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

Tarea 2

Encriptación Simétrica

P1. Esquema de encriptación H

a) Definimos el algoritmo de desencriptación como sigue a continuación:

Algoritmo $\mathrm{Dec}_K(C)$:
  $R \| M \leftarrow F_K^{-1}(C)$
  return M

Este algoritmo tiene el requisito de desencriptación ya que para un mensaje encriptado C arbitrario utiliza la función inversa de F_K, con ello obtiene $R \| M$, para finalmente retornar el mensaje original M.

b) Para realizar esta demostración usaremos contradicción, es decir, tendremos F una PRF segura y asumiremos que H no es IND-CPA segura, de modo que llegaremos a que existe un adversario A tal que posee ventaja significativa contra F, lo cual es contradictorio puesto que asumimos que esta es una PRF segura.

Dado que H no es IND-CPA seguro implica que posee un adversario B contra H tal que posee una ventaja $\mathrm{Adv}_H^{\text{ind-cpa}}(B)$ significativa. Entonces, a partir de este adversario crearemos al adversario A del tipo PRF, que cuenta con un oráculo $F_n(\cdot)$, el cual recibe un mensaje. En el mundo real A encripta usando F_K y en el ideal retorna un valor totalmente aleatorio de largo n. Con ello, el adversario opera como se muestra a continuación:

Adversario $A^{F_n(\cdot)}()$:
  $b \xleftarrow{\$} \{0,1\}$
  while $B^{\mathrm{LR}(\cdot,\cdot,b)}$ haga consultas:
    $R \xleftarrow{\$} \{0,1\}^{\frac{n}{2}}$
    $(M_0, M_1) \leftarrow B^{\mathrm{LR}(\cdot,\cdot,b)}$
    $C \leftarrow F_n(R \| M_b)$
    $C \rightarrow B^{\mathrm{LR}(\cdot,\cdot,b)}$
  $b' \leftarrow B^{\mathrm{LR}(\cdot,\cdot,b)}$
  if $b' = b$:
    return 1
  return 0

Ahora analizaremos la ventaja de este adversario por cada mundo, partiendo con el real:

$$
\begin{aligned}
\Pr\left[\mathrm{Real}_H^A \Rightarrow 1\right] &= \Pr[B \text{ responda correctamente} \mid Fn = E_K] \\
&= \Pr\left[B^{\mathrm{LR}(\cdot,\cdot,b)} \to b\right] \\
&= \Pr\left[B^{\mathrm{Enc}_K(\cdot)} \to b\right] \\
&= \Pr\left[B^{\mathrm{Enc}_K(\cdot)} \to b \mid b = 0\right] \cdot \Pr[b=0] + \Pr\left[B^{\mathrm{Enc}_K(\cdot)} \to b \mid b = 1\right] \cdot \Pr[b=1] \\
&= \frac{1}{2}\left(\Pr\left[B^{\mathrm{Enc}_K(\cdot)} \to b \mid b = 0\right] + \Pr\left[B^{\mathrm{Enc}_K(\cdot)} \to b \mid b = 1\right]\right) \\
&= \frac{1}{2}\left(\Pr\left[\mathrm{Izq}_F^B \Rightarrow 0\right] + \Pr\left[\mathrm{Der}_F^B \Rightarrow 1\right]\right) \\
&= \frac{1}{2}\left(1 - \Pr\left[\mathrm{Izq}_F^B \Rightarrow 1\right] + \Pr\left[\mathrm{Der}_F^B \Rightarrow 1\right]\right) \\
&= \frac{1}{2}\left(1 + \mathrm{Adv}_H^{\text{ind-cpa}}(B)\right)
\end{aligned}
$$

En cambio para el mundo ideal, el adversario B no posee ninguna ventaja contra un oráculo que entrega resultados totalmente aleatorios, de modo que se obtiene $\Pr[\mathrm{Aleat}_H \Rightarrow 1] = \frac{1}{2}$. Con esto podemos concluir que la ventaja del adversario A viene dada por la siguiente expresión:

$$
\begin{aligned}
\mathrm{Adv}_H^{\mathrm{PRF}}(A) &= \left|\Pr\left[\mathrm{Real}_H^A \Rightarrow 1\right] - \Pr[\mathrm{Aleat}_H \Rightarrow 1]\ \right| \\
&= \left|\ \frac{1}{2}\left(1 + \mathrm{Adv}_H^{\text{ind-cpa}}(B)\right) - \frac{1}{2}\ \right| \\
&\geq \frac{1}{2}\mathrm{Adv}_H^{\text{ind-cpa}}(B)
\end{aligned}
$$

Como consideramos que la ventaja de B es significativa, esto implica que la ventaja de A sobre F también lo es bajo los supuestos hechos, pero esto genera una contradicción ya que tomamos a F como una PRF segura.

De este modo, concluimos que si F es PRF segura entonces H es IND-CPA.

P2. REPCTXT

Procederemos por contradicción para realizar la demostración, es decir, asumiremos que existe un adversario B tal que posee una ventaja $\mathrm{Adv}_{\mathcal{SE}}^{\mathrm{REPCTXT}}(B)$ significativa, y llegaremos a que $\mathcal{SE}$ no es IND-CPA seguro.

Dado que $\mathcal{SE}$ no es REPCTXT seguro, crearemos al adversario A del tipo IND-CPA que usa a B como subrutina, el cual cuenta con un oráculo $F_n(\cdot,\cdot)$ que recibe dos mensajes. En el mundo real encripta usando $\mathcal{E}_K$ y en el ideal retorna un valor totalmente aleatorio. Con esto definido, se crea el adversario A como se muestra a continuación:

```
Adversario A^{F_n(·,·)}()
  K <-$ 𝒦
  S <- ∅
  win <- false
  while B^{F_n'(·)} haga consultas:
    M_0 <- B^{F_n'(·)}
    M_1 <-$ ℳ
    C <- F_n(M_0, M_1)
    C -> B^{F_n'(·)}
    win <- B^{F_n'(·)}
  if win:
    return 1
  return 0
```

Analizando este adversario, se tiene que si el adversario B toma tiempo t y q preguntas en ejecutarse, entonces el adversario A toma la misma cantidad de preguntas y su tiempo total será $t_A = t + k$, con k constante para considerar el tiempo que toman las instrucciones extra respecto a la simulación del adversario B.

Y ahora analizando la ventaja del adversario, partiremos con el mundo de la izquierda, notemos que este caso simplemente corresponde a simular el adversario $B^{F_n'(\cdot)}$, puesto que el oráculo encripta siempre su mensaje y le devuelve el texto cifrado mediante $\mathcal{E}_K$, tantas veces como quiera este adversario, de modo que la probabilidad de identificar si estamos en el mundo izquierdo será igual a la ventaja que posee $B^{F_n'(\cdot)}$:

$$\Pr\left[\mathrm{Izq}_{\mathcal{SE}}^{A} \Rightarrow 1\right] = \mathrm{Adv}_{\mathcal{SE}}^{\mathrm{REPCTXT}}(B) = \Pr\left[\mathrm{REPCTXT}_{\mathcal{SE}}^{A} \Rightarrow \mathrm{true}\right]$$

Y por otro lado, en el mundo de la derecha se tiene que su probabilidad dependerá de la cantidad de preguntas q que realice $B^{F_n'(\cdot)}$, ya que en este mundo el mensaje que recibe el oráculo $F_n(\cdot)$ no es el que entrega B, y por tanto, que entregue 1 en este caso dependerá de la probabilidad de que en q preguntas y tiempo t exista al menos una coincidencia para dos cadenas de bits de largo n será:

$$\Pr\left[\mathrm{Der}_{\mathcal{SE}}^{A} \Rightarrow 1\right] = 1 - \frac{2^n!}{(2^n - q)! \cdot (2^n)^q} \approx 0$$

Esta aproximación es verdadera cuando la cantidad de preguntas q es muy alta, lo cual debería ocurrir dado que B no posee ventaja en este mundo.

De esta forma, la ventaja del adversario A es la siguiente:

$$\begin{aligned}
\mathrm{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) &= \left|\ \Pr\left[\mathrm{Der}^{A}_{\mathcal{SE}} \Rightarrow 1\right] - \Pr\left[\mathrm{Izq}^{A}_{\mathcal{SE}} \Rightarrow 1\right]\ \right| \\
&\geq \left|\ 1 - \frac{2^n!}{(2^n - q)! \cdot (2^n)^q} - \Pr\left[\mathrm{REPCTXT}^{A}_{\mathcal{SE}} \Rightarrow \mathrm{true}\right]\ \right| \\
&\approx \Pr\left[\mathrm{REPCTXT}^{A}_{\mathcal{SE}} \Rightarrow \mathrm{true}\right] = \mathrm{Adv}^{\mathrm{REPCTXT}}_{\mathcal{SE}}(B)
\end{aligned}$$

Como asumimos que la ventaja $\mathrm{Adv}^{\mathrm{REPCTXT}}_{\mathcal{SE}}(B)$ es significativa esto implica que la ventaja de A también lo es, por lo que finalmente llegamos a la contradicción, concluyendo entonces que si $\mathcal{SE}$ es IND-CPA seguro, entonces $\mathcal{SE}$ es REPCTXT seguro.