UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERIA ELECTRÓNICA Y TELECOMUNICACIONES
PROGRAMA DE INGENIERIA DE SISTEMAS

ASIGNATURA: INTRODUCCIÓN A LA CRIPTOGRAFÍA
MODALIDAD: PRESENCIAL TEORICO / PRACTICA
INTENSIDAD: 4 HORAS TEORICO / PRACTICA / SEMANA.
PREREQUISITOS:
AREA DE FORMACIÓN: INGENIERIA APLICADA
CREDITOS: 3

OBJETIVO GENERAL

Estudiar los conceptos fundamentales sobre la Criptografía y sus aplicaciones en el mundo de la informática y las telecomunicaciones.

AL FINALIZAR EL CURSO EL ESTUDIANTE DEBE ESTAR EN CAPACIDAD DE :

1. Utilizar las técnicas de cifrado manual y los métodos de análisis de las mismas.
2. Analizar los métodos de cifrado en flujo y en bloque con clave secreta y su diseño y gestión de claves públicas y privadas en redes de computadores y de telecomunicaciones.
3. Analizar los protocolos criptográficos más usuales, construidos a partir de algoritmos de clave pública y clave secreta y las técnicas actuales de factorización de números enteros y polinomios.

METODOLOGIA

1. El alumno adquirirá los conocimientos básicos a través de clases magistrales.
2. El alumno desarrollará talleres en clase que le ayudarán a llevar a la práctica los conocimientos teóricos adquiridos.
3. El alumno deberá profundizar sus conocimientos con temas complementarios y trabajos de investigación.
4. Utilización de varios programas de apoyo para la parte de aplicaciones criptográficas.
5. Se presentarán algunos videos relacionados con la Criptografía.

CONTENIDO

1. CRIPTOGRAFÍA CLÁSICA (14 horas)

1.1. Terminología.
1.2. Historia de la criptografía.
1.3. Amenazas, servicios y mecanismos de seguridad.
1.4. Información y entropía del lenguage escrito.
1.5. Cifrados monoalfabéticos.
1.6. Cifrados polialfabéticos.
1.7. Transposiciones.
1.8. Cifrados producto.
1.9. Libros de códigos.
1.10. Máquinas de cifrar.

2. CIFRADO EN BLOQUE (6 horas)

2.1. Modos de operación.
2.2. Cifrados de Feistel, Data Encription Standard (DES)
2.3. Otros cifrados en bloque.
2.4. Combinación de varios cifrados en bloque.
2.5. Funciones resumen mediante cifrado en bloque.
2.6. Criptoanálisis diferencial.
2.7. Criptoanálisis lineal.

3. GENERACIÓN DE NÚMEROS PSEUDO-ALEATORIOS Y CIFRADO EN FLUJO (6 horas)

3.1. Cifrado en flujo.
3.2. Postulados de Golomb.
3.3. Tests de aleatoriedad.
3.4. Registro de desplazamiento realimentado linealmente, (RDRL).
3.5. Complejidad lineal de una secuencia pseudoaletoria.
3.6. Algoritmos para determinar la complejidad lineal de un generador pseudoaleatorio.
3.7. Generadores pseudoaleatorios combinando varios RDRL.
3.8. Generadores pseudoaleatorios por filtrado no lineal.

4. SISTEMAS DE CLAVE PÚBLICA (4 horas)

4.1. Principios de los criptosistemas de clave pública.
4.2. Sistema de la mochila tramposa.
4.3. Criptosistema RSA.
4.4. Sistema de ElGamal.
4.5. Criptosistemas basados en curvas elípticas.

5. GESTION DE CLAVES (6 horas)

5.1. Ataques a un criptosistema a través de la clave.
5.2. Longitudes adecuadas para las claves.
5.3. Numero de claves necesarias en una red.
5.4. Generación de claves.
5.5. Verificación de claves.
5.6. Renovación y revocación de claves.
5.7. Almacenamiento de claves.

5.8. Reutilización y destrucción de claves.
5.9. Distribución de claves mediante algoritmos de clave secreta.
5.10. Distribución de claves mediante algoritmos de clave pública.
5.11. Ejemplos de protocolos de distribución de claves en el mundo real.

6. PROTOCOLOS (4 horas)

6.1. Intercambio de claves.
6.2. Firma digital.
6.3. Firma digital con RSA.
6.4. Firma digital con El Gamal.
6.5. Firma digital estándar USA (DSS).
6.6. Funciones resumen.
6.7. Autenticación de mensajes.
6.8. Identificación de usuario.
6.9. Computación con datos encriptados.
6.10. Secretos compartidos y secretos repartidos.
6.11. Protocolos avanzados.

7. FACTORIZACIÓN Y PRIMALIDAD (4 horas)

7.1. Los números primos.
7.2. Distribución de números primos.
7.3. La fórmula de Gauss.
7.4. Breve historia.
7.5. Test de primalidad.
7.6. Pseudoprimos y primos probables.
7.7. Factorización de números enteros.
7.8. Métodos de factorización. El método rho de Pollard.

8. APLICACIONES CRIPTOGRAFICAS EN COMUNICACIONES (4 horas)

8.1. Principios de seguridad y aplicaciones en redes de comunicaciones.
8.2. Aplicaciones de seguridad en redes de comunicaciones Sistemas abiertos
8.3. Ataques a la seguridad en redes de comunicaciones
8.4. Normativa y política de seguridad en criptografía
8.5. Correo electrónico seguro
8.6. Web seguro
8.7. Autoridades de certificación
8.8. Arquitecturas de seguridad
8.9. Medios de Pago electrónicos

9. Criptografía y Sistemas Dinámicos (16 horas)

9.1. Criptosistemas Basados en Autómatas Celulares
9.1.1. Generalides de los Autómatas Celulares
9.1.2. Reglas Reversibles
9.1.3. Reglas Irreversibles
9.1.4. Criptografía de clave secreta / publica con autómatas celulares

9.1.5. Criptoanálisis en esquemas basados en autómatas celulares.
9.2. Otros sistemas dinámicos discretos en criptografía

EVALUACIONES

Se realizarán tres (3) evaluaciones de la siguiente forma:

NUMERO	%	COMPONENTES
Primer Parcial	35%	Parcial escrito 60% Talleres y/o Quices 40%
Segundo Parcial	35%	Parcial (Aplicación criptográfica 1) 60% Talleres y/o Quices 40%
Tercer Parcial	30%	Parcial (Aplicación criptográfica 2) 60% Talleres y/o Quices 40%

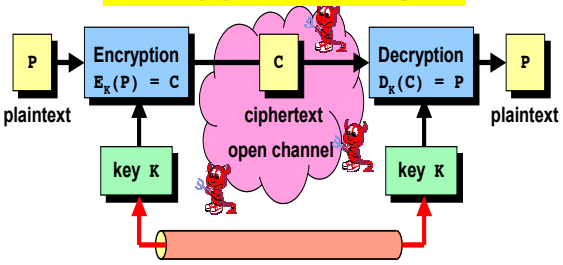
Los trabajos y talleres en grupo serán evaluados individualmente y deben estar debidamente documentados. Todo Proyecto NO sustentado pierde validez. Las sustentaciones serán programadas con anterioridad definiendo fecha y hora para cada alumno.

REFERENCIAS

1. *Applied Cryptography por Bruce Schneier. Protocols, Algorithms and Source Code in C*. Editorial John Wiley & Sons, Inc.
2. *Introducción a la Criptografía.* Pino Caballero. Editorial Alfaomega Ra-Ma.
3. *Técnicas Criptográficas de protección de datos*. Amparo Fuster, Dolores de la Guía Martínez, Luis Hernández Encinas, Fausto Montoya Vitini y Jaime Muñoz Masqué. Editorial Alfaomega Ra-Ma.
4. *Criptología y Seguridad de la Información*. Pino Caballero y Candelaria Hernández. Editorial Alfaomega Ra-Ma.
5. *Una introducción a la criptografía de clave pública*. Wolfgang Willems e Ismael Gutierrez García. Ediciones Uninorte.
6. Marco Tomassini and Mathieu Perrenoud, *Stream Cyphers with One- and Two-Dimensional Cellular Automata*, Lecture Notes in Computer Science, 2000.
7. Subhayan Sen, Chandrama Shaw, Dipanwita Roy Chowdhuri, Niloy Ganguly and P. Pal Chaudhuri, *Cellular Automata Based Cryptosystem (CAC)*, Lecture Notes in Computer Science, 2002.
8. Franciszek Seredynski, Pascal Bouvry and Albert Y. Zomaya, *Cellular automata computations*, Parallel Computing, 2004.
9. Olu Lafe, *Data Compression and Encryption Using Cellular Automata Transforms*, Engng. Applic. Artif. Intell., 1997.
10. Andrew Ilachinski, *Cellular Automata: A Discrete Universe*, World Scientific Publishing Co, 2002.
11. Roland Schmitz, *Use of chaotic dynamical systems in cryptography*, Journal of the Franklin Institute, 2001.
12. Criptografía Simétrica

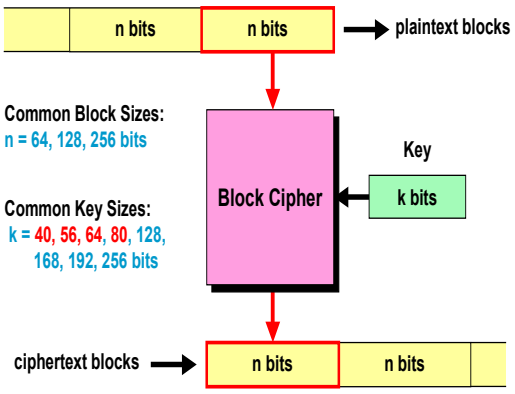
http://ma1.eii.us.es/Material/C02Simetrica.pdf
13. Criptoanálisis y Ataques a Criptosistemas.
http://www.segu-info.com.ar/proyectos/p1_ataques.htm
14. Lectura y herramientas criptográficas.
http://www.criptored.upm.es/

CRIPTOGRAFIA CLÁSICA

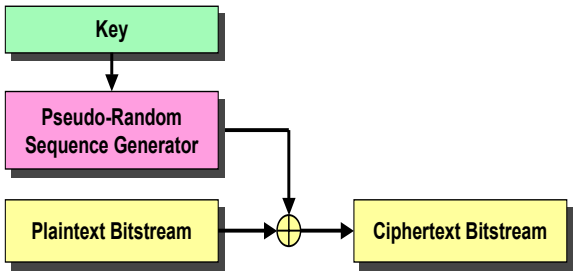


- Same key used for encryption and decryption
- Key must be kept absolutely secret
- Same key can be used for several messages, but should be changed periodically → secure key distribution problem!

CIFRADO EN BLOQUE



CIFRADO EN FLUJO



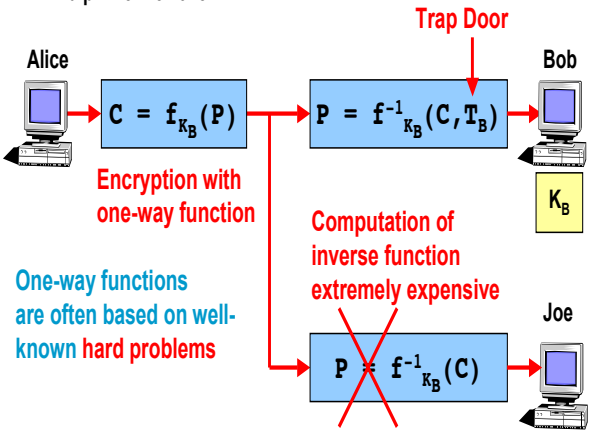
Plaintext Stream	1 1 1 1 1 1 1 1 0 0 0 0 0 0 …
Pseudo-Random Stream	1 0 0 1 1 0 1 0 1 1 0 1 0 0 …
Ciphertext Stream	0 1 1 0 0 1 0 1 1 1 0 1 0 0 …

SISTEMAS DE CLAVE PÚBLICA

- Step 1: Choose two random large prime numbers p and q
  - For maximum security, choose p and q of about equal length, e.g. 512-1024 bits each.
- Step 2: Compute the product $n = p \cdot q$
- Step 3: Choose a random integer $e < (p-1)(q-1)$
  - The numbers e and $(p-1)(q-1)$ must be relatively prime, i.e. they should not share common prime factors.
- Step 4: Compute the unique inverse $d = e^{-1} \bmod (p-1)(q-1)$
  - The equation $d \cdot e \bmod (p-1)(q-1) = 1$ can be solved using the Euclidian algorithm.

CIFRADO DIFFIE-HELLMAN

- The Inventors
  - Whitfield Diffie and Martin Hellman 1976
  - Ralph Merkle 1978



FACTORIZACIÓN Y PRIMALIDAD

- There are 10^{151} primes 512 bits in length or less.
- There are only 10^{77} atoms in the universe.
- The chance that two people choose the same prime factors for key generation is therefore near to nil !
- To prove that a randomly chosen number is really prime you would have to factor it. Try small factors (3, 5, 7, 11, ...)
- Probabilistic Primality Tests (e.g. Rabin-Miller)

Result of Primality Test	not prime	is prime	random number is a
	100 %	0.1 %	composite number
	0 %	99.9 %	prime number

- After passing 5 tests, assume a random number to be prime