Dictée du lycée A.Kastler – Jeudi 23 mars 2017.

Comment sécuriser les cartes bancaires, les communications, le vote électronique ? La cryptologie est, comme l'indique l'étymologie du mot, la science du secret. Aujourd'hui, elle ne se restreint plus au simple chiffrement des messages pour en garantir la confidentialité. Elle s'attache aussi à permettre l'authentification des diverses entités qui communiquent à distance dans un monde virtuel, à autoriser la signature de documents numériques immatériels, à garantir l'intégralité des données dans des réseaux ouverts, à protéger l'anonymat des données personnelles sensibles, à contribuer à la protection des contenus. Elle emprunte ses méthodes à des domaines scientifiques divers, mathématiques et informatique en premier lieu, mais également physique, notamment quantique. Elle n'est plus l'apanage des diplomates et des militaires : aujourd'hui, des centaines de millions d'individus à travers le monde, ont en permanence sur eux un ou plusieurs processeurs cryptographiques, pour leur téléphone cellulaire ou leur carte bancaire en particulier. En ce sens, on peut parler d'ubiquité de la cryptologie.

Jacques Stern, professeur d'informatique à l'École normale supérieure.