TÓPICOS SELECTOS DE LA COMPUTACIÓN
"INTRODUCCIÓN A LA CRIPTOGRAFÍA"

Dr. MOISÉS SALINAS ROSALES, <msalinasr aT CIC>

Martes y Jueves 18:00 a 20:00, Aula A1@CIC

TEMARIO

1. ORIGENES DE LA CRIPTOGRAFÍA.
1.1. NECESIDADES DE SECRECIA EN LA SOCIEDAD
1.2. CRIPTOGRAFIA CLASICA
1.3. SISTEMAS CRIPTOGRÁFICOS EN LA SEGUNDA GUERRA MUNDIAL
1.4. CRIPTOGRAFÍA Y SEGURIDAD DE LA INFORMACIÓN EN EL MUNDO ACTUAL

2. FUNDAMENTOS DE LA CRIPTOGRAFÍA.
2.1. NOCIONES DE TEORIA DE LA INFORMACION.
2.2. CRIPTOGRAFIA Y CRIPTOANALISIS.
2.3. CRIPTOSISTEMAS.
2.4. CLASIFICACIÓN DE LOS CRIPTOSISTEMAS.
2.5. ESQUEMAS, CRIPTOSISTEMAS, ALGORITMOS E IMPLEMENTACIONES

3. ESTRUCTURAS ALGEBRAICAS PARA LA CRIPTOGRAFÍA
3.1. ALGEBRA ABSTRACTA.
3.2. CONJUNTOS
3.3. GRUPOS Y ANILLOS
3.4. CAMPOS FINITOS Y SUS EXTENSIONES
3.5. OTRAS ARITMÉTICAS

4. CIFRADO SIMÉTRICO
4.1. GENERALIDADES DEL CIFRADO DE FLUJO.
4.2. MÉTRICAS PARA EVALUACIÓN DEL CIFRADO DE FLUJO
4.3. LFSR`S EN DEL CIFRADO DE FLUJO
4.4. CONFUSIÓN Y DIFUSIÓN EN CIFRADO DE BLOQUE
4.5. REDES DE FIESTEL.
4.6. TECNICAS DE EXPANSION DE LLAVE.
4.7. CIFRADORES DE BLOQUE MODERNOS
4.8. MODOS DE OPERACIÓN

5. CIFRADO ASIMETRICO
5.1. NOCIONES DE TEORÍA DE NUMEROS.

5.2. DIFFIE-HELLMAN.
5.3. RSA, RABIN Y ELGAMAL
5.4. CRIPTOGRAFÍA DE CURVA ELÍPTICA

6. PROTOCOLOS CRIPTOGRAFICOS.
6.1. DEFINICIÓN
6.2. CLASIFICACION Y REPRESENTACIÓN
6.3. SECRETO COMPARTIDO E INTERCAMBIO DE LLAVES
6.4. PROTOCOLOS DE SERVICIO DE TIEMPO.
6.5. CANALES SUBLIMINALES
6.6. GRUPO DE FIRMAS
6.7. FIRMA CIEGA
6.8. OTRAS PROPUESTAS

BIBLIOGRAFÍA

1. KONHEIM A. G, COMPUTER SECURITY AND CRYPTOGRAPHY, WILEY-INTERSCIENCE, 2007

2. FOROUZAN B. A, CRYPTOGRAPHY AND NETWORK SECURITY, MCGRAW-HILL SCIENCE/ENGINEERING/MATH; 1ST EDITION, 2007.

3. DELFS H, KNEBL H, INTRODUCTION TO CRYPTOGRAPHY: PRINCIPLES AND APPLICATIONS (INFORMATION SECURITY AND CRYPTOGRAPHY), SPRINGER; 2ND EDITION, 2007

4. STALLINGS W, CRYPTOGRAPHY AND NETWORK SECURITY, 4TH EDITION, 2005

5. HENK C.A. VAN TILBORG, ENCICLOPEDYA OF CRYPTOGRAPHY AND SECURITY, SPRINGER, 2005

6. BUCHMANN J, INTRODUCTION TO CRYPTOGRAPHY (UNDERGRADUATE TEXTS IN MATHEMATICS), SPRINGER; 2 EDITION, 2004.

7. FERGUSON N, SCHNEIER B, PRACTICAL CRYPTOGRAPHY, WILEY, 2003

8. WASHINGTON L. C, ELLIPTIC CURVES: NUMBER THEORY AND CRYPTOGRAPHY (DISCRETE MATHEMATICS ANS ITS APPLICATIONS), CHAPMAN & HALL/CRC, 2003

9. MENEZES, P. VAN, OORSCHOT, AND S. VANSTONE, HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS, 1996.

10.BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS ALGORITHMS AND SOURCE CODE IN C, SECOND EDITION, JOHN WILEY & SONS, INC, 1996.

11. DOUGLAS R STINSON, CRYPTOGRAPHY THEORY AND PRACTICE, CRC, 1995