ALGORITMOS CRIPTOGRÁFICOS: TEORÍA Y PRÁCTICA

JULIO LÓPEZ

ALTENCOA8-2018
Popayán, Colombia
23 al 27 de julio de 2018

Resumen. En este minicurso serán presentados conceptos básicos de criptografía simétrica y criptografía pública. En la primera parte, estudiaremos algunos algoritmos de uso industrial tales como el agoritmo de cifrafo AES, los algoritmos SHA2 y SHA3 para calcular el resumen criptográfico de un mensaje, y algoritmos de clave pública para firmas digitales basados en curvas elípticas. En la segunda parte, abordaremos el problema de implementar en software algoritmos criptográficos. Mostraremos algunas técnicas computacionales utilizadas para implementar de forma eficiente y segura los algoritmos AES, SHA, firmas digitales (EdDSA) en los procesadores modernos como Skylake (Intel) y Ryzen (AMD). Finalmente, será mostrado el desempeño de los algoritmos en esos procesadores.

1. Conceptos básicos de criptografía
2. Algoritmos simétricos
3. Algoritmos de clave pública y curvas elípticas
4. Firmas digitales (EdDSA)
5. Implementación en software
6. Resultados de desempeño en los procesadores : Skylale, Haswell, Ryzen

Agradecimientos. Universidade Estadual de Campinas, UNICAMP, Brasil.

Universidade Estadual de Campinas, UNICAMP, Brasil.
Email address: jlopez@ic.unicamp.br

Key words and phrases. Cursillo, Criptografía simétrica y pública, Algoritmos criptográficos. **Aplicaciones**.