Plan de trabajo para Criptografía I

Trimestre 24-O

Profesor y cubículo:
José Noé Gutiérrez (AT-210)
e-mail: ngh@xanum.uam.mx
Asesorías: Miércoles de 14:00 a 15:00 horas, o previa cita.

Exámenes

El curso se evaluará con tres exámenes parciales (o un examen global final), tareas y un reporte escrito.

Las tareas tendrán un valor del 20% de la calificación final, el reporte escrito contará 20% de la calificación final, mientras que el 60% restante se le asignará al resultado de los exámenes.

Los exámenes parciales se aplicarán los días viernes de las semanas 4, 8 y 11 del trimestre, mientras que el examen global será el miércoles de la semana 12.

Escala de calificaciones

Una calificación en el intervalo:
[0, 6) corresponde a NA
[6, 7.5) corresponde a S
[7.5, 8.8) corresponde a B
[8.8, 10] corresponde a MB

Temario

1. **Conceptos Básicos**
   Componentes de un sistema de cifrado.
   Tipos de cifrado.
   Servicios básicos de la criptografía.
2. **Algoritmos de Cifrado Clásicos**
   Cifrados por sustitución monoalfabética.
   Cifrados por sustitución polialfabética.
   Cifrados por transposición.
   Criptoanálisis de algoritmos por sustitución.
3. **Cifrados de clave privada**
   DES: Descripción e implementación.
   IDEA: Descripción e implementación.
   AES: Descripción e implementación.
4. **Cifrados de clave pública**
   El sistema RSA.
   Implementación del RSA de acuerdo al estándar.
   ElGamal sobre curvas de Koblitz.
5. **Temas Optativos**
   1. Secreto dividido. **2.** El algoritmo LLL. **3.** Criptografía visual. **4.** Criptoanálisis lineal. **5.** Factorización de enteros. **6.** Criptoanálisis diferencial. **7.** Generación de sucesiones. **8.** El cifrado de Niederreiter. **9.** El criptosistema de McEliece. **10.** El problema del logaritmo discreto. **11.** Creación de un cifrado permutación-sustitución.

Bibliografía

1. Baumslag, G., Fine, B., Kreuzer, M., Rosenberger. G. *A Course in Mathematical Cryptography*. De Gruyter Graduate, 2015.
2. Boneh, D., Shoup, V. *A Graduate Course in Applied Cryptography*. 2023. Free online https://crypto.stanford.edu/~dabo/cryptobook/
3. Daemen, J. & Rijmen, V., *The Design of Rijndael. The Advanced Encryption Standard (AES).* Springer, 2nd Edition, 2020.
4. Katz, J. and Lindell, Y. *Introduction to Modern Cryptography.* CRC Press, 2nd Edition, 2015.
5. Knudsen, L.R. and Robshaw, M.J.B. *The block cipher companion*. Springer-Verlag, 2011.
6. Stallings, W. *Cryptography and Network Security, Principles and Practice*. PEARSON, 7th Edition, 2017.
7. Stinson, D.R. and Paterson, M.B. *Cryptography: Theory and Practice.* CRC Press, 4th Edition, 2019.