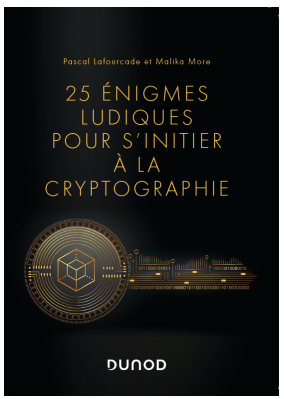
Nuit de la lecture

Les Maths en Scène

Pascal Lafourcade

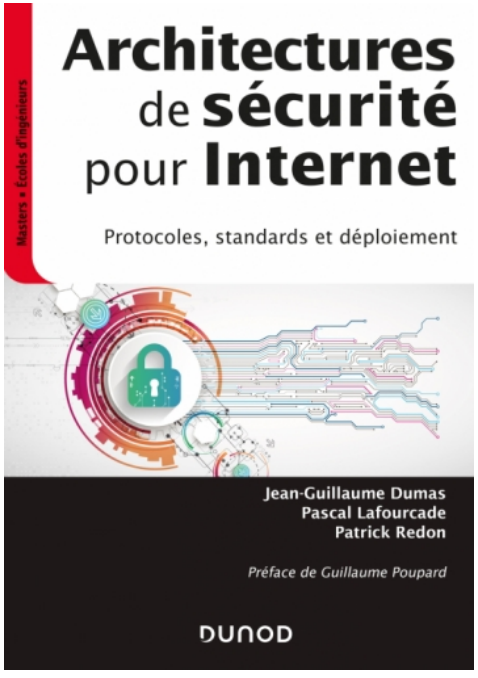


LIMOS

UNIVERSITÉ Clermont Auvergne

Janvier 2023

Extrait : Préface de Guillaume Poupard



2014 - 2022

Énigme 1 : Un message dans le texte ☆

"The best books [...] are those that tell you what you know already."

"Les meilleurs livres [...] sont ceux qui racontent ce que l'on sait déjà."

Georges Orwell, "1984", 1949.

Énigme 2 : Les secrets de Jules ☆

"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major government from reading your files."

"Il y a deux sortes de cryptographies dans le monde : la cryptographie qui empêche votre petite sœur de lire vos fichiers, et la cryptographie qui empêche le Gouvernement de lire vos fichiers."

Bruce Schneier, "Applied Cryptography", 1986.

Énigme 3 : Une image mystérieuse ☆☆☆

“Ars ipsi secreta magistro.”

“Un art caché au maître lui-même.”

Jean Robert du Carlet, thèse publiée en 1644.

Énigme 4 : Un chiffrement presque allemand ☆☆

"German codes are a puzzle. A game, just like any other game."

"Les codes allemands sont comme des énigmes. Un jeu, comme n'importe quel autre jeu."

Le personnage d'Alan Turing, dans le film "Imitation Game", 2014.

Énigme 5 : Un méli-mélo de caractères ☆

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

"Si vous pensez que la technologie peut résoudre vos problèmes de sécurité alors vous n'avez rien compris aux problèmes ni à la technologie."

Bruce Schneier, "Secrets & Lies, Digital Security in a Networked World", 1985.

Énigme 6 : Vous avez dit sûr, ... sûr ☆☆

"Fully secure systems don't exist today and they won't exist in the future."

"Les systèmes parfaitement sûrs n'existent pas aujourd'hui et ils n'existeront pas dans le futur."

Adi Shamir, RSA Conference, 2015.

Énigme 7 : Une modification invisible ☆

“Le vaincu de son cœur.”

Victor Hugo, “Les Quatre Vents de l’esprit”, 1881.

Énigme 8 : Chiffrer deux fois n'est pas deux fois plus sûr

☆☆

"Without strong encryption, you will be spied on systematically by lots of people."

"Sans chiffrement fort, vous serez espionné systématiquement par de nombreuses personnes."

Whitfield Diffie, *The Buffalo News*, 2 février 1999.

Énigme 9 : Le protocole de Diffie-Hellman pour établir une clé ☆☆

"A very small percentage of the population produces the greatest proportion of the important ideas."

"Un très petit pourcentage de la population produit la plus grande proportion des idées importantes."

Claude Shannon, discours "Creative Thinking" à Bell Labs, le 20 mars 1952.

Énigme 10 : Le partage de Shamir ☆☆☆

"Collaboration always wins over competition anytime. And on top of it, it's much more fun. Don't ever believe that research is a zero-sum game. Collaborate as much as you can!"

"La collaboration l'emporte toujours sur la compétition, à tout moment. Et en plus, c'est beaucoup plus amusant. Ne croyez jamais que la recherche est un jeu à somme nulle. Collaborez autant que vous le pouvez !"

Silvio Micali, "Proof, according to Silvio", discours pour le Prix Turing.

Énigme 11 : Un regroupement de nombres ☆☆☆

"Security is a process, not a product."

"La sécurité n'est pas un produit, mais un processus."

Bruce Schneier, "Crypto-Gram", 15 mai 2000.

Énigme 12 : Des chiffrés mélangés ☆

“Only the Paranoid Survive.”

“Seuls les paranoïaques survivent.”

Andy Grove, Cofondateur d’Intel en 1968,
titre de son autobiographie, publiée en 1998.

Énigme 13 : Prouver sans dévoiler ☆☆☆

"It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics."

"C'est insuffisant de nous protéger avec des lois, nous avons besoin de nous protéger avec les mathématiques."

Bruce Schneier, *Applied Cryptography*, seconde édition, 1987.

Énigme 14 : Le mythe de l'antivirus ☆☆☆☆

"Timeo Danaos et dona ferentes."

"Je crains les Grecs, même dans leurs présents.".

Virgile, *L'Énéide* (Livre II, 49), 29 avant J.-C.

Énigme 15 : Désassembler une fonction de hachage ☆☆

"Once you have something on the Internet, you are telling the world, please come hack me."

"Une fois que quelque chose est sur Internet, vous dites au monde entier, s'il vous plaît venez m'attaquer."

Ronald Rivest, le 16 août 2016 sur Fox News.

Énigme 16 : Des images qui en cachent d'autres ☆☆

"L'indifférence dissout le langage, brouille les signes."

Georges Perec, "Un homme qui dort", 1967.

Énigme 17 : L'homme du milieu ☆☆☆

"If you ask amateurs to act as front-line security personnel, you shouldn't be surprised when you get amateur security."

"Si vous demandez à des amateurs d'agir en tant que personnel de sécurité de premier plan, vous ne devez pas être surpris d'obtenir une sécurité d'amateur."

Bruce Schneier, *How We Won the War on Thai Chili Sauce*, 1er novembre 2007.

Énigme 18 : La consommation électrique en dit trop

☆☆☆

“ Crypto will not be broken, it will be bypassed.”

“La crypto ne sera pas cassée, elle sera contournée.”

Adi Shamir, RSA Conference 2015.

Énigme 19 : Le digicode lumineux ☆☆

"We've really screwed up. There's been this desire from the industry to be as fast as possible and secure at the same time. Spectre shows that you cannot have both."

"Nous avons vraiment foiré. Il y a eu ce désir de l'industrie d'être aussi rapide que possible et sûre en même temps. Spectre montre qu'on ne peut pas avoir les deux."

Paul Kocher, *New York Times*, 4 janvier 2018.

Énigme 20 : Des couples clairs chiffrés ☆☆☆

"Somebody will be able to overcome any encryption technique you use!"

"Quelqu'un sera toujours capable de dépasser la technique de chiffrement que vous utilisez!"

Noam Chomsky, *The Guardian*, 17 Octobre 2012.

Énigme 21 : Un chiffrement malléable ☆☆

"La cryptologie, c'est le moteur de l'Internet. Aujourd'hui, plus personne ne regarde sous le capot de sa voiture."

Jacques Stern, cryptographe, médaille d'or du CNRS, *L'Express*, 20 novembre 2006.

Énigme 22 : Payer en bitcoins ☆☆☆

"The crypto currency community hasn't decided whether they want to be anarchist rebels or to replace the establishment."

"La communauté des cryptomonnaies n'a pas décidé s'ils veulent être des rebelles anarchistes ou remplacer l'ordre établi."

Adi Shamir, RSA Conference, 2015.

Énigme 23 : La solidité d'un mot de passe ☆☆

" If someone steals your password, you can change it. But if someone steals your thumbprint, you can't get a new thumb. The failure modes are very different."

"Si quelqu'un vous vole votre mot de passe, vous pouvez le changer. Mais si quelqu'un vole votre empreinte de pouce, vous ne pouvez pas obtenir un nouveau pouce. Les modes de défaillance sont très différents.".

Bruce Schneier, *NewYork Times*, 28 décembre 2013.

Énigme 24 : Un vote naïf ☆☆

"Your rights matter, because you never know when you're going to need them."

"Vos droits sont importants, car vous ne savez jamais quand vous en aurez besoin."

Edward Snowden, "We don't have to give up liberty to have security", exposé à TED en visio, 18 mars 2014.

Énigme 25 : Des indices qui deviennent compromettants

☆☆

"People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems."

"Les gens représentent souvent le maillon faible de la chaîne de sécurité et sont régulièrement responsables des échecs des systèmes de sécurité."

Bruce Schneier,
Secrets and Lies: Digital Security in a Networked World, chapitre 17 *The Human Factor*, 15ème anniversaire, édition 2015.

Merci pout votre attention

Questions?