Criptografía de Clave Pública

Trimestre 21P
Profesor: José Noé Gutiérrez H.
Cubículo: AT-210
Correo: ngh@xanum.uam.mx
Asesorías: Asesorías: jueves de 14:00 a 14:40 horas o previa cita

TEMARIO

1. **Introducción** (2 semanas)
1.1. Motivación del uso de la Criptografía. Aplicaciones actuales de la Criptografía.
1.2. Sustitución simple y poli-alfabética. (Cifrados tipo Julio César, Vigenere, etc.)
1.3. Algunas técnicas de cripto-análisis.
1.4. Modelos de cifrado de Playfair y de Hill.
1.5. Secreto perfecto.
2. **Cifrados en flujo** (2 semanas)
2.1. Descripción de los cifrados en flujo.
2.2. Generadores de números pseudoaleatorios.
2.3. Registros lineales con retroalimentación.
3. **Cifrados de clave privada** (4 semanas)
3.1. El criptosistema DES.
3.2 El criptosistema IDEA.
3.3. El criptosistema AES.
4. **Cifrados de clave pública.** (3 semanas)
4.1 El criptositema RSA. Cifrado y firma digital.
4.2 Cálculo de generadores del grupo de unidades de los enteros módulo un primo.
4.3 El criptosistema ElGamal. Cifrado y firma digital.

Evaluación del curso

El 70% de la calificación se asignará al resultado de tres exámenes parciales, o bien al de un global. Las tareas tendrán un valor de 30% de la calificación final.

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 indicada se penalizarán con un punto menos sobre la calificación obtenida, por cada día natural de retraso.

Las tareas pueden resolverse con ayuda de un sistema de cómputo, como Maxima, Cryptool, Mathematica o SAGE.

Los exámenes parciales se aplicarán los días jueves **26 de agosto**, martes **21 de septiembre** y lunes **11 de octubre**. El examen final se aplicará el día lunes 18 de octubre. Si al final del curso tiene dos parciales aprobados puede presentar reposición de un parcial o bien el examen global, pero sólo una opción.

Colocaré material del curso en:
https://sites.google.com/site/cdematem/

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

Bibliografía

1. Delfs, H, and Knebl, H. *Introduction to Cryptography. Principles and Applications*. Springer Verlag, Third Edition, 2015.
***2.** Hoffstein, J. et al. *An Introduction to Mathematical Cryptography*. Springer, (UTM), 2008.
3. Katz, J. and Lindell, Y. *Introduction to Moder Cryptography.* Second Edition. CRC Press, Second Edition, 2015.
4. Klein, A. *Stream Ciphers*. Springer, 2013.
5. Menezes, A., van Oosrcot, P. C., Vanstone, S. A., *Handbook of Applied Cryptography*. CRC Press, 1996.
***6.** Paar, C., Pelzl, J., *Understanding Cryptography*, Spinger-Verlag, 2010.
7. Robling, D. E., *Cryptography and Data Security*, Addison-Wesley, 1983.
8. Stinson, D. R., *Cryptography: Theory and Practice*, CRC Press, 2006.
9. Van Tilborg, H.C.A. *Fundametals of Cryptology*. Kluwer Academic Publishers, 2002.