BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA
FACULTAD DE CIENCIAS DE LA COMPUTACIÓN

Profr. Carlos Alberto López Andrade
Materia: Estructuras Discretas

Proyecto (Exposiciones)

Aviso

Este proyecto aporta $10\,\%$ (1 pto.) de la evaluación final.

Código de Honor

Debe asegurarse de que todos los miembros de su equipo contribuyan al proyecto. No deje que una persona haga todo el trabajo. Si usted tiene un miembro del equipo que no está contribuyendo, hable conmigo al respecto.

Instrucciones

- Formar equipos de 3 o 4 miembros.
- Seleccionar alguno de los temas que aparecen abajo para su exposición en clase ($20 - 30$ minutos) y comunicármelo a la brevedad para ver la disponibilidad de los mismos.
  - *Criptografía simétrica*
    - Corrimiento simple
    - Cifrados de Transposición
    - Cifrados por Permutación
  - *Criptografía asimétrica*
    - RSA
  - *El problema del logaritmo discreto (Asignado)*
  - *Generación de números pseudoaleatorios (Asignado)*
- Apoye su exposición con ejemplos.
- Utilice transparencias (OpenOffice.org Presentaciones, Beamer, etc.) y/ó mapas conceptuales (CmapTools) y/ó algún CAS (acrónimo de Computer Algebra System), si es necesario, para su exposición.
- Fecha de inicio de la presentación de las exposiciones: Viernes 6 de Mayo de 2011.

Textos sugeridos [Kob94], [MvOV97], [Sti95].

Bibliografía

[Kob94] N. Koblitz, *A course in number theory and cryptography*, 2nd ed., Springer-Verlag, 1994.

[MvOV97] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1997.

[Sti95] Douglas R. Stinson, *Cryptography: Theory and practice*, CRC Press, 1995.

Puebla, Pue., a 17 de abril de 2011