LSIN603 - Cryptographie

Présentation du Cours

Yann Rotella

UVSQ - Université Paris-Saclay

22 janvier

Votre Enseignant

- Yann Rotella
- Enseignant-chercheur en Cryptographie (cryptanalyse)
- Bureau B309 - Bâtiment Descartes
- https://rotella.fr
- Communication par mail

✍ yann.rotella@uvsq.fr

✍ https://yannrotella.github.io/cryptol3/

Modalités d'Évaluation

Contrôle continu :

- deux dates (le mardi 10 mars 2026 et le mardi 21 avril 2026)
- sur papier, sans document, 10 cours et 10 exercices

Rattrapage CC :

- uniquement si ABJ - voir avec la scolarité
- Idem, et sur tout le programme
- remplace la (ou les) notes

Examen :

- 7 cours et 13 exercices

Note finale :

- 40% CC et 60% Examen
- Le rattrapage final remplace tout

Cours et Travaux Dirigés

12 Travaux Dirigés et 12 Cours Magistraux

Il n'est pas possible de suivre les TDs sans avoir compris le cours

Trois groupes de TDs :

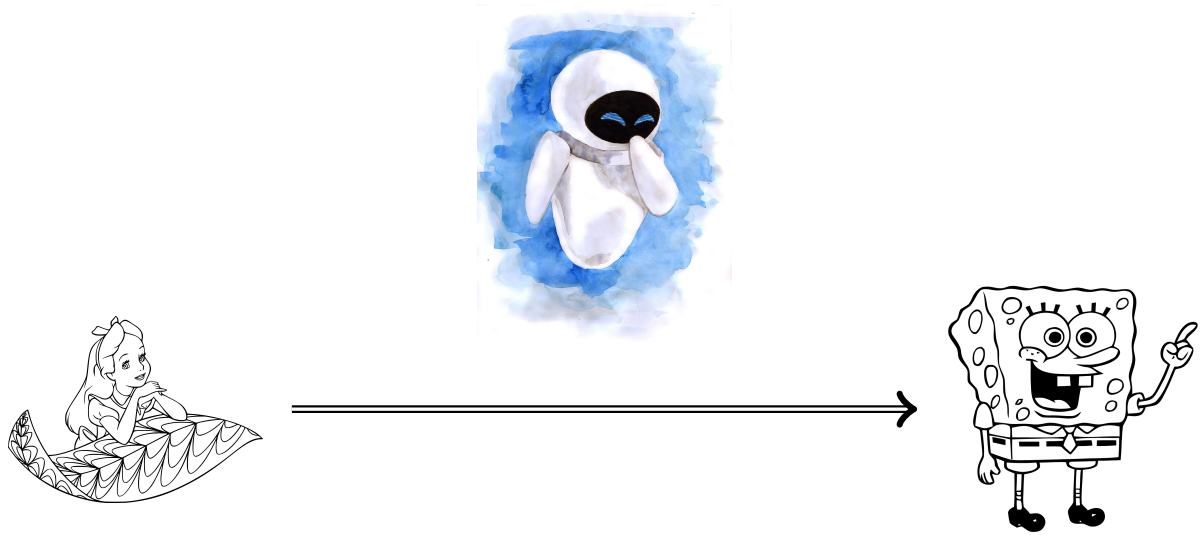
- Groupe TD1 : les mercredi après-midi avec Jules Baudrin
- Groupe TD2 : les jeudi après-midi avec Yann Rotella
- Groupe TD3 : les Lundis après-midi avec Maxime Louvet

Plan du cours

1. Histoire de la cryptographie (jusqu'à 1950)
2. Théorie de Shannon, concept de sécurité
3. Définitions de Sécurité et Primitives
4. Stratégies de Conceptions (des Chiffrements par Bloc)
5. Cryptanalyse des Chiffrements par Bloc
6. Fonctions de Hachage Cryptographiques
7. Modes Opératoires, MACs et AEAD
8. Arithmétique, Diffie-Hellman, El-Gamal et Réductions
9. Arithmétique, RSA, RSA-OAEP
10. Signatures numériques et authentification
11. Certificats, protocoles et confiance
12. Aperçu de Cryptographie Avancée

Qu'est ce que la cryptographie ?

Kruptos (caché) et graphein (écrire)

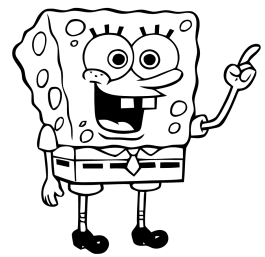


- Confidentialité : protéger les informations échangées, les données (sensibles)
- Authenticité : s'assurer de la légitimité de l'expéditeur du message
- Intégrité : s'assurer de la non-modification d'un message (intentionnellement ou non)

CRYPTOGRAPHIE SYMÉTRIQUE

On suppose que Alice et Bob possèdent un secret commun appelé la clef notée k

$$k \in \mathcal{K}, m \in \mathcal{M}$$
$$E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$$
$$E_k(m) = E(k,m) = c$$



$$k \in \mathcal{K}, c \in \mathcal{C}$$
$$D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$$
$$D_k(c) = D(k,c) = m$$

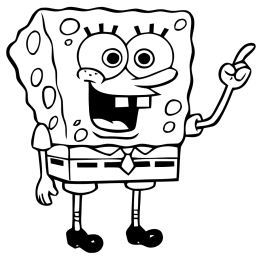
Il faut que E et D soient construits de telle sorte que

$$\forall k \in \mathcal{K}, \forall m \in \mathcal{M}, D_k(E_k(m)) = m.$$

CRYPTOGRAPHIE ASYMÉTRIQUE

Bob possède une clef publique (pk_B - public) et une clef privée (sk_B - secret)

$$pk_B \in \mathcal{P}_k, m \in \mathcal{M}$$
$$Enc : \mathcal{P}_k \times \mathcal{M} \to \mathcal{C}$$
$$Enc_{pk_B}(m) = Enc(pk_B, m) = c$$



$$sk_B \in \mathcal{S}_k, c \in \mathcal{C}$$
$$Dec : \mathcal{S}_k \times \mathcal{C} \to \mathcal{M}$$
$$Dec_{sk_B}(c) = Dec(sk_B, c) = m$$

Il faut que Enc et Dec soient construits de telle sorte que

$$\forall (pk, sk) \in \mathcal{P}_k \times \mathcal{S}_k, \forall m \in \mathcal{M}, Dec(sk, Enc(sk, m)) = m.$$

Avoir en tête

- Algorithmes de chiffrement et de déchiffrement.
- Qu'est ce que Eve connaît ?
- Coût des algorithmes.
- Aucun algorithme pratique n'est 100% sûr.
- Cryptanalyse - décrypter.
- message clair, message chiffré, clef (secrète, publique, privée), chiffrer et déchiffrer.
- Confidentialité, Authenticité et Intégrité.