Déchiffre et Delettre*

Chiffrement avec clé unique, RSA et

… survol de la transmission quantique de clés... si on a le temps.

Avant 1996, le chiffrement privé était interdit en France. Pire, il “était considéré comme une arme de guerre de deuxième catégorie” (cf wikipédia). Je n’aurais donc pas pu proposer cet atelier. Ce n’est plus le cas grâce entre autres à des militants des libertés civiles. Alors profitez de cette liberté pour écrire votre propre (petit) logiciel pour par exemple, chiffrer vos mails ou MP en étant sûr qu’ils ne seront jamais stockés en clair sauf chez vous et votre destinataire, jamais “étudiés” par les IA des GAFAM !

Nous allons voir en premier le chiffrement/déchiffrement d'un message avec une même clé secrète puis avec le système RSA (clé publique pour chiffrer et privée pour déchiffrer).

Cet atelier durera 2 heures.
Pour cela nous n'écrirons que les modules liés au coeur du sujet ; les autres modules périphériques étant déjà fournis et testés.

Pré-requis:

Une connaissance minimum de Java-script ou d'un autre langage de programmation est souhaitable.
Voir si besoin : https://fr.eloquentjavascript.net/contents.html

Venir avec son ordinateur en ayant installé si besoin, un éditeur de texte comme www.flashdevelop.org/ (windows) ou www.sublimetext.com/ (Mac, Linux et Windows)

Cible :

Toute personne ayant envie de comprendre les bases du chiffrement/déchiffrement de donnée, de préférence avec des notions élémentaires de math. (Il n'y aura pas de démonstration théorique)

Date / Lieu / Inscription :

L’atelier aura lieu le xx/04/2019 de 19H à 21H à (adresse + lien)
(Add meetup widget)

Intervenant :

Cet atelier sera animé par Jean Michel *Delettre front & back-end developer www.pixaline.net/