Universidad Politécnica de Cartagena

Escuela Técnica Superior de Ingeniería de Telecomunicación

SEGURIDAD EN REDES DE COMUNICACIONES

Práctica 1: Comparativa de métodos de cifrado en comunicaciones inalámbricas

María Dolores Cano Baños

Natalio López Martínez

Objetivos

- Deducir a través de la experimentación la rapidez de ejecución de los algoritmos de cifrado y la carga de procesado que conllevan en las conexiones inalámbricas.

Desarrollo de la práctica

- Cada grupo de dos personas, deberá crear un programa de cifrado (opcionalmente descifrado) que incluya al menos un algoritmo simétrico y otro asimétrico que permite la transmisión de un archivo de forma confidencial a través de una enlace inalámbrico (WLAN, 3G o Bluetooth):
  - Algoritmos simétricos (3DES, AES, etc.)
  - Algoritmos asimétricos (RSA, DSA, ECC, etc.)
- Cada grupo tendrá que enviar un correo electrónico semanal (martes por la tarde) a mdolores.cano@upct.es con los avances que se han hecho durante la semana en el desarrollo de la práctica.
  - Fase 1 (2 semanas): selección de dispositivo y tecnología inalámbrica a emplear para el estudio. Búsqueda de códigos libres abiertos en Internet que faciliten la labor a desarrollar.
  - Fase 2 (2 semanas): selección e implementación de los algoritmos de cifrado (opcionalmente descifrado) a comparar. Búsqueda de códigos libres abiertos en Internet que faciliten la labor a desarrollar.
  - Fase 3 (1 semana): realización de pruebas, obtención de resultados y análisis de resultados.
- Cada grupo deberá extraer sus propias conclusiones (por ejemplo, sobre los tiempos de ejecución, uso de CPU, etc.) justificados con los resultados obtenidos.
- Con fecha límite el martes 10/05/2011 a las 19h hay que entregar por correo electrónico mdolores.cano@upct.es lo siguiente:
  - Copia del código fuente del programa
  - Breve *howto* del programa
  - Conclusiones (máximo 2 páginas)