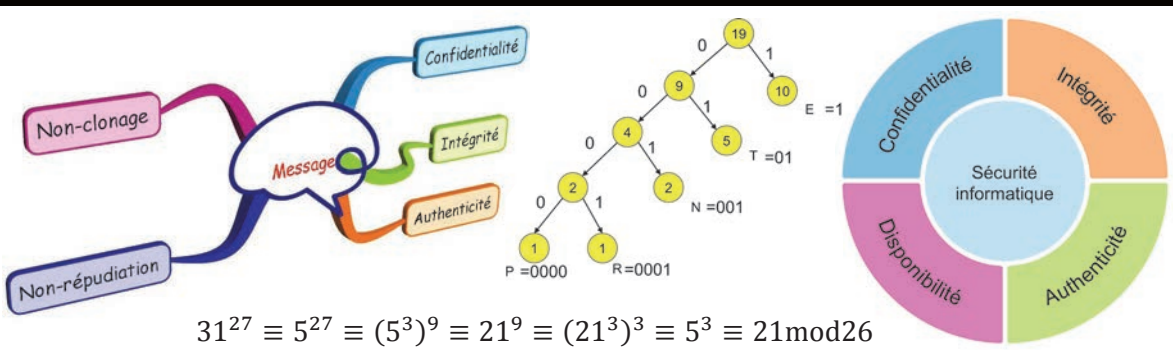


$$31^{27} \equiv 5^{27} \equiv (5^3)^9 \equiv 21^9 \equiv (21^3)^3 \equiv 5^3 \equiv 21 \bmod 26$$

Quintesciences

Énergie, entropie, information, cryptographie et cybersécurité

Christian Ngô

edp sciences

Énergie, entropie, information, cryptographie et cybersécurité

Avec 115 exercices corrigés

Énergie, entropie, information, cryptographie et cybersécurité

Avec 115 exercices corrigés

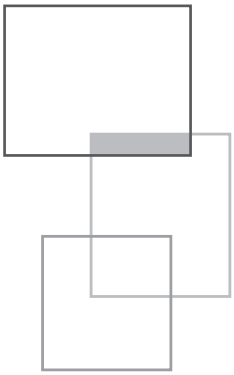
Christian NGÔ

edp sciences

Imprimé en France

ISBN (papier) : 978-2-7598-2333-8 – ISBN (ebook) : 978-2-7598-2349-9

Table des matières



Introduction

Ce livre est en partie basé sur un cours dispensé en L2 à l'EFREI intitulé « énergie, entropie et information ». Il explicite également deux sujets qui avaient été effleurés dans ce cours : la cryptologie et la cybersécurité.

Il peut sembler étrange de regrouper des sujets qui paraissent à première vue très différents. Ils ont en fait un point commun : l'entropie et ce qui lui est attaché, la notion d'ordre et de désordre ainsi que la notion d'irréversibilité. L'entropie est en effet une mesure du désordre d'un système. Ce concept est largement utilisé dans le domaine de l'énergie et dans les sciences plus fondamentales comme la thermodynamique ou la physique statistique. L'entropie est aussi une notion utilisée en théorie de l'information, un domaine développé initialement par Shannon, dont les idées ont révolutionné ce domaine. L'information contenue dans un message peut être ainsi quantifiée en termes d'entropie de l'information dont la forme mathématique est très proche de l'entropie thermodynamique ou de l'entropie statistique.

Envoyer un message, c'est d'abord le comprimer au maximum pour qu'il puisse être transmis de manière efficace par les moyens de communication. C'est aussi lui ajouter de l'information permettant de détecter et corriger les erreurs qui se produisent toujours lors de son transfert de l'émetteur vers le destinataire. Enfin, un message est la plupart du temps confidentiel et doit être crypté pour que des personnes indiscrètes n'interceptent pas son contenu.

L'utilisation de moyens électroniques pour véhiculer l'information est un réel progrès par rapport aux moyens classiques utilisés dans le passé. Cependant, ces vecteurs de communication ont des faiblesses que ne manquent pas d'utiliser des personnes mal intentionnées pour voler des données, les corrompre ou pour empêcher qu'elles arrivent à bon port. La cybercriminalité est un domaine en pleine expansion où le défenseur a

toujours un coup de retard sur l'attaquant. Ce domaine étant important, nous donnons quelques notions élémentaires de cybersécurité dans un dernier chapitre.

Cet ouvrage n'a pas d'autre ambition que d'être une introduction aux différents sujets cités dans son titre. Ce n'est donc pas un livre pour spécialistes, mais un ouvrage pour acquérir des notions élémentaires dans tous ces domaines. Il doit être complété, pour les lecteurs qui le souhaiteront, par des ouvrages plus approfondis dont certains sont cités à la fin de chaque chapitre et qui contiennent aussi de nombreuses références.

L'ouvrage est divisé en onze chapitres.

Le chapitre 1 introduit la notion d'énergie. Sans énergie, il n'y a ni vie ni activité économique. L'énergie intervient dans tout processus physique, chimique ou biologique dans lequel il se produit un changement. Ce sont les transformations d'une forme d'énergie vers une autre qui sont intéressantes pour l'utilisateur, comme transformer la chaleur émise lors de la combustion du gaz naturel en électricité. Même avec les meilleures technologies, le rendement est limité par le second principe de la thermodynamique, c'est-à-dire par le sens de l'évolution de l'entropie.

Le chapitre 2 est une courte introduction à la thermodynamique. Cette science, née au XIX^{e} siècle, avait notamment pour but de comprendre et d'améliorer le rendement des machines à vapeur qui ont permis le démarrage de la révolution industrielle. La notion d'entropie a peu à peu émergée pour expliquer les limites observées lors de la conversion de chaleur en travail.

Le chapitre 3 rappelle quelques notions de mécanique quantique. Au niveau microscopique, c'est-à-dire à l'échelle des atomes des molécules ou des noyaux, la mécanique classique est incapable de décrire certains phénomènes et n'est plus applicable. Certaines propriétés quantiques vont à l'encontre de notre intuition qui s'est construite à partir de l'observation d'un monde classique. Ces propriétés quantiques gouvernent un grand nombre de propriétés utilisées dans les technologies utilisées dans la vie de tous les jours.

Le chapitre 4 introduit la physique statistique qui permet de comprendre la thermodynamique à partir des phénomènes microscopiques. Elle va même au-delà en permettant de décrire de nombreux phénomènes macroscopiques mettant en jeu un grand nombre de particules et notamment les systèmes à l'équilibre sous contraintes. L'équilibre statistique est obtenu lorsque l'entropie est maximale, c'est-à-dire lorsque l'information connue sur le système est minimale.

Le chapitre 5 est un rappel sur les probabilités. C'est une branche des mathématiques très utilisée, que ce soit en physique statistique ou en théorie de l'information.

Le chapitre 6 définit l'information de manière quantitative et introduit l'entropie d'information. Ce sont les notions de base de la théorie de l'information qui a été initiée pour une bonne part par Shannon.

Le chapitre 7 donne le cadre général d'un transfert d'information entre un émetteur et un destinataire. Il présente les principaux problèmes auxquels on est confronté pour réaliser cette tâche.

Le chapitre 8 s'intéresse au codage source, c'est-à-dire à la manière dont l'émetteur va préparer les messages avant de les transmettre dans les canaux d'information. L'objectif est d'avoir des messages aussi compacts que possible, car les « tuyaux » d'information ne peuvent pas tout accepter, de même qu'une canalisation d'eau a un débit maximum.

Le chapitre 9 traite du codage canal. Il s'agit de tenir compte des erreurs qui se produisent inévitablement lors des transferts d'information. Il faut pouvoir identifier les erreurs et éventuellement les corriger.

La cryptographie est un élément essentiel pour transmettre des messages confidentiels. On crypte un message pour qu'il ne soit pas lu par un tiers. Le chapitre 11 donne une introduction sur la cryptologie qui comprend à la fois la cryptographie et la cryptanalyse. La cryptographie consiste à chiffrer un message avant de le transmettre à son destinataire afin que son contenu reste confidentiel. La fonction de déchiffrement doit être rapide si l'on possède la clef et extrêmement difficile si on ne la possède pas. La cryptanalyse consiste à essayer de déchiffrer un message dont on n'a pas la clef. Elle peut avoir un but malveillant, mais sert aussi à tester la vulnérabilité du chiffrement.

Le monde moderne repose maintenant beaucoup sur les transferts d'information et le stockage de données. Le contenu du trafic et les données stockées ont de la valeur et attirent des personnes malveillantes. D'autres attaques visent à perturber ou détruire certaines des infrastructures (logicielles ou matérielles) d'une entreprise. Ainsi, environ 30 % des sociétés françaises subissent une attaque informatique chaque année. Certaines de ces attaques conduisent à des pertes importantes pour la société attaquée, pouvant aller jusqu'à la disparition de celle-ci. C'est l'objet du chapitre 11.

Chacun des chapitres de ce livre peut être abordé indépendamment, sauf les chapitres 8 et 9 qu'il est préférable de lire dans cet ordre.

La particularité de cet ouvrage est qu'il comprend aussi 115 exercices (chapitre 12) sur les différents chapitres abordés. Ceux-ci sont intégralement corrigés (chapitre 13) et permettent de tester et de compléter les connaissances acquises de chacun des chapitres. Quelques exercices portant sur des compléments de mathématiques sont aussi proposés ainsi que des exemples de programmation en langage Python (chapitre 14).

1

L'énergie

L'énergie est une notion complexe à appréhender. Elle se présente, pour nos usages, sous de multiples formes. Ce chapitre donne quelques notions sur ce sujet.

1.1 Les multiples facettes de l'énergie

L'énergie est nécessaire à la vie et au développement économique. C'est une notion difficile à définir, car elle recouvre de multiples aspects. Pour le physicien théoricien, l'énergie est la quantité qui se conserve par suite de l'existence d'une symétrie particulière de l'espace et du temps.

Dans l'univers, il y a de l'**énergie** et de la **matière**. L'énergie E et la masse m d'une particule de masse sont reliées par la relation d'Einstein :

$$E = mc^2$$

Où c est la vitesse de la lumière. Cette relation exprime le fait qu'il y a équivalence entre énergie et masse. De l'énergie peut se transformer en matière et réciproquement. Par exemple, un photon γ (énergie) de 1,022 MeV peut créer, lors d'une interaction avec la matière, un électron e^- (matière) et un positon e^+ (antimatière). Cette transformation est utilisée dans les détecteurs de photons de haute énergie, mais aussi dans les détecteurs de rayonnement gamma utilisés dans le domaine du médical. De même, un positon e^+ peut s'annihiler avec un électron e^- pour donner deux photons γ. C'est le principe de la tomographie par émission de positons utilisé en imagerie médicale.

Pour satisfaire nos besoins énergétiques, ce n'est pas tant l'énergie elle-même qui nous intéresse, mais ses transformations d'une forme vers une autre, car elles vont permettre d'en récupérer une partie pour satisfaire nos besoins (travail ou chaleur).

La nourriture nous fournit de l'énergie pour vivre, mais nous n'allons pas nous intéresser à cette forme d'énergie ici. Nous allons plutôt considérer d'autres formes d'énergie comme le pétrole, qui permet d'obtenir de l'essence ou du gazole pour propulser les véhicules ou l'électricité qui est nécessaire au fonctionnement de nombreux dispositifs domestiques (réfrigérateur, télévision, lampes, convecteurs, etc.).

1.2 Symétrie et conservation de l'énergie

Le **théorème de Noether**, publié en 1918 par la mathématicienne allemande Emmy Noether, dit, en termes simples, que chaque fois qu'il existe une **invariance des lois physiques** lors de certaines transformations (ce que l'on désigne habituellement sous le nom de **symétries**), il existe une **loi de conservation**.

Il y a invariance des lois physiques par translation dans le temps (elles restent les mêmes au cours du temps). On dit que le **temps est uniforme,** ce qui signifie que si l'on réalise une expérience aujourd'hui et qu'on la reproduit dans 1 an dans les mêmes conditions, on trouvera le même résultat. La conséquence de l'uniformité du temps est qu'il existe une quantité, appelée **énergie**, qui est conservée pour un système isolé, c'est-à-dire sans interaction avec le milieu extérieur.

Cette définition de l'énergie nous dit que c'est une quantité conservée pour un système isolé, mais elle ne nous renseigne en rien quant aux formes d'énergie qui sont utiles pour satisfaire les besoins de l'espèce humaine. Or, ce qui nous intéresse dans la vie courante, ce sont les différentes **formes d'énergie** et les **transformations** d'une forme d'énergie vers une autre. Les formes qui sont en particulier intéressantes pour nos besoins sont la **chaleur** et le **travail**. En brûlant du bois, on va par exemple produire de la chaleur permettant de se chauffer. En utilisant de l'essence dans une voiture, on va transformer une partie de son énergie de combustion en travail pour propulser le véhicule.

L'espace est aussi **homogène, isotrope**.

L'homogénéité de l'espace signifie qu'il est invariant par translation. Cette invariance exprime le fait qu'une translation d'un dispositif expérimental, par exemple de Paris à Marseille, ne change pas les résultats. Cette invariance par translation se traduit par la **conservation de l'impulsion** d'un système mécanique isolé.

L'isotropie de l'espace signifie qu'il est invariant par rotation. La rotation d'un dispositif expérimental ne change pas les résultats. Cette propriété conduit à la **conservation du moment cinétique** d'un système isolé.

L'homogénéité de l'espace, son isotropie et l'uniformité du temps conduisent aux lois de conservation de la figure 1.1.

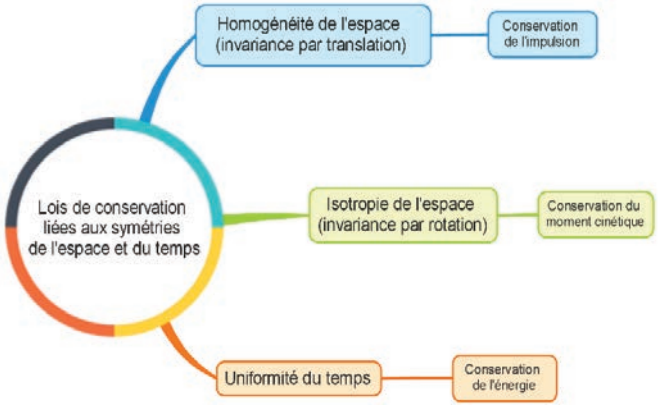


Figure 1.1

1.3 Les différentes formes de l'énergie

L'énergie peut se présenter sous différentes formes. Certaines sont indiquées dans la figure 1.2. L'homme a besoin d'énergie pour fournir du travail, pour produire de la chaleur afin de chauffer les lieux où il vit ou travaille, pour fabriquer du froid pour climatiser ses locaux lorsqu'il fait trop chaud, etc. Il obtient la forme d'énergie dont il a besoin par transformation d'une forme énergétique vers une autre. Chaque transformation a un rendement qui est plus ou moins bon. On peut par exemple produire de l'électricité dans une centrale à charbon en brûlant ce dernier. La combustion est une réaction chimique. Le rendement de production de l'électricité varie typiquement entre 30 et 40 % selon la technologie utilisée. Cette électricité peut

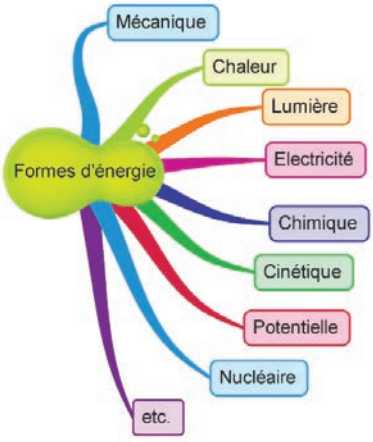


Figure 1.2

alimenter un moteur électrique que l'on va par exemple utiliser pour faire tourner le tambour d'une machine à laver. Le rendement entre l'électricité et le travail mécanique fourni par le moteur est très bon, proche de 100 %.

L'énergie intervient dans tout processus physique, chimique ou biologique qui se traduit par un changement. De l'énergie peut ainsi être absorbée ou libérée lors du processus.

1.4 La consommation d'énergie

Au niveau mondial, la consommation d'énergie augmente régulièrement.

- D'une part parce que la population mondiale augmente. Il y a chaque jour environ 200 000 nouveaux habitants sur la Terre. Ce sont de nouveaux consommateurs d'énergie. La figure 1.3 montre l'évolution de la population mondiale lors du dernier millénaire. On remarque que la croissance de la population mondiale a été très rapide depuis le début de la révolution industrielle, il y a un peu plus de deux siècles. Les dates indiquées correspondent au passage d'un nouveau milliard d'habitants. Le premier milliard a été atteint en 1804. En 2011, on a atteint 7 milliards d'habitants.
- D'autre part parce que le niveau de vie des populations des pays émergents ou en développement augmente régulièrement, ce qui a pour conséquence d'augmenter la consommation d'énergie au niveau de la planète.

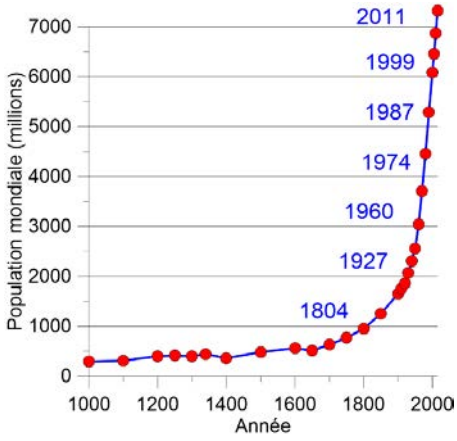


Figure 1.3

Pour évaluer les quantités d'énergie produites ou consommées, les économistes utilisent la notion **d'énergie** primaire. Il s'agit de l'énergie contenue dans une source énergétique avant toute transformation. C'est, par exemple, le cas du pétrole brut,

T

U

V

W

Z

Quintesciences

Énergie, entropie, information, cryptographie et cybersécurité

Christian Ngô

L'énergie et l'information jouent un rôle important dans les sociétés modernes. Ces deux domaines ont un point commun : l'entropie. Celle-ci est reliée à l'irréversibilité des transformations énergétiques et permet de quantifier l'information pour mieux la traiter.
La thermodynamique permet de comprendre les échanges de travail et de chaleur à l'échelle macroscopique. La physique statistique et la mécanique quantique en donnent une compréhension microscopique. Énergie, thermodynamique, physique statistique et mécanique quantique sont introduits à un niveau élémentaire.
L'information occupe une place de plus en plus importante dans les sociétés modernes. Un message doit pouvoir être transmis rapidement, en toute sécurité, sans modification et en toute confidentialité. Ceci nécessite d'évaluer la quantité d'information qu'il contient pour coder celle-ci afin qu'il occupe le moins de place possible avant de le transmettre. Il faut être capable de détecter et corriger les erreurs toujours présentes lors de sa transmission et en assurer sa confidentialité (cryptographie). Ces points sont abordés dans plusieurs chapitres de cet ouvrage qui se termine par des notions de cybersécurité car outre les erreurs accidentelles existant lors de la transmission d'un message, il existe de plus en plus d'actions malveillantes visant à l'intercepter, le détruire, le modifier ou en prendre connaissance.
Plus d'une centaine d'exercices avec un corrigé détaillé complètent l'ouvrage et permettent au lecteur de vérifier ses connaissances ou de les compléter.

***Christian Ngô** a publié plus d'une douzaine d'ouvrages, seul ou en collaboration avec un autre auteur, sur plusieurs sujets allant de la physique de base (physique statistique, mécanique quantique, physique nucléaire, physique des semi-conducteurs) à des domaines plus appliqués comme l'énergie, les nanotechnologies, les déchets et la pollution, le soleil, etc. Il a fait de la recherche fondamentale pendant une vingtaine d'années avant de s'orienter vers la recherche appliquée où il a occupé plusieurs postes de responsabilité. Il dirige actuellement la société EDMONIUM.*

978-2-7598-2333-8

edp sciences
www.edpsciences.org

La collection QuinteSciences s'adresse à un public spécialisé. Elle propose des ouvrages de référence, écrits par des experts reconnus dans leur domaine et aborde, de manière approfondie, un sujet scientifique. QuinteSciences contribue ainsi à la diffusion des savoirs fondamentaux.