Criptografía: Aspectos Teóricos y Prácticos — Proyecto final

En vez de tener un examen final, habrá un proyecto final que se tratará de un tema criptográfico. Constará de tres partes:

- la implementación de algo relacionado con el tema
- una presentación sobre el tema
- un paper hablando de aspectos históricos del tema y el fundamento matemático del tema.

Será requerido que trabajen en equipos de tres.

Implementación

Las implementaciones se escribirán en python/Sage y deberían funcionar sin problem en el servidor de Sage. Se entregará el último día de clases.

Presentaciones

Las presentaciones serán durante la última semana de clases y cada presentación durará 25 minutos. Parte de la calificación de las presentaciones será determinada por la audiencia usando una rúbrica que será publicada antes de las presentaciones. La presentación debería hablar un poco sobre la implementación, aspectos históricos y los fundamentos matemáticos. Se entregará el último día de clases.

Papers

Los papers deberían ser entre 4 y 8 páginas de largo. Antes de las presentaciones se publicará una rúbrica para los papers.

Temas

El tema del proyecto es a elección para incluyo una lista para darles una idea:

- criba de cuerpos de números
- como hallar raíces primitivas
- el algoritmo LLL
- funciones hash
- generadores de números aleatorios y pseudo-aleatorios
- pruebas con cero conocimiento (Zero-Knowledge proofs)
- esquemas para compartir cosas en secreto
- criptografía con curvas hiperelípticas
- steganografía
- SIGABA/Enigma
- el cifrado Solitaire
- el cifrado Beale
- Bitcoin

- códigos que corrigen errores
- Kerberos
- DES y AES
- SSL y TLS
- esquemas de firmas (ElGamal, ataques de cumpleaños)