RECURSOS PEDAGÓGICOS PARA UN PRIMER ACERCAMIENTO A LA CRIPTOLOGÍA.

Rosalía Peña[1], Juan José Escribano[2]

[1] *Departamento C.C. de la Computación (Universidad de Alcalá de Henares)*
e-mail: ccrpr@cc.alcala.es

[2] *CEES. (Centro de Estudios Europeos Superiores de Madrid)*
e-mail: jje@dpris.esi.uem.es

Resumen: Se presenta un conjunto de herramientas pedagógicas para proporcionar una visión general de la Criptología actual de forma atractiva y concisa, minimizando el tiempo de docencia requerido.

1.- INTRODUCCIÓN.

Todas las civilizaciones han mostrado una preocupación común por proteger la información valiosa de accesos no deseados. El arte y la ciencia de almacenar y/o transmitir información confidencial, y su contrapartida de desvelar información cifrada se llama criptología.

Cada vez resulta más indiscutible el papel de la información en la evolución de nuestro sistema, por ello continuamente se mejora la tecnología que facilita su almacenamiento y las redes de ordenadores que permiten la comunicación de la información, pero estos nuevos desarrollos tecnológicos dificultan la confidencialidad; lo que implica la necesidad de un crecimiento paralelo de las herramientas que sirven para preservar la información de accesos (lecturas y/o modificaciones) no deseados. De hecho la criptología está cobrando gran interés y, en los últimos años, surgen nuevas publicaciones tanto en ingles como en español y está siendo incorporada en los curricula de los estudios universitarios de informática, aunque frecuentemente como una materia optativa. De modo que muchos alumnos

finalizan sus estudios sin haber tenido ningún contacto con esta rama de la informática.

Los temarios de cualquier materia están siempre cargados, los estudios de informática no son una excepción y resulta difícil encontrar un hueco para realizar un acercamiento a la criptología sin perjudicar los contenidos de otras materias.

Incluso la propia criptología es tan densa que, a pesar de lo interesante que resulta apreciar cómo determinados sucesos relacionados con la criptología han condicionado el devenir de la Historia de la humanidad, algunos autores proponen la conveniencia de eliminar del temario una revisión de los métodos de cifrado clásicos para adentrarse directamente en el estudio de los métodos de cifrado por ordenador (Scneier1994, Pastor 1998, Fúster1997) mientras otros se extienden en ella (Pino1996, Sgarro 1989).

Se presentan recursos pedagógicos para mostrar las bases de la criptología moderna de forma breve, concisa y atractiva, de modo que con una hora de dedicación, el alumno pueda hacerse una idea del papel, la importancia actual de esta rama de la informática y los mecanismos en que está basada.

Esta sesión de docencia podría ser impartida en horas de la asignatura de Bases de datos o en la de Redes de ordenadores, ambas troncales, de modo que la materia se presenta a todos los alumnos. Estos recursos pueden emplearse también para proporcionar una visión global de la materia en una asignatura específica de criptología, sirviendo como marco de referencia para posteriores desarrollos.

La primera necesidad pedagógica es ubicar el problema que se pretende resolver y apuntar los mecanismos disponibles para atajarlo. Para ello pueden servir las dos primeras transparencias que adjuntamos, indicando que nos vamos a centrar en las herramientas técnicas de protección de la información. La tercera transparencia acerca al alumno al vocabulario básico.

RED = ~~Mundo virtual~~

MUNDO REAL
Documentos reales

⇓ Problemas reales

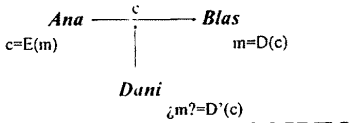
Necesitan PROTECCION
® Técnica
® Legal
® Ética

Transparencia 1: Necesidad de la Criptología

1er Problema

* La red llega a "todas partes"
* Susceptible de "pinchar"

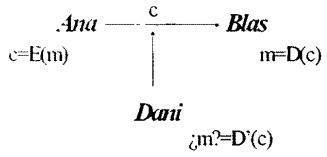
1ª Solución: Que no viaje m sino.....c



CRIPTOLOGÍA

Transparencia 2: Solución

Vocabulario

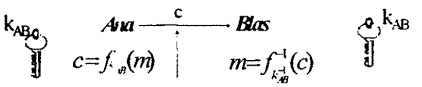


* m : texto en claro
* c : criptograma, texto cifrado
* E : cifrar, encriptar
* D : descriptar, descifrar
* D': criptanalizar

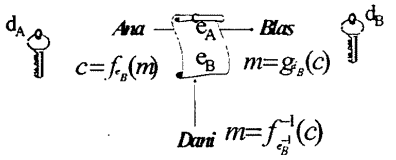
Transparencia 3: Vocabulario

Clasificación

CLAVE SECRETA



CLAVE PÚBLICA



Transparencia 4: Clasificación

Los algoritmos en que está basada la criptología actual pueden clasificarse en dos grupos: simétrica o de clave privada y asimética o de clave pública.

2.- CRIPTOLOGÍA DE CLAVE SIMÉTRICA.

Los métodos de clave simétrica incluyen dos operaciones fundamentales: Sustitución (cambio de unos caracteres por otros) y Transposición (cambio de posición de los caracteres). Para ejemplificar cada operación elemental empleamos un cifrador. Para la sustitución hemos construido un cifrador del estilo de los discos de Alberty, compuesto por dos discos concéntricos divididos en 27 partes iguales, cada una etiquetada con una letra A,...,Z. Los discos giran uno sobre el otro. Cifrar en clave D, supone irar el disco interior hasta que su D este en la posición de la A del exterior, y construir el criptograma leyendo en el interior las letras que corresponden a las del texto en claro en el exterior (ver figura 1).

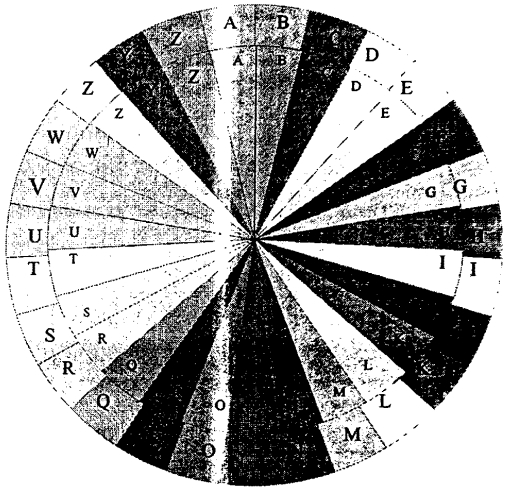


Figura 1: Discos de Alberty. Sustitución

El mismo cifrado podría obtenerse con la siguiente fórmula

$$ci = S[P(m_i) + P(k) - 1]_{mod\ 27} \quad (1)$$

donde mi es cada una de las letras del texto en claro, ci la correspondiente cifrada, k es la clave de cifrado y P(m) es la posición de la letra en un alfabeto de 27 caracteres y S[p] es el símbolo que corresponde a una posición.

Para ejemplificar la operación básica de transposición hemos construido un cifrador basado en la scitala espartana. Un listón de madera con una púa en un extremo, que permite fijar una cinta, para enrollarla sobre el listón. Con la cinta enrollada se escribe el mensaje, una vez desenrollada la cinta, es difícil de leer el texto. Ver Figura 2.

Estos cifradores requieren muy poco tiempo de preparación para el profesor, y son palpables, por lo que resultan muy gráficos al alumno.

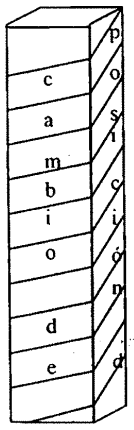


Figura 2. Scitala espartana: Cambio posición

Una vez comprendidas las operaciones fundamentales, es fácil entender cómo en el ordenador transforma un grupo de 8 letras (por ejemplo) es decir 64 bit, por otras 8 distintas, tras haber sumado (XOR) los bit de la clave con los del mensaje y haber cambiado de posición los bits resultantes.

3.- CRIPTOGRAFÍA DE CLAVE ASIMÉTRICA.

La criptología de clave asimétrica se basa en la existencia de funciones unidireccionales con trampa. En este caso, la dificultad es entender que se va a tomar ventaja del diferente consumo de recursos de una operación y su inversa.

Para comprender las propiedades de este tipo de funciones proponemos a los alumnos realizar unos sencillos cálculos. Todos los alumnos saben multiplicar dos números, factorizar y resolver sencillos sistemas de ecuaciones. Para garantizar que la memoria no juegue una mala pasada, se puede factorizar un número sencillo con todos ellos y plantear y resolver una ecuación similar a la que se va a proponer después. Se divide a los alumnos en dos grupos, por ejemplo, el de la derecha va a multiplicar dos números, mientras que el de la izquierda va a realizar la operación inversa. Los de la última fila de la izquierda factorizarán sabiendo una propiedad de

los factores que permite determinarlos univocamente. Al menos un alumno de cada grupo dispone de calculadora. Se les entrega un papel bocaabajo en el que se solicita la operación asignada, rogándoles lo vuelvan todos a la vez y se pongan de pie cuando hayan terminado sus cálculos.

El contenido de las instrucciones será por ejemplo:
Derecha: Multiplica 373*379
Izquierda: Factoriza 141367
Izquierda última fila: Factoriza 141367 sabiendo que uno de los factores es 6 unidades mayor que el otro. Es decir 141367=x(x+6).

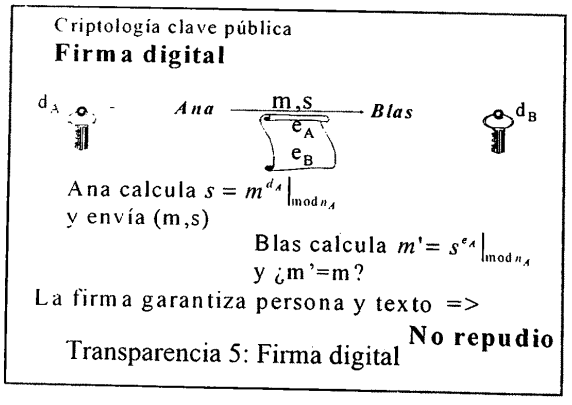
Previsiblemente el profesor podrá interrumpir el proceso cuando hayan terminado muchos del primer grupo y sólo algunos del tercero.

Todos los alumnos están capacitados para resolver cualquiera de las tres solicitudes, sin embargo estas requieren diferentes recursos (tiempo o mejor calculadora). En criptografía pública la seguridad del criptograma es el costo de los recursos para calcular la función inversa. El mensaje dentro de un tiempo determinado será legible a todos, si ese tiempo es mayor que el necesario de confidencialidad, el mensaje está seguro.

4.- GESTIÓN DE CLAVES.

El resto de la sesión se utilizará para apuntar las diferencias en cuanto a seguridad y distribución de las claves en ambos tipos de criptografía, apoyándonos en la trasparencia 4.

5.- FIRMA DIGITAL.



Transparencia 5: Firma digital

El concepto de firma digital es muy importante y realmente llamativo. Dependiendo de cómo haya funcionado la dinámica de la clase puede dar tiempo, o no, a explicarlo apoyándonos en la transparencia 5.

6.- BIBLIOGRAFIA.

B.Schneier. *Applied cryptography. Protocols, Algoritms and Source code in* C.J.Wiley & Sons,Inc. EEUU 1994. ISBN:0-471-59756-2

Pino Caballero. *Introducción a la Criptografía.* Editorial RA-MA 1996. ISBN84-7897-210-2

A. Fúster, D. de la Guía, L. Hernández, F. Montoya, J. Muñoz, Técnicas Criptográficas de protección de datos. Ra-ma 1997 ISBN: 84-7897-288-9

A.Sgarro; Códigos secretos. Piramide. 1989, ISBN:84-368-0525-9.
José Pastor y Miguel Angel Sarasa López; Criptografía Digital: Fundamentos y Aplicaciones. isbn:84-7733-491-9. Prensas Universitarias de Zaragoza (1998).