Práctico 4: Criptografía

Entrega. Se deberán entregar resueltos los ejercicios ??. Tener en cuenta que la presentación de los mismos será evaluada.

1. Usualmente se dice que el método *one-time-pad* es un método irrompible. Piense un posible ataque para one-time-pad teniendo dos textos de la misma longitud cifrados con la misma clave. Si consigue un ataque exitoso, ¿cómo puede ser entonces que el método sea clasificado usualmente como "irrompible"?

2. ¿Cuál es la diferencia entre los modos de operación ECB y CBC? ¿Cuál recomendaría para encriptar el contenido de una imagen en forma de mapa de bits?

3. Resolver el challenge 8 de Matasano.

4. Las claves de DES son cortas para los requerimientos actuales. Una posibilidad es tener dos claves k_1 y k_2, y encriptar el mensaje usando primero k_1, y luego encriptar el resultado usando k_2. Proponga cómo funcionaría la desencriptación. ¿Qué vulnerabilidades puede tener este esquema, asumiendo que el atacante tiene mucha memoria disponible?

5. Explicar cómo funciona la mejora 3DES para DES. Explicar por qué esta alternativa no tiene los problemas del esquema visto en el ejercicio anterior.

6. Si se desea encriptar un archivo de 1M. ¿Cómo utilizaría RSA para encriptarlo?

7. Suponga que Alice y Bob tienen claves RSA públicas guardadas en un servidor. Ellos se comunican regularmente usando mensajes autenticados y confidenciales. Eve desea leer los mensajes, pero no puede crackear las claves RSA privadas de ninguno de ellos. Sin embargo, Eve puede hackear el servidor y alterar los archivos donde se guardan las claves públicas de Alice y Bob.

1. ¿Cómo debería alterar el archivo Eve de manera que pueda leer los mensajes confidenciales entre Alice y Bob, y simular mensajes de ambos?

2. ¿Cómo podría Alice y/o Bob darse cuenta de la modificación de las claves públicas?