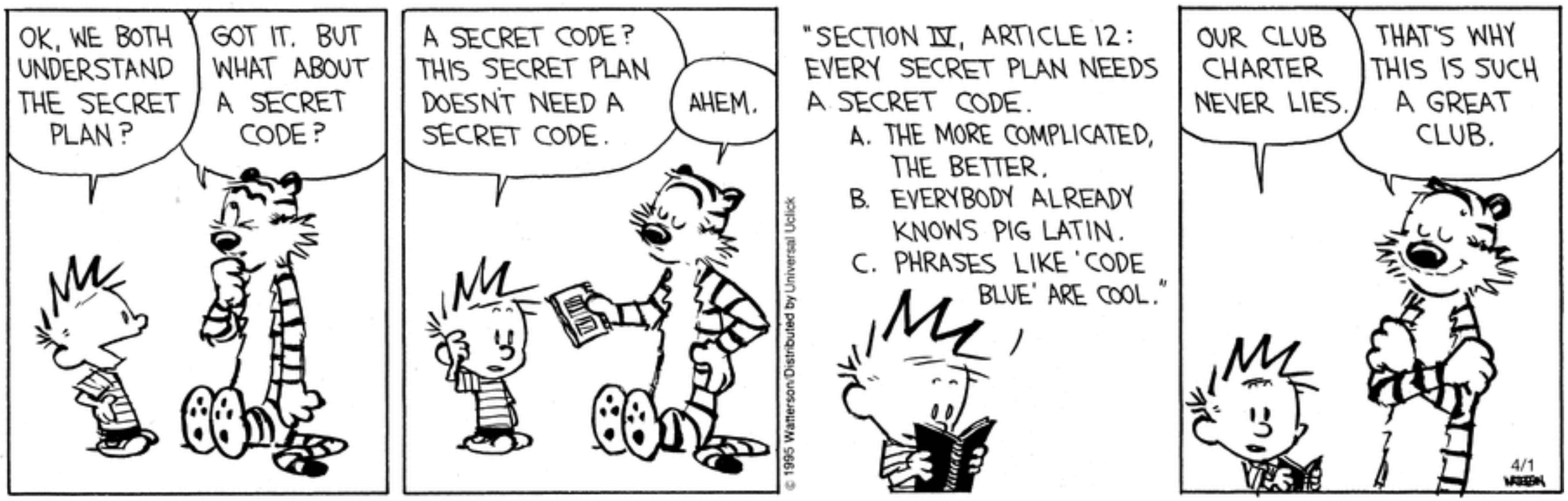
Introduction to Cryptology

Pierre Karpman: https://membres-ljk.imag.fr/Pierre.Karpman/
Bruno Grenet: https://membres-ljk.imag.fr/Bruno.Grenet/

- Cryptology: how to communicate in the presence of adversaries

- Goal of this course: Introduction to the main objects & concepts of cryptography



Content of the course

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

- Maths background (modular arithmetic, discrete probabilities, finite groups…)
- Presentation of symmetric-key cryptosystems (block ciphers, sym. encryption schemes, hash functions, MACs…)
- Some examples of public-key cryptosystems (discrete logarithm-based key exchange, signatures)
- Overview of a few applications & real-life attacks

What this course is <u>not</u> about

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

- Vulgarisation or “historical” cryptography
- How to use cryptography as a black box
- Cryptographic protocols (TLS, SSH…)
- Advanced functionalities (FHE, MPC, SNARKs…)

What this course is about

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

- Definitions

- Definitions

- Definitions

Definitions are everything

hhttps://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

A typical definition

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

$\mathbf{Adv}^{\mathrm{PRP}}$

$$\mathbf{Adv}^{\mathrm{PRP}}_{\mathcal{E}}(q,t) =$$

$$\max_{A_{q,t}} \left| \Pr[A^{\mathbb{O}}_{q,t}() = 1 : \mathbb{O} \twoheadleftarrow \mathrm{Perm}(\mathcal{M})] \right.$$

$$\left. - \Pr[A^{\mathbb{O}}_{q,t}() = 1 : \mathbb{O} = \mathcal{E}(k,\cdot), k \twoheadleftarrow \mathcal{K}] \right|$$

$A^{\mathbb{O}}_{q,t}$: An algorithm running in time $\leq t$, making $\leq q$ queries to $\mathbb{O}$

Why so many definitions??

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

- Definitions are essential to:
  - Formalise our objectives (“hide information”, “check the authenticity of a document”…)
  - Decide when we’re happy (when is the “hiding” good enough?)
  - Design “interfaces” between different levels of functionality (modularity is nice!)
- → The language used to work with crypto (in research, the industry…)

Why is crypto fun?

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

- It mixes computer science, maths and electrical engineering
- It's about engineering in an adversarial context → —it's only the worst case that matters! —no room for improvisation (good training for any domain where there are adversaries, incl. e.g. computer security at large)

Organisation/Schedule

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

- Two lecturers: Pierre Karpman (first half) and Bruno Grenet (second half)
- Mix of lectures and tutorials (one of each per week)
- One (graded) lab session over two weeks ← The contrôle continu
- One final exam

Is it (not) the course for me?

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

- Maybe for you if:
  - You want to learn about crypto
  - You're considering applying to the cybersecurity or CSI M2 next year
- Maybe not for you if:
  - You have no interest for crypto
  - You hate maths and/or algorithmics