Criptografía de Clave Pública

Trimestre 18I
Profesor: José Noé Gutiérrez H.
Cubículo: AT-243
Correo: ngh@xanum.uam.mx
Asesorías: jueves de 12:00 a 13:00 y de 14:00 a 15:00 horas
viernes de 12:00 a 13:00 horas

TEMARIO

1. **Introducción** (3 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 de llave privada** (3 semanas)
2.1. El criptosistema DES.
2.2. El criptosistema AES.
2.3. Aplicaciones.
3. **Cifrados en flujo** (3 semanas)
3.1. Descripción de los cifrados en flujo.
3.2. Generadores de números pseudoaleatorios.
3.3. Registros lineales con retroalimentación.
4. **Normas de seguridad para redes de comunicación.** (2 semanas)

Evaluación del curso

El 80% de la calificación se asignará al resultado de tres exámenes parciales, o bien al de un global. Las tareas tendrán un valor de 20% de la calificación final.

Las tareas se entregarán los días lunes y 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.

Los exámenes se aplicarán los días viernes 29 de mayo, lunes 29 de junio y miércoles 15 de junio. El examen global se aplicará el día viernes 24 de julio.

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, 7.4) corresponde a S
[7.4, 8.7) corresponde a B
[8.7, 10] corresponde a MB

Bibliografía

1. Fúster Sabater, A. et al. *Criptografía, protección de datos y aplicaciones*. Alfaomega Ra-Ma, 2013.
2. Gómez Vieites, A. *Enciclopedia de la Seguridad Informática*. Alfaomega Ra-MA, 2011.
***3.** Hoffstein, J. et al. *An Introduction to Mathematical Cryptography*. Springer, (UTM), 2008.
4. Klein, A. *Stream Ciphers*. Springer, 2013.
5. Koblitz, N., *A Course in Number Theory and Cryptography*. Springer-Verlag, 1994.
6. Menezes, A. (Editor), *Applications of finite fields*., Kluwer Academic Press, 1993.
7. Menezes, A., van Oosrcot, P. C., Vanstone, S. A., *Handbook of Applied Cryptography*. CRC Press, 1996.
***8.** Paar, C., Pelzl, J., *Understanding Cryptography*, Spinger-Verlag, 2010.
9. Robling, D. E., *Cryptography and Data Security*, Addison-Wesley, 1983.
10. Schneier, B., *Applied Cryptography*, JohnWilley & Sons, 1996.
11. Stinson, D. R., *Cryptography: Theory and Practice*, CRC Press, 2006.
12. Van Tilborg, H.C.A. *Fundametals of Cryptology*. Kluwer Academic Publishers, 2002.