Laboratorio 1

Ataque Padding Oracle

Integrantes: Andrés Calderón y Nicolás Arancibia

a) Pruebe los servicios con distintos tipos de entrada (distintos largos, modificaciones de bytes, etc). Documente el análisis exploratorio realizado y sus conclusiones.

R: Durante la exploración de ambos servicios pudimos notar que, dado un mismo mensaje, se obtuvieron distintos textos cifrados entregados por el servicio A.

Y también pudimos notar que el tamaño de los bloques del texto cifrado aumentaban según el largo del mensaje, por ejemplo, a partir de 9 caracteres de mensaje, el tamaño del texto cifrado aumenta, luego a partir de 25 igual, y así cada 16 caracteres más, es por esto que deducimos que los bloques del texto cifrado corresponden a 16 bytes, y en el caso particular del inicio se explica porque la *key* también es parte del texto cifrado (8 carácterers adicionales, sumando 16 finalmente en el primer bloque).

b) Cree un programa basado en el código base que envía un mensaje *m* al servidor A y le envía la respuesta del servidor A al servidor B. Documente lo observado.

R: Es posible notar que el servidor B siempre es capaz de desencriptar los mensajes enviados por el servidor A.

c) Responda brevemente, ¿cómo podría conocer en un contexto genérico, el tamaño del bloque del cifrador utilizado, sin conocer el cifrador? Solo responda teóricamente, ya que el tamaño del bloque en AES es conocido.

R: Bajo un contexto genérico, es posible identificar el largo de bloque cambiando el largo del mensaje de entrada, de modo que cuando ocurre un cambio en el largo de la salida es porque se tuvo que realizar *padding* para llenar un bloque nuevo.

f) Ejecute satisfactoriamente el ataque descrito para obtener *key*, registre su valor en el informe del laboratorio.

R: Tras realizar el ataque satisfactorio, logramos obtener *key*, cuyo valor es:
83c804bf74f04b841b9c186342c62a1797cd87b1fe6ce7bf54d32c4a16390020