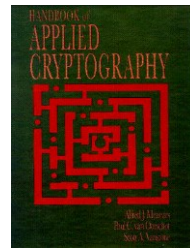


galoisenlinea
 http://galois.azc.uam.mx
 14-P
 Cupo limitado
 Insíbete
 +
 PLAN DE AGREDIACIÓN
 PARA OVENGES














- SAI Criptografía
- SAI Matemáticas Discretas
- SAI Introducción al Cálculo
- SAI Introducción al Álgebra Lineal
- SAI Complementos de Matemáticas Tradicional
- Taller de Matemáticas





Libro de texto: **Menezes A. J., Van Oorschot P. C., Vanstone S. A., "Handbook of applied cryptography", CRC Press, 2001**




Click aqui, para descargar el libro



Clases de Restos Módulo m		http://www2.uca.es/matemáticas/Docencia/ESI/1711003/Apuntes/Leccion13.pdf				
Teorema Fundamental de la Aritmética		http://www2.uca.es/matemáticas/Docencia/ESI/1711003/Apuntes/Leccion11.pdf				
Divisibilidad. Algoritmo de la División		http://www2.uca.es/matemáticas/Docencia/ESI/1711003/Apuntes/Leccion10.pdf				
Criptografía de llave secreta (simétrica) Algoritmos de cifrado Definir el problema con este tipo de cifrado Criptografía de llave pública (asimétrica) Algoritmos de cifrado Definir el problema con este tipo de cifrado Firmas digitales Sobres digitales Certificado digital Autoridad certificadoras		http://www.matem.unam.mx/~rajsbaum/cursos/web/presentacion_seguridad_1.pdf				
Cifrados numericos, cifrados alfabeticos, cifrados graficos. Frecuencias en los textos. Ocultando mensajes no escritos en clave.		http://inform.pucp.edu.pe/~edavila/scouts/manualdecriptografia.pdf				
Conceptos Basicos sobre Criptografía. Fundamentos Teóricos de la Criptografía. Teoría de la Información. Complejidad algorítmica. Aritmética modular. Urvas lípticas. Aritmética entera de multiprecisión. Criptografía y números aleatorios. Criptografía de llave privada. Cifrado por bloques. Cifrado de flujo. Algoritmos asimétricos de		http://iie.fing.edu.uy/ense/asign/seguro/Criptografia.pdf				

Introducción a la Criptografía, Seguridad Informática y Gestión de la Seguridad. Calidad de Información y Programas Malignos. Teoría de la Información. Teoría de los Números. Teoría de la Complejidad Algorítmica. Sistemas de Cifrado Clásicos. Introducción a la Cifra Moderna. Sistemas de Cifrado en Flujo. Cifrado Simétrico en Bloque.		http://www.criptored.upm.es/guiateoria/gt_m001a.htm				
Algoritmos muy basicos de criptografia clasica		http://genomorro.files.wordpress.com/2007/09/trabajo.pdf				
Algoritmos muy basicos de criptografia clasica		http://www.criptohistoria.es/files/CIFRAS.pdf				
Presentacion criptografia clasica y moderna		http://190.90.112.209/http/criptografia/2013-02-01-Presentacion_criptografia_clasica_y_moderna.pdf				
Criptografia clasica		http://criptosec.unizar.es/doc/tema_c1_criptosec.pdf				
Criptografia clasica		http://serdis.dis.ulpgc.es/~ii-cript/DOCTORADO-CRIPT-CLASICA.pdf				
Tesis doctoral: Propuesta y análisis de criptosistemas de clave pública basados en matrices triangulares superiores por bloques.		http://rua.ua.es/dspace/bitstream/10045/4081/1/tesis_doctoral_vicent_frances.pdf				
Criptografia basica para principiantes.		http://www.hacienda.go.cr/centro/datos/Articulo/Criptograf%C3%ADa%20B%C3%A1sica-Principiantes.pdf				
Tesis Licenciatura: CIFRADORES DE FLUJO PARA APLICACIONES EN TRANSMISIÓN DE VÍDEO DIGITAL		http://tesis.bnct.ipn.mx/dspace/bitstream/123456789/1180/1/roman.pdf				
Tesis: Sistema de Encripción de Datos Empleando Verificación Compartida para Redes de Área Local		http://www.cenidet.edu.mx/subaca/web-elec/tesis_mc/187MC_egel.pdf				
TESIS: Desarrollo de encriptado AES en FPGA		http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Liberatori.pdf				
Tesis: Estudio del algoritmo de cifrado Rijndael. Comparativa entre los algoritmos de cifrado DES y Rijndael		http://pitagoras.usach.cl/~eflores/lcc/cd_redes/proyecto-rinjdael.pdf				
TESIS: CRIPTOGRAFÍA CON CURVAS ELÍPTICAS SOBRE CUERPOS p-ADICOS		http://cybertesis.uni.edu.pe/bitstream/uni/281/1/medina_ar.pdf				

Algoritmos criptograficos		http://www.google.com.mx/url?sa=t&rct=i&q=&esrc=s&source=web&cd=2&sqi=2&ved=0CDQQFjAB&url=http%3A%2F%2Fwww.uv.es%2F~montanan%2Fledes%2Ftrabajos%2Falgoritmos-criptograficos.ppt&ei=msC3UufHlrs2wX8gYHwCA&usg=AFQjCNH3rbG5AcChC-aapqFtPIXVd8HXlg&bvm=bv.5818717				
Ataques sobre algoritmos criptograficos		https://www.anf.es/es/pdf/ataque.pdf				
Criptografia.		http://www.victorbravo.info/media/archivos/CursoSISeccion4.pdf				
Diseño e implementación de algoritmos criptograficos sobre FPGA		http://eprints.ucm.es/8911/1/Memoria_de_Proyecto.pdf				
Seguridad en desarrollo de software		http://manglar.uninorte.edu.co/bitstream/handle/10584/2204/Criptograf%EDa%20I.pdf;jsessionid=8207E51A22A3755E3D3694A8E3621023?sequence=1				
ALGORITMO DE CIFRADO SIMÉTRICO AES. Aceleracion de tiempo de computo sobre arquitecturas multicore.		http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Pousa_Adrian.pdf				
Criptografia asimetrica		http://www.iit.upcomillas.es/palacios/seguridad/cap05.pdf				
Cifrador de bloques: DES		http://spi1.nisu.org/recop/al02/jgargallo/index.html				
Cifrador de bloques: DES		http://es.kioskea.net/contents/130-introduccion-al-cifrado-mediante-des				
Cifrador de bloques: DES		http://es.wikipedia.org/wiki/Data_Encryption_Standard				
Cifrador de bloques: IDEA		http://es.wikipedia.org/wiki/International_Data_Encryption_Algorithm				
Aplicaciones criptograficas		http://www.iec.csic.es/gonzalo/descargas/AplicacionesCriptografiaEFS.pdf				
Cifrador de bloques: DES		http://www.tierradelazaro.com/public/libros/des.pdf				
Criptografía clásica. Criptografía moderna. Comunicación segura. Firma digital. Funciones Hash. Fundamentos matemáticos. DES. Triple DES. RC5. IDEA. AES. Diffie-Hellman. RSA. PGP. Problemas con las claves. Aspectos de seguridad.		http://usuaris.tinet.cat/acl/html_web/seguridad/cripto/cripto_1.html				
Secreto perfecto. Cifrado con clave secreta. Cifradores bloque. Ejemplos: DES, AES y otros. Cifradores flujo. Generacion de claves (secuencias cifrantes).		http://www.ia.urjc.es/cms/sites/default/files/userfiles/file/SEG-I/2012/s3xClaveSimetrica%281%29.pdf				

Criptografía de la A a la Z. Segu.Info		http://www.segu-info.com.ar/proyectos/p1_algoritmos-llave-privada.htm				
Cifrador de bloques: DES		http://dcc.puc.cl/cursos/pluginfile.php/347/mod_resource/content/0/Transparencias/iic3252-06-DES-handout.pdf				
Criptosistemas simétricos. Ventajas e inconvenientes. Cifrado por bloques. Cifrado producto. Cifrados por bloques. DES. AES. IDEA. Otros cifrados simétricos		http://ma1.eii.us.es/Material/Cripto_ii_Simetrica.pdf				