Criptografía II

Trimestre 25-I
Profesor: José Noé Gutiérrez H., Cubículo AT-210
Correo: ngh@xanum.uam.mx
Asesorías: lunes de 13:00 a 14:00 horas, por Zoom los jueves de 14:00 a 15:00 horas o previa cita

TEMARIO

Funciones hash y autenticación

Integridad de los datos. Seguridad de las funciones hash. El modelo del Oráculo aleatorio. La construcción esponja. SHA-3

Códigos autenticadores de mensajes

MAC y HMAC. CBC-MAC. Cifrado autenticado. MAC incondicionalmente seguros. Familias hash fuertemente universales

Criptoanálisis lineal y diferencial

Descripción e importancia de las técnicas de criptoanálisis lineal y diferencial.

Criptografía basada en retículas

NTRU, Kyber.

Evaluación del curso

El 70% de la calificación se asignará al resultado de tres exámenes parciales, o bien al de un global. Quienes tengan dos exámenes parciales aprobados tendrán derecho a presentar reposición de un parcial. Las tareas tendrán un valor de 30% de la calificación final. Los ejercicios de las tareas pueden responderse con ayuda de la computadora, por ejemplo utilizando Sage, Python, Maxima o Mathematica.

Las tareas pueden realizarse en equipo, sin límite de integrantes por equipo. Los equipos pueden cambiar en cualquier momento. Las tareas entregadas después de la fecha señalada se penalizarán con 1 punto por cada día natural de retraso. No se aceptarán tareas con más de 5 días de retraso.

Los exámenes se aplicarán los días viernes ***7** de marzo, **4** de abril y **25** de abril,* del presente trimestre. El examen final se aplicará el día martes 6 de mayo.

Escala de calificaciones

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

Bibliografía (*: libro de texto)

1. FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard. https://csrc.nist.gov/pubs/fips/203/final

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.