CC5301-1 Introducción a la Criptografía Moderna
Profesor: Alejandro Hevia A.
Auxiliar: Bryan Ortiz
Estudiante: Andrés Calderón Guardia

Tarea 1

CP, Cifradores de Bloque y PRF

P1. 2-SDES

Considerando el cifrador 2-SDES, tomaremos dos mensajes iniciales m y m', tal que m' es igual a m excepto que su primer bit está invertido. Teniendo esto en cuenta, tras la permutación inicial el bit invertido estará en una de las dos mitades utilizadas para la primera ronda de Feistel.

Entonces analicemos el valor de las dos mitades tras cada ronda para el mensaje m:

$$L_1 = R_0, \quad R_1 = L_0 \oplus f(R_0, K_1)$$

$$L_2 = R_1, \quad R_2 = L_1 \oplus f(R_1, K_2)$$

$$\Rightarrow L_2 = L_0 \oplus f(R_0, K_1), \quad R_2 = R_0 \oplus f(L_0 \oplus f(R_0, K_1), K_2)$$

Y en el caso particular en que para m' el bit acaba en la primera mitad tras la permutación se obtiene:

$$\Rightarrow {L_2}' = {L_0}' \oplus f(R_0, K_1), \quad {R_2}' = R_0 \oplus f({L_0}' \oplus f(R_0, K_1), K_2)$$

Con esto, notemos que como el bit invertido acaba en alguna posición de la mitad izquierda tras la permutación inicial, digamos el segundo índice sin pérdida de generalidad, entonces ${L_2}'$ tiene solamente su segundo bit cambiado, y de esto podemos decir entonces que el segundo bit del preoutput fue invertido con seguridad.

Finalmente, dado que se aplica la permutación inversa, en este caso el segundo bit terminará en la primera posición del output final, dado que asumimos que el primer bit terminó en la segunda posición tras la permutación inicial, y así, este algoritmo hizo que este bit se invirtiera respecto a la salida original (es decir, que si consideramos c y c' como los textos cifrados de m y m' respectivamente, estos tendrán el primer bit distinto con toda seguridad).

Un detalle es que el preoutput tendrá su lado derecho bastante cambiado dado que se cambió un bit en la entrada que recibe la función f, lo cual finalmente resulta en que habrán a lo más la mitad más uno de bits cambiados en el output final, pero este comportamiento no será necesario tenerlo en cuenta para el algoritmo final.

Adicionalmente, el análisis hecho es análogo en caso de que la permutación inicial mueva el bit invertido al lado derecho, y también se puede generalizar este comportamiento si invertimos un solo bit en cualquier posición de m, esto ya que independientemente del lugar en que quede el bit invertido, la permutación inversa lo devolverá a su posición original.

De esta forma, creamos el adversario A de la siguiente forma:

```
Adversario A:
    m ← {0,1}^64
    c ← 2-SDES(m)
    for i = 1, ..., 64:
        m' ← m
        m'[i] ← ¬m'[i]
        c' ← 2-SDES(m')
        if m[i] == m'[i]:
            return False
    return True
```

Este algoritmo lo que busca es hacer una verificación por cada posición del mensaje, de forma que si el bit en esa respectiva posición son iguales, quiere decir que estamos en el mundo aleatorio, ya que con 2-SDES se garantiza que este se debe haber invertido, por lo que si para los 64 bits siempre fueron distintos entonces estamos en el mundo real, de modo que se tiene:

$$\Pr\left[\text{Real}^{A}_{\text{2-SDES}} \Rightarrow \text{True}\right] = 1$$

Y si, en cambio, se estuviese en el mundo aleatorio, entonces para los 64 bits se tendría que haber elegido al azar justamente el bit invertido en cada posición, por lo que la probabilidad resultante es:

$$\Pr\left[\text{Aleat}^{A}_{\text{Rec(2-SDES)}} \Rightarrow \text{True}\right] = \frac{1}{2^{64}}$$

Con lo cual finalmente se obtiene la ventaja:

$$\text{Adv}^{\text{prf}}_{\text{2-SDES}} = |\Pr\left[\text{Real}^{A}_{\text{2-SDES}} \Rightarrow \text{True}\right] - \Pr[\text{Aleat}^{A}_{\text{Rec(2-SDES)}}| = 1 - 2^{-64}$$

Así que se concluye que 2-SDES no es PRF segura.

Por último, el número de consultas que se le realizan al oráculo son 65, una para determinar el mensaje cifrado del mensaje original, y las otras 64 para obtener un mensaje cifrado por cada posición disponible, de forma que a su vez el tiempo estimado de ejecución sería del orden de $O(\text{S-DES}) + O(k)$, con k constante, puesto que la mayoría del tiempo utilizado por el adversario se va en realizar las llamadas al oráculo, con un tiempo adicional pero de un orden constante para realizar el resto de instrucciones.

P2. Función E'_K

Para este caso asumiremos que E'_K es PRF, por lo que para demostrarlo razonaremos por contradicción, es decir, supondremos que E'_K no es PRF. Esto implica que existe un adversario $A_{E'_K}$ tal que $\mathrm{Adv}^{\mathrm{prf}}_{E'_K}\left(A_{E'_K}\right)$ es significativa.

Construiremos entonces un adversario $A_{E'_K}$ tal que $\mathrm{Adv}^{\mathrm{prf}}_{E'_K}\left(A_{E'_K}\right)$ también sea significativa, lo cual nos va a generar una contradicción, dado que nuestro supuesto es que E_K sí es PRF segura.

```
Adversario A_{E_K}:
    x ← {0,1}^n
    x' ← {0,1}^n
    c_0 ← E_K(x ⊕ x')
    c_1 ← E_K(x ⊕ x̄')
    res ← A_{E'_K}(c_0 ‖ c_1)
    return res
```

Notemos que:

$$\Pr\left[\mathrm{Real}^{A_{E_K}}_{E_K} \Rightarrow \mathrm{True}\right] = \Pr\left[\mathrm{Real}^{A_{E'_K}}_{E'_K} \Rightarrow \mathrm{True}\right]$$

Esto puesto que en el mundo real A_{E_K} simula perfectamente el oráculo de E'_K, entregando de forma exacta lo que entregaría este. En consecuencia, la probabilidad de que A_{E_K} adivine que está en el mundo real es la misma que la de $A_{E'_K}$.

Por otro lado, también se tiene que:

$$\Pr\left[\mathrm{Aleat}^{A_{E_K}}_{\mathrm{Rec}(E_K)} \Rightarrow \mathrm{True}\right] = \Pr\left[\mathrm{Aleat}^{A_{E'_K}}_{\mathrm{Rec}(E'_K)} \Rightarrow \mathrm{True}\right]$$

Pues, tanto c_0 y c_1 son uniformes e independientes, ya que $x \oplus x'$ es diferente de $x \oplus \overline{x'}$) y asumimos que E_K sí es PRF, resultando en que lo entregado a $A_{E'_K}$ es también perfectamente aleatorio en $\mathrm{Rec}(E'_K)$.

Finalmente se tiene que:

$$\begin{aligned}
\mathrm{Adv}^{\mathrm{prf}}_{E_K}\left(A_{E_K}\right) &= |\Pr\left[\mathrm{Real}^{A_{E_K}}_{E_K} \Rightarrow \mathrm{True}\right] - \Pr\left[\mathrm{Aleat}^{A_{E_K}}_{\mathrm{Rec}(E_K)} \Rightarrow \mathrm{True}\right]| \\
&= |\Pr\left[\mathrm{Real}^{A_{E'_K}}_{E'_K} \Rightarrow \mathrm{True}\right] - \Pr\left[\mathrm{Aleat}^{A_{E'_K}}_{\mathrm{Rec}(E'_K)} \Rightarrow \mathrm{True}\right]| \\
&= \mathrm{Adv}^{\mathrm{prf}}_{E'_K}\left(A_{E'_K}\right)
\end{aligned}$$

Con esto llegamos a que la ventaja de A_{E_K} es idéntica a la de $A_{E'_K}$, pero esta última supusimos que es significativa, lo cual se contradice con la hipótesis inicial, de forma que se genera la contradicción, y por ende, se concluye que si E_K es PRF segura, entonces E'_K también lo es.