

PROGRAMAS TENTATIVOS DE LAS MATERIAS
“CRIPTOGRAFIA” (como optativa de computacion)
y “CRIPTOLOGIA” (curso de posgrado)
Segundo cuatrimestre de 2005
Profesor: Daniel Penazzi

Programa de “CRIPTOGRAFIA”

Generalidades y Criptografia Clasica Criptografia, criptoanálisis, criptología. Cifres, códigos. Cifres clásicos: permutación, claves de transposición. Substitución (mono y polialfabetica): Cesar, Vigenere, Playfair. Seguridad perfecta: el cifre Vernam (“one-time-pad”). Substitución-permutación: el cifre alemán ADFGVX. Algoritmos matriciales de Hill. Maquinas de rotor: ENIGMA.

Claves: vida útil y longitud necesaria.

Cifres de Bloque (de 64 bits) Cifres de bloque. Substitution-Permutation Networks. (SPN). Cifres Feistel. Ventajas y desventajas de SPN vs Feistel.

DES. S-boxes, difusión. Ataques contra DES. Criptoanálisis Diferencial y lineal. Ataque Davies: corolario: usar S-boxes invertibles.

Modos de operación: ECB, CBC, CFB, OFB. Ventajas y desventajas de c/u.

Otros algoritmos Feistel de 64 bits: FEAL. GOST 28147-89.

Cifres sin S-boxes: RC5.

SPN cifres con S-boxes: SAFER, sin S-boxes: IDEA

Cifres con random S-boxes: Blowfish.

Cifres con Estructura Matsui: MISTY1 y MISTY2.

Combinando Cifres: Doble encriptación. Meet-in-the-middle Attack. Triple encriptación. 3DES: modo EDE.

Cifres de bloque mas modernos

Cifre intermedio: 3-WAY.

Algoritmos de bloque de 128 o mas bits.

Finalistas de la ronda 2 del AES: Serpent, MARS, Rijndael, RC6, Twofish.

Serpent como ejemplo de SPN network heurístico con alta resistencia a DC/LC. El cifre COCONUT y el ataque “Boomerang”. Aplicación a “Serpent”. Ataques “Rectángulo” .

RC6 como ejemplo de cifre heurístico sin S-boxes.

Mars como ejemplo de diseño heterogeneo.

Cuerpos finitos. Teorema de Nyberg sobre S-boxes optimos. Construccion de S-boxes "algebraicos".

Branch Number. Codigos MDS. (Maximum Distance Separable Codes). Polinomios.

Rijndael como ejemplo de aplicacion de la teoria de cuerpos finitos y codigos MDS. Similitudes con sus antecesores, especialmente el cifr SQUARE. Resistencia de Rijndael a DC y LC. Ataque de integral cryptanalysis contra Rijndael. Ataque algebraico o XSL contra Rijndael. Rijndael como subcifr del cifr BES. Debilidad del S-box de Rijndael.

Twofish como cifr casi Feistel con aplicaciones de codigos MDS y S-boxes aleatorios.

Finalista del proyecto Nessie: el cifr Camellia. Teorema de Kanda para cifers Feistel con funciones de ronda SPN. Semejanzas y diferencias con Rijndael.

Algoritmos de Clave publica/Clave privada Principios basicos. Algoritmo RSA. Posibles ataques. Uso de RSA para firma. Posibles debilidades en combinacion con encripcion. Algoritmo de Rabin. Metodo de Intercambio de claves de Diffie-Hellmann. Algoritmo ELGAMAL (encriptado y firma). Firmas: Algoritmos de firma y autentificacion de Schnorr.

Digital Signature Standard:DSA. Standard Sovietico: GOST 34.10-94. Generalizacion a esquemas generales de firma que usan el problema del logaritmo discreto.

Feige-Fiat-Shamir. Gillou-Quisquater. Algoritmo de mochila (knapsack) de Merkle-Hellmann. Blum-Goldwasser.

Algoritmo HFE (Hidden Field Equations) y ataque XSL contra el mismo.

Teoria de numeros Testeos de primalidad: Test de Fermat. Simbolo de Jacobi. Test de Solovay-Stroessen. Test de Miller-Rabin.

Generacion de primos de DSA. Primos demostrables

Funciones de Hash Principios Generales. Ataque del cumpleaños.

Usando cifers de bloque como funciones de Hash:

Esquema de Davis-Meyer. Esquemas generales similares a Davis-Meyer. Casos particulares: esquemas de Matyas-Meyer-Oseas y Miyaguchi-Preneel.

Funciones de Hash que no dependen de cifers: Snefru, N-Hash, la familia MD4: MD4, MD5, SHA, RIPEMD-160.

Inseguridades de ellas.

Hashes mas modernos: Whirpool y SHA-2.

Uso de funciones de Hash como algoritmos de bloque: esquemas de Karn y Luby-Rackoff. Cifers de Bloque SHACAL-1 y SHACAL-2.

Cifers de corriente (Stream ciphers) y generadores de bits pseudoazar Generaciones de congruencia lineal, cuadraticos, cubicos. RSA generador. Blum-Blum-Shub.

Linear Feedback Shift Registers (LFSR). Polinomios primitivos. Complejidad lineal. Algoritmo de Berlekamp-Massey para determinar la complejidad lineal.

Combinaciones de LFSR. Generador Geffe. Otros esquemas. Esquemas de control del reloj de LFSR por otro LFSR. Alternating Step Generator. Shrinking Generator.

Non lineal FSR. FSR con carries. Numeros p-adicos.

Stream Cifers que no son LFSR: RC4, SEAL.

Stream Cifers mas modernos: SNOW, SOBER, LILI, HELIX, SCREAM, TURING, BMGL.

Programa de "CRIPTOLOGIA"

Todos los contenidos de la materia "CRIPTOGRAFIA", pero con enfasis extra en los aspectos matematicos y cryptoanaliticos de la misma. En particular, como curso de posgrado se estudiaran mas en detalle los ataques de Criptoanalisis Diferencial, Lineal e Integral, y los ataques Boomerang y Rectangulo, asi como los ataques de interpolacion, para lo cual deberan estudiarse las referencias [BBS99], [DKR97],[H],[JK97],[KKS99],[KW02],[LMM91] y [W99]. Dependiendo del tiempo se podrá estudiar el ataque algebraico de [CP02].

Ademas, como temas extras se analizaran algunos de los cifers del proyecto NESSIE y la teoria de decorrelacion de Vaudenay. ([V98]).

Bibliografia

.- **Applied Cryptography, 2nd Ed.**, *Bruce Schneier*, John Wiley & Sons, 1996.

.- **Handbook of Applied Cryptography**, *Alfred Menezes, Paul van Oorschot, Scott Vanstone*, CRC Press, 1997.

[ABK98]: R. Anderson, E. Biham, L. Knudsen, "Serpent: A Proposal for the Advanced Encryption Standard", *AES algorithm submission*, Junio, 1998, disponible en [AES].

[B99]: C. Burwick, et al., "MARS – A Candidate Cipher for AES", *AES algorithm submission*, Agosto, 1999, disponible en [AES].

[BBS99]: Eli Biham, Alex Biryukov, Adi Shamir, "Miss in the Middle Attacks on IDEA and Khufu", *Fast Software Encryption 6, LNCS 1636*, Springer -Verlag 1999, pp 124-138

[BDK01]: Eli Biham, Orr Dunkelman, Nathan Keller, “The Rectangle Attack- Rectangling the Serpent”, *Advance in Cryptology, EUROCRYPT 2001, LNCS 2045*, Springer-Verlag 2001, pp 340-357

[CP02]: N. Courtois, J. Pieprzyk, “Cryptanalysis of Block Ciphers with Overdefined Systems of Equations”, *Proceedings of AsiaCrypt02*, LNCS 2501, Springer-Verlag 2002. Tambien en <http://www.iacr.org>

[DKR97]: J. Daemen, L.R.Knudsen, V. Rijmen, “The Block Cipher SQUARE”, *Fast Software Encryption*, LNCS 1267, E. Biham, Ed., Springer-Verlag, 1997, pp 149-165.

[DR99]: J. Daemen, V. Rijmen, “AES Proposal: Rijndael”, *AES algorithm submission*, Septiembre, 1999, disponible en [AES].

[H]: Howard Heys, “A Tutorial on Linear and Differential Cryptanalysis”.
<http://citeseer.nj.nec.com/443539.html>

[JK97]: T.Jacobsen, L.R.Knudsen, “ The interpolation attack on block ciphers”, *Fast Software Encryption, LNCS 1267*, E. Biham, Ed., Springer-Verlag 1997, pp 28-40.

[KKS99]: John Kelsey, Tadayoshi Kohno, Bruce Schneier, “Amplified Boomerang Attacks Against Reduced Round MARS and Serpent”, *Fast Software Encryption 7, LNCS 1978*, Springer Verlag 1999, pp 75-93.

[KW02]: Lars Knudsen and David Wagner, “Integral Cryptanalysis (Extended Abstract)” ,
<http://citeseer.nj.nec.com/knudsen02integral.html>

[LMM91]: X. Lai, J.L. Massey, S. Murphy, “Markov Ciphers and Differential Cryptanalysis”, *Advances in Cryptology, EUROCRYPT 91 Proceedongs*, LNCS 547, Springer-Verlag, 1991, pp 17-38.

[MR02]: S. Murphy, M. Robshaw. “Essential algebraic structure within the AES”, *Proceedings of Crypto'02*, LNCS 2442, pp 17-38, Springer-Verlag 2002

[R98]: R. Rivest, et al., “The RC6 Block Cipher”, *AES algorithm submission*, Junio, 1998, disponible en [AES].

[S98]: B. Schneier, et al., ”Twofish: A 128-Bit Block Cipher”, *AES algorithm submission*, Junio, 1998, disponible en [AES].

[V98]: S. Vaudenay, “Provable Security for Block Ciphers by Decorrelation”, *STACS98, LNCS1373*, Springer-Verlag, 1998, pp 249-275

[W99]: D. Wagner “The boomerang attack”, *Fast Software Encryption 6, LNCS 1636*, Springer-Verlag 1999, pp 156-170