LISTADO DE TRABAJOS

CRIPTOGRAFÍA

CURSO 2010/11

1. **Correo electrónico certificado**.

   Se trata de explicar algunas características del correo certificado electrónico que vienen descritas en el documento de referencia.

   Referencias:
   J. Ferrer-Gomilla, J. Onieva, M. Payeras, J. López. Certified electronic mail: Propierties revisited. Computer & Securetiy 29 (2010) 169-179.

2. **Tarjetas de crédito virtuales**

   Las tarjetas de crédito virtuales son una herramienta para aportar seguridad al comercio electrónico. En este trabajo se debe explicar un esquema tarjeta de créditos virtuales con numeración dinámica que viene explicado en el artículo de referencia.

   Referencias:
   I.Molloy, J. Li, N. Li. Dynamic Virtual Credit Card Numbers. LNCS 4886 (2007) 208-223.

3. **Un protocolo de intercambio de claves basado en teoría del caos**

   Se trata de explicar un protocolo de intercambio de claves basado en funciones caóticas que viene descrito en el artículo de la bibliografía. Una implementación del mismo sería muy bien valorada.

   Referencias:
   X. Wang, J. Zhao. An improved key agreement protocol based on chaos. Commun Nonlinear Sci Numer Simulat 15 (2010) 4052-4057.

4. **Identificación forense y extracción de claves criptográficas**

   En el escenario de un delito digital, el recuperar las claves con la que aparecen cifradas las evidencias es una necesidad imperiosa. En este trabajo, se debe exponer las aportaciones que se dan en este sentido en el artículo de referencia.

   Referencias:
   C. Maartmann-Moe, S. Thorkildsen, A. Arnes. The persistence of memory: Forensic identification and extraction of cryptographic keys. Digital Investigation 6 (2009) 134-140.

5. **Algoritmos de cifrado de vídeo**

   Cada vez es más común el uso del vídeo en las comunicaciones digitales. En este trabajo se deben explicar una serie de algoritmos de cifrado de vídeo que vienen recogidos en el artículo de referencia.

   Referencias:
   F. Liu, H. Koenig. A survey of video encryption algorithms. Computer $ Security 29 (2010) 3-15.

6. **Un algoritmo para cifrar imágenes basado en funciones caóticas**

   Se trata de explicar un método de cifrado para imágenes basado en teoría del caos. Una implementación del método sería muy bien valorada. El método viene descrito en el artículo de referencia.

   Referencias:
   M. Amin, O. Faragallah, A. Abb El-Latif. A chaotic block cipher algorithm for image cryptosystems. Commun Nonlinear Sci Numer Simulat 15 (2010) 3484-3497.

7. **PGP**
   Pretty Good Privacy o PGP (privacidad bastante buena) es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales. En este trabajo se hará un informe del estado **actual** de PGP y de las ventajas e inconvenientes sobre otros sistemas. Una demostración de su uso es recomendable.

   Referencias:
   http://es.wikipedia.org/wiki/Pretty_Good_Privacy

8. Hacking con Google

Google es la herramienta de búsqueda en Internet más potente y versátil de la actualidad. En manos de los atacantes, Google puede descubrir vulnerabilidades, revelar información confidencial, servir de cabeza de puente para perpetrar ataques, sacar a la luz servicios de red y encontrar contraseñas, convirtiéndose así en una de las herramientas más temibles de la Red.

Referencias:

http://www.criptored.upm.es/guiateoria/gt_m063a.htm

Hacking con Google, *Johny Long*, Anaya multimedia.

9. Un criptosistema para imágenes a color

Se trata de implementar un método para cifrar y descifrar imágenes a color usando funciones caóticas. El método viene explicado en el documento de referencia.

Referencias:

OCML-based colour image encryption. R. Rhouma, S. Meherzi and S. Belghith. Chaos, Solitons & Fractals xxx (2007).

10. Una versión del criptosistema de la mochila

Se trata de realizar una implementación del criptosistema descrito en en el artículo de refencia basado en una novedosa versión del problema de la mochila.

Referencias:

A knapsack-based probabilistic encryption scheme. B. Wang, Q. Wu and Y. Hu. Information Sciences 177 (2007) 3981-3994.

11. Un cifrado para el formato MPEG

Se trata de explicar un cifrado para vídeo en formato MPEG. Toda aportación que se haga en la dirección de una implementación del método será muy bien valorada.

Referencias:

A Selective Video Encryption Scheme for MPEG Compression. G. Liu, T. Ikenaga, S. Goto, T. Baka. IEICE Trans. Fundamentals, Vol.E89-A, NO.1 2006

12. Intercambio cuántico de claves BB84

Este protocolo se publicó en 1984 por Charles Bennet y Gilles Brassard y con él se produce el nacimiento de la Criptografía Cuántica. En este protocolo la transmisión se logra utilizando los fotones polarizados enviados entre el emisor y el receptor mediante un canal cuántico, por ejemplo una fibra óptica.

Referencias:

http://scholar.google.es/scholar?q=Quantum+cryptography:+public+key+distribution+and+coin+tossing&hl=es&as_sdt=0&as_vis=1&oi=scholart
http://en.wikipedia.org/wiki/BB84

13. Ocultar datos en imágenes con compresión

La esteganografía es la ciencia en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos dentro de otros, llamados portadores (cubierta), de modo que no se perciba su existencia.

En las imágenes es posible obtener unos porcentajes altos de compresión sin mucha pérdida de calidad aparente debido a su alto grado de redundancia (es decir, la existencia de información cuya desaparición no altera esencialmente el mensaje). En este trabajo se estudiarán e implementarán distintos métodos, así como se desarrollará un análisis de la fortaleza de los métodos.

Referencias:

http://www.docstoc.com/docs/6267030/Steganography

14. Ocultar datos en archivos de sonido

La esteganografía es la ciencia en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos dentro de otros, llamados portadores (cubierta), de modo que no se perciba su existencia.

Los archivos con sonido digital presentan peculiaridades que requieren métodos específicos. En este trabajo se estudiarán e implementarán distintos métodos, así como se desarrollará un análisis de la fortaleza de los métodos.

Referencias:

http://herkules.oulu.fi/isbn9514273842/isbn9514273842.pdf

15. Detección para sistemas esteganográficos

La esteganografía es la ciencia en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos dentro de otros, llamados portadores (cubierta), de modo que no se perciba su existencia.

En este trabajo se estudiarán los principales métodos para hacer su análisis (estegoanálisis) y obtener los mensajes ocultos.

Referencias:

http://www.jjtc.com/Steganalysis/