PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Criptografía y Seguridad Computacional - IIC3253
Tarea 1
Plazo de entrega: jueves 10 de abril

Instrucciones

Cualquier duda sobre la tarea se deberá hacer en los *issues* del repositorio del curso. Los issues son el canal de comunicación oficial para todas las tareas.

Configuración inicial. Para esta tarea utilizaremos *github classroom*. Para acceder a su repositorio privado debe ingresar a un link que le enviaremos a más tardar mañana, seleccionar su nombre y aceptar la invitación. El repositorio se creará automaticamente una vez que haga esto y lo podrá encontrar junto a los repositorios del curso.

También deberá responder este formulario, en el que se le pedirá una **llave simétrica** que será utilizada para encriptar sus notas y correcciones usando el esquema AES. La llave debe tener como **máximo** un largo de 32 caracteres. En el repositorio del curso se publicará además el valor de hash de su llave utilizando SHA256. Si usted pierde dicha llave podrá recuperarla incurriendo en una penalización de dos décimas en el promedio de sus tareas. Si otra persona descubre su llave antes de que se publiquen las notas de la segunda tarea, el promedio de tareas de dicha persona aumentará en cinco décimas, mientras que el suyo disminuirá en cinco décimas.

Recomendación: **Use un administrador de contraseñas**.

Entrega. Al entregar esta tarea, su repositorio se deberá ver exactamente de la siguiente forma:

```
Repositorio
├── Tarea1
│   ├── Pregunta1
│   │   ├── cipher.txt
│   │   └── plain.txt
│   └── Pregunta2
│       └── pregunta2.pdf
├── .gitignore
├── README.md
└── .git
```

Para cada problema cuya solución se deba entregar como un documento (en este caso la pregunta 2), deberá entregar un archivo `.pdf` que, o bien fue construido utilizando LaTeX, o bien

es el resultado de digitalizar un documento escrito a mano. En caso de optar por esta última opción, queda bajo su responsabilidad la legibilidad del documento. Respuestas que no puedan interpretar de forma razonable los ayudantes y profesores, ya sea por la caligrafía o la calidad de la digitalización, serán evaluadas con la nota mínima.

Preguntas

1. En esta pregunta usted deberá decriptar un mensaje que ha sido encriptado usando OTP, pero cometiendo el error de usar una llave más corta que el mensaje a encriptar.

   Los ayudantes crearán una rama en su repositorio personal llamada *tarea-1*, que contendrá el archivo `/Tarea1/Pregunta1/cipher.txt`. Usted deberá decriptar el contenido de dicho archivo, y dejar un archivo `/Tarea1/Pregunta1/plain.txt` en la rama `main` de su repositorio a modo de solución. Este archivo deberá contener el texto plano original que fue encriptado.

   En el repositorio del curso encontrará un ejemplo del archivo que subirán los ayudantes del curso a su repositorio personal, en `/Tareas/Tarea1/ejemplo_pregunta1/cipher.txt`. También encontrará el archivo `/Tareas/Tarea1/ejemplo_pregunta1/plain.txt`, que corresponde al texto plano original, ejemplificando lo que usted tendrá que entregar.

2. Sean q y n dos números naturales tales que $2 \leq q \leq n$, y sea (Gen, Enc, Dec) un esquema criptográfico definido sobre los espacios $\mathcal{M} = \mathcal{C} = \{0,1\}^n$ y $\mathcal{K} = \{0,1\}^{nq-1}$. En esta pregunta usted debe demostrar que este esquema no es una pseudo-random permutation (PRP) con q rondas. En particular, debe demostrar que el adversario gana el juego que define una PRP con una probabilidad mayor o igual a $\frac{1}{2} + \frac{1}{6}$.