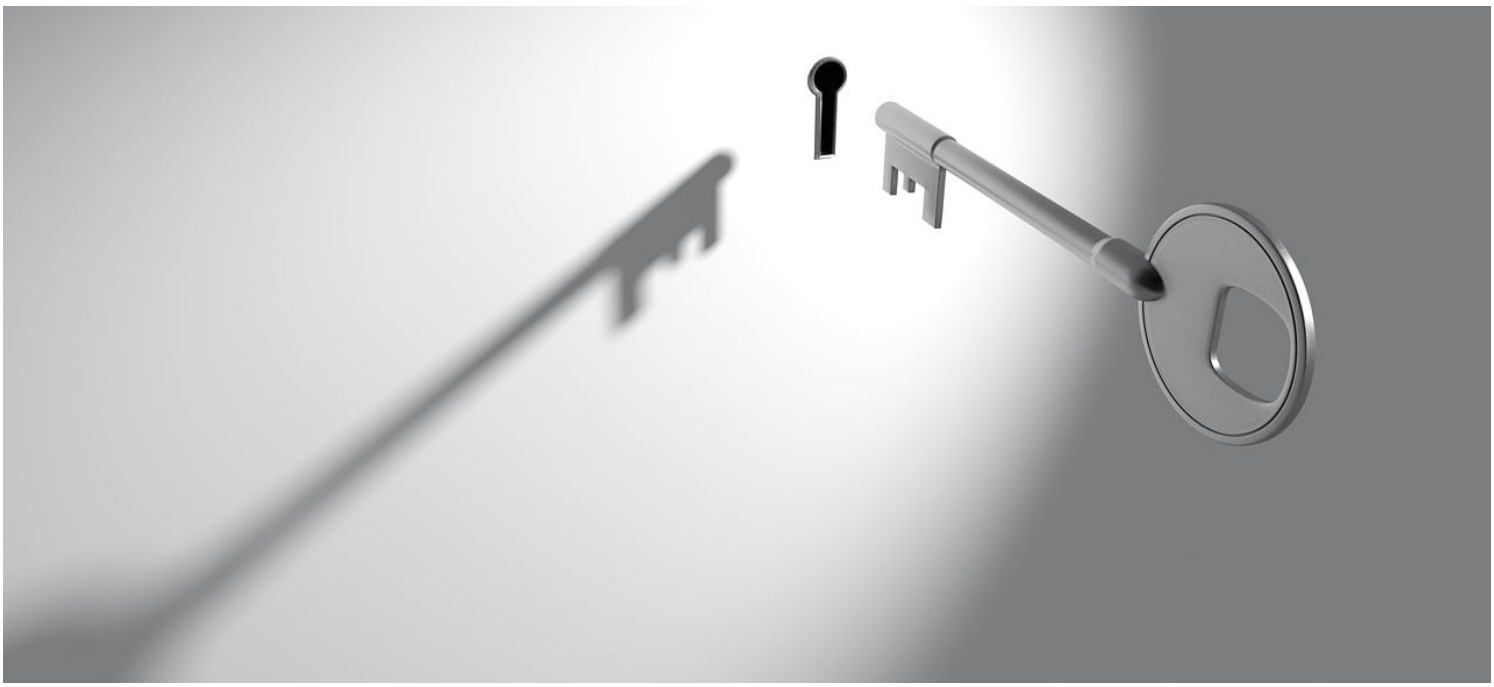
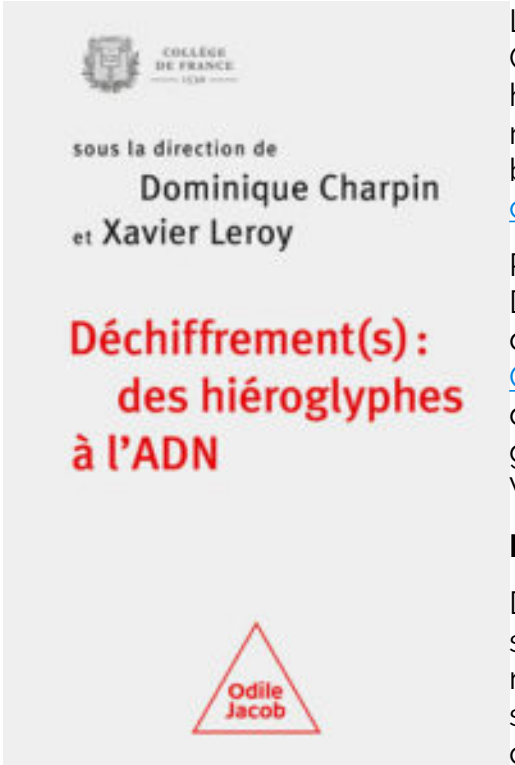
DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

TROUVER UN CHIFFREMENT INDÉCHIFFRABLE

Publié le 27 novembre 2023



par Raphaël Duboisdenghien



"Déchiffrement(s): des hiéroglyphes à l'ADN", par Dominique Charpin et Xavier

Le 22 septembre 1822, le jeune égyptologue Jean-François Champollion explique comment il a percé le mystère des hiéroglyphes égyptiens au secrétaire perpétuel de l'Académie royale des inscriptions et belles-lettres à Paris. Pour célébrer le bicentenaire de cet événement, le Collège de France l'a choisi comme thème de son colloque de rentrée 2022-2023.

Professeurs à l'établissement d'enseignement et de recherche, Dominique Charpin et Xavier Leroy prolongent cette rencontre dans «Déchiffrement(s): des hiéroglyphes à l'ADN» aux éditions Odile Jacob. Avec dix spécialistes du déchiffrement. Notamment d'écritures anciennes, des sciences de l'Univers, du code génétique, des informations chiffrées, des 34 tableaux du peintre Vermeer de Delft.

Le travail sur le terrain

Dominique Charpin étudie les civilisations mésopotamiennes et ses langues, le sumérien et l'akkadien. «Les difficultés du travail ne manquent pas», raconte le conférencier au Collège Belgique, spécialiste de l'écriture cunéiforme dont les signes en forme de clous et de coins étaient employés en Mésopotamie.

Ces difficultés sont dues à la nature des textes découverts. «Certes, les supports de l'écriture cunéiforme sont très nombreux.

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

Leroy. Editions Odile Jacob. VP 27,90 euros, VN 22,99 euros

Mais la majorité des écrits se trouvent sur des tablettes d'argile, dont la détection et le traitement sont loin d'être aisés. Une situation plus privilégiée est constituée par les tablettes stockées dans des récipients en céramique. Mais ce cas de figure n'est pas le plus fréquent.»

«L'observation du contexte est très importante, car elle permet de déterminer le statut qui était celui des textes au moment de la destruction de la couche archéologique dans laquelle ils se trouvent». C'est une fois les tablettes enlevées de leur contexte que commence le travail de déchiffrement proprement dit. Le degré de difficulté de ce travail dépend de l'état dans lequel se trouvent les tablettes. Après le nettoyage, avec de l'entraînement, un original bien conservé peut se lire en peu de temps. Mais le même texte, s'il est lacunaire, peut exiger des heures de travail.»

Impossible de savoir si l'on peut faire confiance

Spécialiste du chiffrage des messages, Anne Canteaut s'intéresse à la conception de nouveaux algorithmes pour protéger la confidentialité des données. Et la sécurité des systèmes existants.

«Dans ce monde bipolaire, les utilisateurs légitimes doivent, contrairement aux adversaires, pouvoir accéder à l'information qui a été chiffrée», dit la directrice de recherche à l'Institut français de recherche en sciences et technologies du numérique (Inria). «Trouver un chiffrement mathématiquement indéchiffrable est chose mathématiquement possible. Mais matériellement impossible.»

Tous les chiffrements utilisés peuvent, en théorie, être décryptés... «Sans un investissement important et durable de la communauté académique dans les disciplines algorithmiques, informatiques et mathématiques, il est impossible de savoir si l'on peut faire confiance à nos systèmes de chiffrement. En cryptographie comme dans bien des domaines, la confiance ne se décrète pas.»

Apprendre à lire les signes

«Notre société a perdu beaucoup de sa compétence dans l'interprétation des signes et, pour tout dire, dans le statut de ce qu'est un signe», note la philologue et linguiste Emmanuelle Damblon, professeure à l'Université libre de Bruxelles. «Or, le succès actuel des théories du complot peut s'entendre comme un retour à l'antique usage de l'interprétation des signes sur un mode dégradé.»

Pour la membre de la Classe des lettres de l'Académie royale de Belgique, «l'interprétation des indices à l'œuvre n'est pas le fait d'une erreur, d'un mensonge ou d'une manipulation. Mais bien le témoin d'un besoin inassouvi de pratiquer l'activité interprétative. Il ne s'agit pas de reconnaître une validité dans les théories complotistes. Il s'agit de comprendre qu'elles font appel à des qualités intellectuelles utiles mais largement disqualifiées.»

L'enseignement, a-t-il un rôle à jouer? «Peut-être nos méthodes d'éducation devraient-elles remettre à l'honneur les nombreuses formations qui apprennent à lire les signes qui ne trompent pas afin que cette exigence de rationalité, aujourd'hui largement inassouvie, ne soit pas récupérée par des acteurs de la « complosphère » qui s'improvisent tour à tour prophètes, devins, guérisseurs, philologues ou simplement enquêteurs du réel.»