Projet : Rapport et Oral

L'objectif de ce TP est à la fois de vous permettre d'explorer une thématique de votre choix et vous sert d'entrainement à la vulgarisation. Il s'agit d'un travail **individuel**.

Oral. Vous présenterez votre sujet sur les séances du **lundi 28 novembre** et **mardi 29 novembre**. Votre présentation doit durer 10 minutes **au plus** et donner un bon aperçu de votre sujet. Vous pouvez utiliser des diapos, auquel cas il faudra les envoyer la veille de la séance, avant 18h, pour ne pas perdre de temps.
Vous passerez par ordre alphabétique.
Faites des répétitions avant l'oral, si vous dépasser trop au niveau du temps nous devrons mettre fin à la présentation pour ne pas prendre de retard.

Rapport. À rendre pour le **dimanche 20 novembre au plus tard**. Le rapport doit faire au moins **5 pages de contenu** (en restant raisonnable sur les marges, la taille de police, etc...) et peut être rédigé en français ou en anglais. Vous pouvez bien sûr vous aider de schémas et d'illustrations (encore une fois dans la limite du raisonnable). Pour clarifier : les pages de garde, sommaire et autres ne comptent pas comme du contenu. En cas de doutes, demandez moi.
N'oubliez pas de bien citer vos sources, quelles qu'elles soient.
Implémentation : si le sujet s'y prête, fournir une implémentation (C/C++/Python/Sage) en lien avec le sujet.

Sujets. Voici une liste de sujets potentiels. Si vous avez des idées de sujet en lien avec la cryptographie, n'hésitez pas à le proposer. Vous êtes libre d'aborder le sujet sous l'angle qui vous intéresse, dans la mesure où vous conservez l'aspect cryptographique (dans le doute, demandez).

1. Le problème du sac à dos, cryptosystèmes associés et attaques.
2. Vote électronique (= à distance).
3. Étude du WEP et attaques.
4. Étude de WPA2 et attaques.
5. Étude de WPA3 (améliorations, attaques, ...).
6. Cryptanalyse du DES.
7. Cryptanalyse de l'AES.
8. Algorithme AKS pour la primalité.
9. Codes correcteurs de paquets d'erreurs (codes CIRC des CD par exemple).
10. Système des cartes bancaires.
11. Cryptosystème de McEliece (basé sur les codes correcteurs) et attaque.
12. La machine Enigma.
13. Fonctionnement des DRM (Digital Rights Management).
14. Algorithme QFS (voire NFS) pour la factorisation.
15. Le système CSS (protection des DVD).
16. GPG/PGP (outils grand public de communication électronique sécurisée).
17. Présentation et cryptanalyse de FEAL (chiffrement par bloc).

18. Attaques de MD5 (fonction de hachage).
19. Attaques de SHA1 (fonction de hachage).
20. Sécurité des passeports éléctroniques.
21. Algorithme de Shor pour casser RSA et/ou le logarithme discret avec un ordinateur quantique.
22. Compromis temps-mémoire et rainbow tables pour casser les mots de passe.
23. Cryptomonnaies (type bitcoin).
24. Sécurité des applications de messagerie instantanée (WhatsApp/Signal par exemple).
25. Le système de chiffrement par flot ChaCha.
26. La cryptographie en boite blanche.
27. L'algorithme de Berlekamp-Massey pour attaquer les LFSR.
28. Système de chiffrement préservant le format (chiffrement homomorphe).
29. TLS (v1.3).
30. L'outil John the Ripper (fonctionnement, utilisation, limites, ...).
31. Les gestionnaires de mots de passe.
32. Attaques sur RSA.
33. Les ransomwares.
34. Principes/techniques de génération aléatoire.
35. Attaques micro-architecturales (e.g. cache-attacks) visant les implémentations cryptographiques.
36. Vulnérabilités dans les communications sécurisés par mail (rejoint GPG/PGP).
37. Attaques par canaux cachés sur implémentations cryptographiques.
38. <insérez votre super bonne idée ici>