Cours de cryptologie appliquée de l'EPITA
TLS - partie 3

Manuel Pégourié-Gonnard
mpg@elzevir.fr

ARM France - IoT - mbed TLS

26 novembre 2015

`https://github.com/mpg/cours-tls`

Actu : Lucky 13 frappe Amazon s2n

https://eprint.iacr.org/2015/1129

Références complémentaires - TLS

- Rappel : RFC 5246 TLS 1.2, RFC 7525 recommandations pratiques, RFC 7457 attaques
- `https://www.trustworthyinternet.org/ssl-pulse/` statistiques sur les serveur HTTPS populaires
- `https://www.ssllabs.com/ssltest/` testez votre serveur !

Références crypto elliptique – en ligne

- Courte introduction aux courbes et à des techniques d'implémentation efficace : `https://www.imperialviolet.org/2010/12/04/ecc.html`
- Intro plus détaillé avec code Python : `http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/`
- Un article retraçant l'histoire et pourquoi (on croit que) ça marche, avec un des inventeurs : `http://www.sciencedirect.com/science/article/pii/S0022314X09000481`
- Une version gratuite des standards : `http://www.secg.org/sec1-v2.pdf`

Références crypto elliptique – livres

- Koblitz, *A Course in Number Theory and Cryptogrphy*, Springer, GTM 114. Tout le bagage mathématique nécessaire, et plus encore, en 200 pages (dont 40 sur les courbes elliptiques), avec une approche assez pratique (complexité algorithmique) pour un livre de maths.
- Hankerson, Menezes, Vanstone, *Guide to Elliptic Curve Cryptography*, Springer. La bible de l'implémenteur il y a 10 ans, quelques manques depuis (side-channels, nouvelles formes de courbes).
- Cohen, Frey (Eds), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall. Juste *la* référence sur tous les aspect théoriques.

Projets

`https://github.com/mpg/cours-tls`