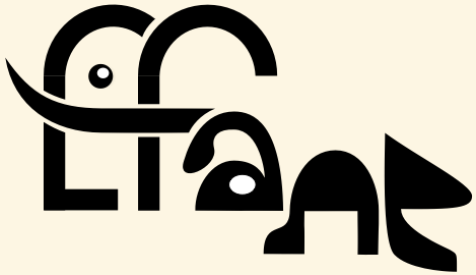
Cryptologie – Introduction aux Cours

2015/03/22 – EMA, Libreville

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest



Cryptologie à clé publique

Cryptologie :

- Chiffrement ;
- Authenticité ;
- Intégrité.

La cryptologie à clé publique est basée sur une fonction à sens unique (avec trappe)
$\Rightarrow$ chiffrement asymétrique, signatures, preuves sans connaissances...

Applications :

- Militaires ;
- Vie privée ;
- Communications (internet, téléphones...)
- Commerce électronique...

Contexte Historique

- Riche histoire ; chiffrement de messages depuis l'antiquité au moins ;
- Principale application auparavant militaire ;
- Dorénavant la cryptologie joue un rôle essentiel pour garantir la sécurité des communications ;
- Cryptanalyse : déchiffrement d'Énigma par le groupe Ultra (Secret) à Blentchey Park lors de la seconde guerre mondiale ;
- À la fin de la guerre, vente des machines Énigma capturées par les alliés à des pays du Tiers Monde.

Contexte actuel

- http://en.wikipedia.org/wiki/PRISM_(surveillance_program) :
  « The Prism program collects stored Internet communications based on demands made to Internet companies » (Microsoft, Yahoo !, Google, Facebook, Paltalk, YouTube, AOL, Skype, Apple...)
- En sus de ce programme d'espionnage, utilisation de virus extrêmement sophistiqués, capables de s'infiltrer dans le firmware des disques durs : Stuxnet, Flame, Equation Group.
- Officiellement pour lutter contre le terrorisme ;
- Mais aussi utilisé pour l'espionnage économique :
  http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
- Les États-Unis ne sont pas les seuls à avoir des systèmes de surveillance...
  http://www.theguardian.com/world/2013/jul/04/france-electronic-spying-operation-nsa

⇒ L'utilisation de la cryptographie est un enjeu de souveraineté nationale !

Quelle cryptographie ?

- Tout système ad-hoc, non basé sur des standards a été cassé (DECSS, GSM, WEP...)
- Utiliser un standard suffit-il ?

Quelle cryptographie ?

http://blog.cryptographyengineering.com/2013/09/on-nsa.html

Matthew Green – « The NSA has been :

- Tampering with national standards (NIST is specifically mentioned) to promote weak, or otherwise vulnerable cryptography.
- Influencing standards committees to weaken protocols.
- Working with hardware and software vendors to weaken encryption and random number generators.
- Attacking the encryption used by “the next generation of 4G phones”.
- Obtaining cleartext access to “a major internet peer-to-peer voice and text communications system”
- Identifying and cracking vulnerable keys.
- Establishing a Human Intelligence division to infiltrate the global telecommunications industry.
- decrypting SSL connections.

»

Quelle cryptographie ?

- Tout système ad-hoc, non basé sur des standards a été cassé (DECSS, GSM, WEP...)
- Utiliser un standard suffit-il ?

⇒ On a besoin d'une cryptographie issue de la recherche publique, conduite par des experts universitaires, en lien avec le milieu économique local.

But du cours : expliquer les concepts clés de la cryptologie, plutôt que de donner des « boîtes à outils » toutes prêtes.