Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Criptografía

Ejercicios prácticas autodirigidas. Bloque 2. Cifrado Simétrico.

---

1. Demuestra que si $a > 1$, la función $f(x) = a^{-x}$ definida de $\mathbb{N}$ en $\mathbb{R}^+$ es despreciable.

2. Escribe el proceso de cifrado y cifrado completo de un cifrador en bloque en modo CBC.

3. Llamamos ataque de maleabilidad a aquel en el que el adversario construye un cifrado C válido modificando un cifrado legítimo, de manera que controle la variación asociada en el texto claro subyacente. Los modos OFB y CTR son vulnerables a este tipo de ataques: comprúebalo. [1]

4. Sea E un cifrador en bloque que usaremos en modo OFB. Supongamos que no actualiza la semilla IV, es decir, el bloque C_0 es fijo. Demuestra que un adversario que conozca un par (M, C) construido con una clave K, puede construir un cifrado C' asociado a un mensaje $M' \neq M$ con la misma clave K (sin conocer ésta).

5. Descifrado de una red de Feistel. Considera una red de Feistel donde operamos con una secuencia de clave $K_0, \ldots, K_{n-1}$ y el cifrado se construye como vimos en la presentación de esta unidad, esto es: el texto inicial está dividido en parte izquierda y derecha L_0, R_0, y para $j = 1, \ldots, n$ hacemos:

$$L_j := R_{j-1}$$
$$R_j := L_{j-1} \oplus f(R_{j-1}, K_{j-1}).$$

   Output: (R_n, L_n)

   Explica el proceso de descifrado.

[1] el modo CBC también lo es, si bien es algo más complicado verlo...puedes intentarlo considerando dos bloques de cifrado c_i, c_{i-1}como tu texto objetivo