Criptografía y seguridad
Tarea 3

Andrea Itzel González Vargas
Carlos Gerardo Acosta Hernández

Entrega: 27/03/17
Facultad de Ciencias UNAM

1. Con tus propias palabras explica por qué el siguiente esquema de cifrado para mensajes de tamaño ℓ(n) es seguro:
Sea G un generador seudoaleatorio con factor de expansión ℓ(n). El algoritmo Gen, con entrada n, devuelve una clave k escogida uniformemente del conjunto $\{0, 1\}^n$. El algoritmo de cifrado Enc recibe como entradas una clave k de tamaño n y un mensaje m de tamaño ℓ(n) y devuelve el mensaje cifrado c = G(k) $\oplus$ m. Para descifrar se calcula m = G(k) $\oplus$ c.

2. Supongamos que Alicia y Bartolo se quieren mandar mensajes cifrados y solo tienen una clave k de 128 bits que ambos conocen. Para mandar un mensaje m hacen lo siguiente:

- Se elige una cadena aleatoria s de 80 bits.
- Se obtiene el mensaje cifrado c = RC4(s $\|$ k) $\oplus$ m.
- Se manda la pareja (s, c).

a) Si Alicia manda un mensaje (s, c), ¿qué tiene que hacer Bartolo para recuperar el mensaje claro?

b) Si un adversario puede ver una lista de mensajes (s_1, c_1), (s_2, c_2), . . . que fueron enviados entre Alicia y Bartolo, ¿cómo puede comprobar que se usó el mismo flujo de claves para cifrar dos mensajes? (Flujo de claves es la salida de RC4.)

c) Usando la paradoja del cumpleaños, ¿aproximadamente cuántos mensajes tendría que enviar Alicia para que se repita un flujo de claves?

3. Explica qué es una función seudoaleatoria y qué relación tiene con los algoritmos de cifrado por bloques.

4. En el cifrado por bloques los errores se propagan de manera distinta dependiendo del modo de operación que se utilice. Explica qué ocurre en el mensaje descifrado cuando se usan los modos ECB, CBC, OFB y CTR, si el texto cifrado contiene un error de un solo bit.

5. Para usar un cifrado por bloques de tamaño n es necesario que el mensaje tenga longitud múltiplo de n, así que se agrega un padding cuando hace falta. Si se establece que se usará alguna forma de padding (por ejemplo, agregar un uno seguido de ceros), ¿por qué es necesario agregar padding aun en los mensajes de tamaño múltiplo de n?