PROGRAMA TENTATIVO DE LAS MATERIA

"CRIPTOLOGIA" (curso de posgrado)

Segundo cuatrimestre de 2007

Profesor:Daniel Penazzi

Generalidades y Criptografia Clásica Criptografía, criptoanálisis, criptologia. Cifers, códigos. Cifers clásicos:permutación, claves de transposición. Substitución (mono y polialfabetica):Cesar, Vigenere, Playfair. Seguridad perfecta: el cifer Vernam ("one-time-pad"). Substitución-permutación: el cifer aleman ADFGVX. Algoritmos matriciales de Hill. Maquinas de rotor: ENIGMA.

Claves: vida útil y longitud necesaria.

Cifers de Bloque (de 64 bits) Cifers de bloque. Modos de operación: ECB, CBC, CFB, OFB. Ventajas y desventajas de c/u.

Substitution-Permutation Networks. (SPN). Cifers Feistel. Ventajas y desventajas de SPN vs Feistel.

DES. S-boxes, difusión. Ataque Davies: corolario: usar S-boxes invertibles. Mención de los ataques de criptanalisis diferencial y lineal (luego se ven en mas detalle)

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

Cifers sin S-boxes: RC5.

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

Cifers con random S-boxes: Blowfish.

Cifers con Estructura Matsui: MISTY1 y MISTY2.

Combinando Cifers: Doble encripcion. Meet-in-the-middle Attack. Triple encripcion. 3DES: modo EDE.

Criptoanálisis Diferencial y lineal. Criptoanálisis Diferencial: Probabilidad diferencial, δ-uniformidad, caracterisitica diferencial, diferenciales. Ejemplo de aplicación en un cifer reducido.

Criptoanálisis Lienal: Mascaras. Biases, correlaciónes y probabilidades lineales. Piling-up lemma de Matsui. Ejemplo de aplicación del ataque en un cifer reducido. Resistencia al criptoanalisis lineal. Transformada de Walsh. Relación con la no linealidad de un S-box.

Cifers de bloque mas modernos

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 heuristico con alta resistencia a DC/LC. El cifer COCONUT y el ataque "Boomerang". Aplicacion a "Serpent". Ataques "Rectangulo" .

RC6 como ejemplo de cifer heuristico sin S-boxes.

Mars como ejemplo de diseño heterogeneo.

Rijndael (AES) Cuerpos finitos, construcción y propiedades. Construcción de S-boxes "algebraicos". Teorema de Nyberg , primera parte: Sea S el S-box dado por inversión en el cuerpo finito $GF(2^n)$. Entonces S es 2-uniforme si n es impar y 4-uniforme si n es par.

Función traza. Propiedades. Teorema de Nyberg, segunda parte: Sea S el S-box dado por inversión en el cuerpo finito $GF(2^n)$. Entonces la probabilidad lineal maxima de S es menor o igual que 2^{-n+2}.

(Diferential) Branch Number de una transformación lineal. Repaso de códigos. Singleton bound. Códigos MDS. (Maximum Distance Separable Codes). Matrices MDS. Caracterización en términos de determinantes. Corolario: una matriz es MDS sii su transpuesta lo es. Linear branch number. Igualdad del diferential branch number y el linear branch number para matrices MDS.

Rijndael como ejemplo de aplicación de la teoria de cuerpos finitos y codigos MDS. Teorema: en cuatro rondas consecuticas de Rijndael hay al menos 25 S-boxes activos. Resistencia de Rijndael a DC y LC.

Introducción al criptoanalisis integral. Ataque de integral cryptanalisis contra Rijndael.

Introducción al ataque algebraico o XSL contra Rijndael. Rijndael como subcifer del cifer BES. Debilidad del S-box de Rijndael.

Propiedad: En cualquier S-box algebraico, las componentes booleanas estan todas linealmente relacionadas.

Otros cifers con alguna similaridad con Rijndael:

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

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

Algoritmos de Clave publica/Clave privada Principios básicos. Algoritmo RSA. Posibles ataques. Uso de RSA para firma. Posibles debilidades en combinación con encripción. Algoritmo de Rabin. Metodo de Intercambio de claves de Diffie-Hellmann.

Algoritmo ELGAMAL (encriptado y firma). Firmas: Algoritmos de firma y autenticación de Schnorr.

Digital Signature Standard:DSA. Standard Sovietico: GOST 34.10-94. Generalización 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-Goldwaser.

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

Generación de primos de DSA. Primos demostrables.

Funciones de Hash Principios Generales. Ataque del cumplea$\tilde{n}$os.

Funciones de hash a partir de funciones de compresión: teorema de Merkle-Damgard.

Usando cifers de bloque como funciones de Hash:

Esquema de Davis-Meyer. Esquemas generales similares a Davis-Meyer. (esquemas PGV) 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. (ataques de Dobertin y Wang)

Hashes mas modernos: Whirpool y SHA-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:

.....

Aclaración: esta materia se dictara en forma (casi) conjunta con la optativa de grado de computación "Criptografia". Los contenidos son similares, pero en "CRIPTOGRAFIA" son algunos menos. En particular, como curso de posgrado se estudiaran mas en detalle los ataques de Criptoanálisis Diferencial, Lineal e Integral, y los ataques Boomerang y Rectangulo, asi como los ataques de interpolación, 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] y la teoria de decorrelación de Vaudenay. ([V98]), o mas en detalle los ataques de Wang. ([WY05], [WYY05-1],[WLFCY05], [WYY05-0]).

Los requerimientos de aprovación de criptografia (que tambien lo serán para Criptologia) incluyen un examen final escrito, un take-home práctico, y un proyecto de programación. Ademas de eso, para el curso de posgrado Criptologia, el alumno deberá hacer un informe escrito sobre al menos dos papers de los listados (o algún otro con el que nos pongamos de acuerdo), y luego deberá rendir un examen oral (ademas del escrito) en el cual expondrá sus conclusiones sobre esos papers.

Bibliografia

.- **Applied Criptography, 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 Encription, 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