les fenêtres :

Je jette quatre pièces par la fenêtre, quelle est la probabilité que deux tombent sur pile et deux sur face ?

3 / 8

Combien de carrés ?

6



En minutes, s'il vous plaît... :

En minutes, combien vaut 1 / 3,333... heure ?

18 mn

HL

Bitcoin et cryptomonnaies

Les Etats disposent d'une prérogative régalienne de création et de gestion monétaire. La valeur de la monnaie fiduciaire dont ils ont le monopole repose essentiellement sur la confiance que leur accordent les citoyens. Dans un esprit libertaire, ce monopole a été contesté par un groupe d'informaticiens anonymes connu sous le nom de Satoshi Nakamoto qui fut, en 2008, à l'origine du premier projet de monnaie virtuelle destiné à s'affranchir de toute autorité de tutelle : le *bitcoin* (BTC).

En s'appuyant sur Internet, ils ont développé un réseau de transactions numériques ouvert à tous et un concept de confiance partagée entre des utilisateurs anonymes, n'ayant *a priori* aucune raison de se faire confiance et pouvant entrer ou sortir de ce réseau à leur gré. Pour y parvenir, il fallait tout d'abord donner à cette monnaie immatérielle les mêmes propriétés que la monnaie physique : un même bitcoin ne peut être détenu que par une seule personne à la fois et ne peut être dépensé qu'une seule fois par cette dernière. La solution a été de construire un grand livre numérique où sont consignées toutes les transactions regroupées en blocs, appelé *blockchain*. Plusieurs processus cryptologiques sont utilisés pour assurer la signature, l'intégrité des transactions et celle de ce grand livre. Mais il faut aussi que tous les utilisateurs aient confiance dans une telle « cryptomonnaie » autrement dit qu'ils soient tous d'accord pour considérer que le grand livre qui gère et mémorise toutes leurs transactions est bien authentique et non l'œuvre, à partir d'une certaine date, d'une collusion d'autres utilisateurs qui pourraient donc falsifier les comptes et les transactions à leur profit. Pour y parvenir sans qu'il soit nécessaire de faire appel à un tiers de confiance, les concepteurs ont mis au point une procédure de « consensus distribué » qui rend pratiquement impossible la prise de contrôle du réseau Bitcoin par une collusion de moins de 50% des quelques milliers de principaux utilisateurs, ceux en charge de l'élaboration et la vérification des blocs de transactions. Le réseau Bitcoin fonctionne aujourd'hui avec une capitalisation d'environ 6 milliards de dollars et une valeur voisine de $400 pour 1 BTC. Il a déjà été imité par plusieurs centaines d'autres cryptomonnaies. Mais c'est surtout la « blockchain » inventée par bitcoin qui fait école au point que même les plus grandes banques mondiales s'y intéressent de très près ce que n'avait sans doute pas prévu Satoshi Nakamoto!

Joël Lebidois

Le Sourcier est publié par le Cercle des Sources,

Adresse : 6 avenue Bonaparte, 06600 Antibes
Site web : www.Cercledessources.org

Directrice de la publication : Dominique Beudin
Rédacteur en chef : Hervé Lehning

Comité de rédaction :
Edwige Vernocke, Robert Dray, Pierre Morichau.

Contact : contact@Cercledessources.org

Actualités immobilières

Divisé par trois : c'est le montant des intérêts d'emprunt si l'on souscrit un prêt immobilier sur vingt ans aujourd'hui par rapport à 2008.

Même sur une période plus récente, avec les taux de crédit qui ne cessent de reculer, ce coût s'est divisé par un et demi par rapport à 2014.

Cela relance évidemment les nouveaux emprunts, mais aussi… les renégociations !
Selon les estimations de la Banque de France, il resterait 90 milliards d'euros de crédits potentiellement renégociables dans les portefeuilles de prêts des banques, c'est-à-dire un peu plus de 10% de l'encours total des crédits immobiliers en France.

Voici quelques conseils sur le bienfondé d'une renégociation.
Il est intéressant de se pencher sur : - les contrats signés entre 2006 et 2014 - les crédits avec un taux hors assurance supérieur à 3% / 3,20% - les crédits avec un capital restant dû supérieur à 70.000 euros
Et plus généralement, dès que l'on ne compte pas revendre son bien immobilier dans les 2 ans Si vous vous reconnaissez dans ce descriptif, prenez un peu de temps pour faire réétudier votre dossier, car dans ce cas précis :

Temps dépensé = beaucoup d'argent économisé !

Sébastien Butruille, Directeur

Ce n'est pas sorcier...

La famille :

Un homme a sept filles. Chacune de ses filles a un frère. Combien cet homme a-t-il d'enfants ?

La bataille navale :

Une bataille navale se joue sur un carré de 25 cases. Un bateau rectangulaire occupe 3 cases. Quel est le nombre minimum de tirs permettant de toucher le bateau à coup sûr ?

La liste de nombres :

On écrit les nombres de 1 à 100 à la suite les uns des autres. Quel est le chiffre qu'on a écrit le plus souvent ?

Un point commun :

Les mots EXHIBE? CHICHI et CHOIX ont un point commun rare, lequel ?

HL