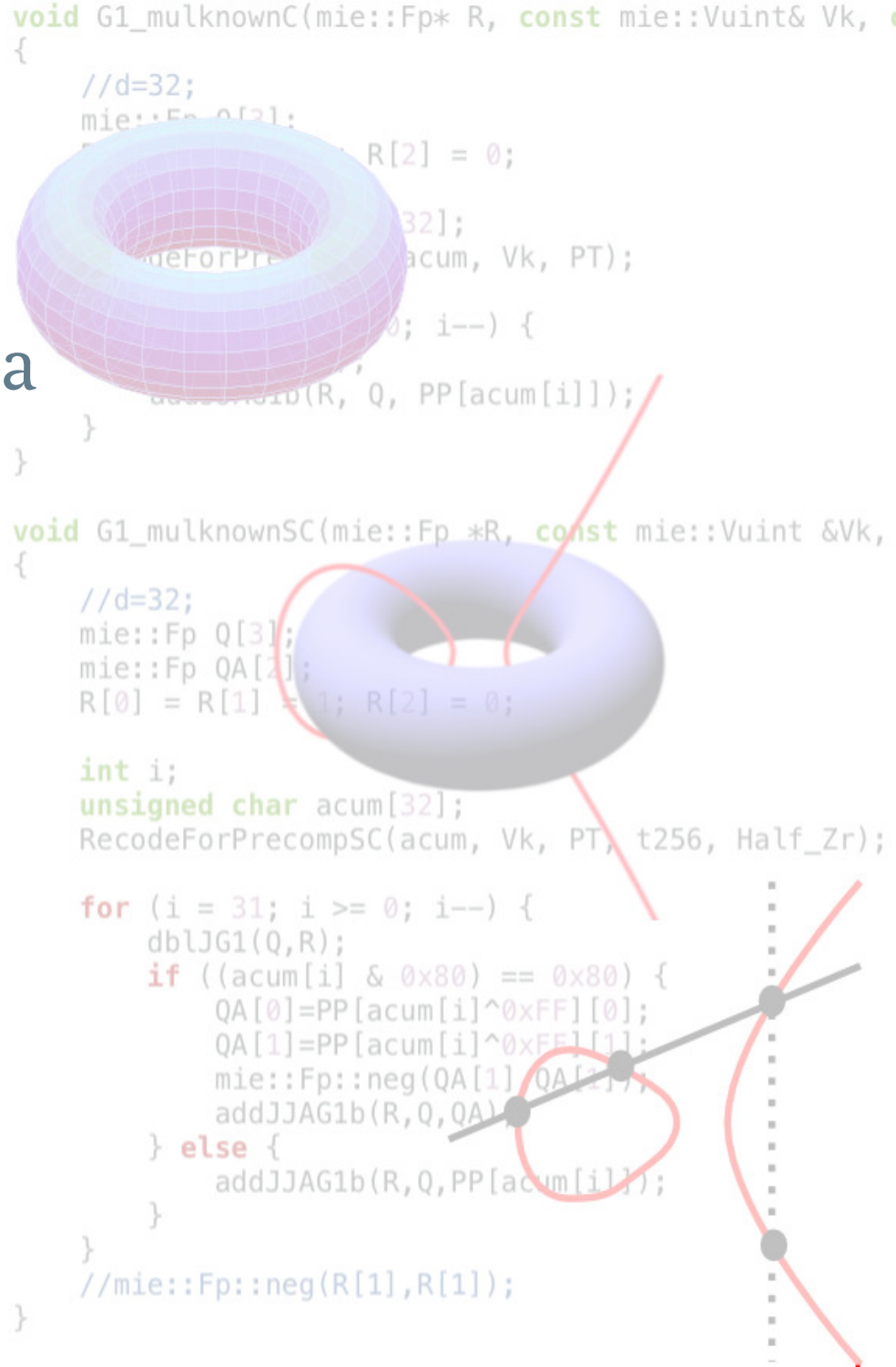
Matemáticas aplicadas a la criptografía

Dr. Luis J. Dominguez Perez

Universidad Don Bosco

Abril 22, 2013



Criptología

La criptología se divide en:

- Criptografía
- Criptoanálisis

- La criptografía busca construir esquemas de protección a la información
- El criptoanálisis busca sus debilidades , sólo así sabremos si los esquemas son seguros o no.

Criptología

La criptología se divide en:

- Criptografía
- Criptoanálisis

- La criptografía busca construir esquemas de protección a la información
- El criptoanálisis busca sus debilidades , sólo así sabremos si los esquemas son seguros o no.

Criptología

La criptología se divide en:

- Criptografía
- Criptoanálisis

- La criptografía busca construir esquemas de protección a la información
- El criptoanálisis busca sus debilidades , sólo así sabremos si los esquemas son seguros o no.

Criptografía

- Dentro de la criptografía, están los esquemas simétricos (utilizados principalmente para proteger la información), y los esquemas asimétricos (utilizados para proteger las ``llaves''). En la práctica los sistemas son híbridos.

- En este curso veremos aprenderemos acerca de las matemáticas alrededor de los esquemas simétricos y sobre algunos esquemas asimétricos.

Los esquemas asimétricos permiten elaborar protocolos de seguridad muy complejos, pero su implementación también lo es.

Criptografía

- Dentro de la criptografía, están los esquemas simétricos (utilizados principalmente para proteger la información), y los esquemas asimétricos (utilizados para proteger las ``llaves''). En la práctica los sistemas son híbridos.

- En este curso veremos aprenderemos acerca de las matemáticas alrededor de los esquemas simétricos y sobre algunos esquemas asimétricos.

Los esquemas asimétricos permiten elaborar protocolos de seguridad muy complejos, pero su implementación también lo es.

Criptografía

- Dentro de la criptografía, están los esquemas simétricos (utilizados principalmente para proteger la información), y los esquemas asimétricos (utilizados para proteger las ``llaves''). En la práctica los sistemas son híbridos.

- En este curso veremos aprenderemos acerca de las matemáticas alrededor de los esquemas simétricos y sobre algunos esquemas asimétricos.

Los esquemas asimétricos permiten elaborar protocolos de seguridad muy complejos, pero su implementación también lo es.

Contenido

- Bases matemáticas
- Teoría de números
- Campos finitos
- Logaritmo discreto
- Aritmética modular
- Criptosistemas de bloque
- Criptosistemas de flujo

Bases matemáticas generales

Repaso general, y utilización de SAGE:

- Tipos de números
- Teorema, lema, corolario, proposición
- Teoría de conjuntos, matrices, y vectores

Tópicos de Teoría de Números

Introducción a la Teoría de Números

- Panorama general

Tópicos selectos de teoría de números

- Estimados de tiempo para hacer aritmética
- Divisibilidad y el algoritmo de Euclides
- Congruencias
- Factorización y sus aplicaciones

Campos Finitos

Campos finitos y residuos cuadráticos

- Grupos, anillos, polinomios, y campos finitos
- Residuos cuadráticos, y reciprocidad

Logaritmos discretos

Logaritmos discretos y Diffie-Hellman

- El problema del logaritmo discreto
- Intercambio de llaves de Diffie-Hellman
- Dureza del DLP, y sus ataques
- Teorema Chino del residuo

Aritmética Modular

- Operaciones aritméticas básicas
- Técnicas de reducción

Criptosistemas de bloque

Criptosistemas de bloque

- Confusión y difusión
- Redes de Feistel
- Cajas de sustitución
- Técnicas de expansión de llave
- Estándar de cifrado triple de datos
- Estándar de cifrado avanzado
- Modos de operación

Criptosistemas de flujo

- Generalidades
- Pseudo/aleatoriedad
- Postulados de Goulomb y Maurer
- Registro de desplazamiento de regeneración lineal (Linear Feedback Shift Register LFSRs)
- Complejidad Lineal
- Operaciones no lineales

Sección virtual

- Se dará asesoría virtual mediante la página del curso.
- De haber suficiente cantidad de interesados, se podrá complementar el curso con una introducción a los siguientes temas (vía google hang-out o similar):
  - Curvas elípticas
  - Retículas (Lattices)
  - Cómputo cuántico
  - Criptografía poscuántica

Aspectos de evaluación

- Exposiciones (60%):
  - Participación en clase: 40%
  - Participación virtual (página): 20%

- Trabajos (40%):
  - Proyecto unidad VI: 15%
  - Proyecto unidad VII: 15%
  - Caso de estudio: 10%

Proyectos de evaluación

Actividad	Fecha de entrega
Cifrado AES	2013-05-05
Análisis RC4	2013-05-12
Estimación de costos	2013-05-19

Documentos exportados a formato PDF, a más tardar el día indicado a la hora de El Salvador.

Sage

- Sage es un software matemático open-source con licencia GPL. Combina el poder de muchos paquetes open-source en una interfaz Python.

- Busca ser una alternativa viable a Magma, Maple, Mathemática y Mathlab.

http://www.sagemath.org

Instalación de Sage

- La instalación es sencilla, y existen paquetes listos para OSX, Windows, Linux, y otros.
- El instalador es autocontenido, trae todas las herramientas.
- Dado que es open-source, se cuenta con la posibilidad de bajar el software. (aunque en algunos casos puede requerir instalar los ``esenciales'')
- Sin embargo, requiere mucho espacio en disco: $\sim$580 MB del instalador, y poco más de 2.3GB en disco.

Instalación de Sage

- La instalación es sencilla, y existen paquetes listos para OSX, Windows, Linux, y otros.
- El instalador es autocontenido, trae todas las herramientas.
- Dado que es open-source, se cuenta con la posibilidad de bajar el software. (aunque en algunos casos puede requerir instalar los ``esenciales'')

- Sin embargo, requiere mucho espacio en disco: $\sim$580 MB del instalador, y poco más de 2.3GB en disco.

Instalación de Sage

Práctica:

- Descargar Sage
- Distribuir Sage
- Instalar
- Línea de comando
- Interfaz Notebook