Criptografía de clave pública

Trimestre 24-O
Profesor: José Noé Gutiérrez H., Cubículo AT-210
Correo: ngh@xanum.uam.mx
Asesorías: por Zoom, los martes de 14:00 a 15:00 horas o previa cita

TEMARIO

1. **Introducción** (a) Motivación del uso de la Criptografía. Aplicaciones actuales de la Criptografía. (b) Sustitución simple y poli-alfabética. (Cifrados tipo Julio César, Vigenere, etc.) (c) Algunas técnicas de cripto-análisis. (d) Modelo de cifrado de Hill. (e) Secreto perfecto.
2. **Cifrados en flujo** (a) Descripción de los cifrados en flujo. (b) Registros lineales con retroalimentación.
3. **Cifrados de clave privada** (a) El criptosistema DES. (b) El criptosistema IDEA. (c) El criptosistema AES.
4. **Cifrados de clave pública** (a) El criptosistema RSA. Cifrado y firma digital. (b) Prueba de primalidad de Miller-Rabin (b) Factorización de enteros por métodos de p-1 de Pollard y por diferencia de cuadrados. (c) Cálculo de generadores del grupo de unidades de los enteros módulo un primo. (c) El criptosistema ElGamal. Cifrado y firma digital. (d) Curvas elípticas sobre $\mathbf{Z}_p$.

Actividades

Las clases serán a distancia, cuando sea posible se compartirán las grabaciones. Tareas y exámenes se subirán a Gradescope.

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 SageMath, 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 parciales se aplicarán los días viernes de las semanas 4 y 8, así como el miércoles de la semana 11. El examen final se aplicará el día miércoles de la semana 12.

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. Buchmann, J. Introduction to Cryptography, 2nd Ed. Springer, (UTM), 2004.
2. Delfs, H, and Knebl, H. *Introduction to Cryptography. Principles and Applications*. Springer Verlag, Third Edition, 2015.
3. *Hoffstein, J. et al. *An Introduction to Mathematical Cryptography, 2nd Ed*. Springer, (UTM), 2014.
4. Klein, A. *Stream Ciphers*. Springer, 2013.
5. Mollin, R.A., An introduction to Cryptography, 2nd Ed., Chapman & Hall/CRC, 2007.
6. Menezes, A., van Oosrcot, P. C., Vanstone, S. A., *Handbook of Applied Cryptography*. CRC Press, 1996.
7. *Paar, C., Pelzl, J., *Understanding Cryptography*, Spinger-Verlag, 2010.
8. Salomaa, A., Public Key Cryptography, 2nd Ed. Springer, 1996.
9. Smart, N. P. *Cryptography Made Simple*, Springer, 2016.
10. Van Tilborg, H.C.A. *Fundametals of Cryptology*. Kluwer Academic Publishers, 2002.