Tarea 2

Criptografía y seguridad 2020-2

Fecha límite de entrega: 12 de marzo

Indicaciones

- Resuelve cada uno de los ejercicios, todos tienen el mismo valor.
- Puede hacerse de forma individual o en pareja, en caso de hacerla en pareja basta que se entregue una solución.
- **Sube tu tarea solo cuando estés completamente seguro de que es correcta, ya que solo se puede subir una vez.**
- Escribe los cálculos que realizaste, o en caso de haber usado otra herramienta (como un programa) indícalo en tu respuesta.
- Para los ejercicios que requieren programar utiliza un lenguaje de los siguientes: Python, Java, C o Haskell. Anexa tu código fuente.
- Organiza tus archivos en un archivo `.zip`, incluyendo los datos de los alumnos, y súbelo en `https://forms.gle/uvL8TshVQivNzMXw6`

Ejercicios

1. Alicia y Bartolo escogen un espacio de claves $\mathcal{K}$ que contiene 2^{56} claves. Supón que Eva tiene una computadora que puede revisar 10^{10} claves por segundo.

   a) ¿Cuántos días le tomaría a Eva revisar todas las claves de $\mathcal{K}$?

   b) Si Alicia y Bartolo cambian su esquema por uno con un conjunto más grande, con 2^B claves, ¿qué tan grande debe ser B para que la computadora de Eva tarde 100 años revisando todas las claves? (Puedes suponer que un año tiene 365,25 días.)

2. ¿Los siguientes esquemas de cifrado son perfectamente seguros? Explica.

   a) Los mensajes claros son $\mathcal{M} = \{0, 1, \ldots, 9\}$. El algoritmo KeyGen devuelve una clave al azar del conjunto $\mathcal{K} = \{0, 1, \ldots, 10\}$. La función $\mathsf{Enc}_k(m)$ calcula $(k + m)$ mód 10, y $\mathsf{Dec}_k(c)$ devuelve $(c - k)$ mód 10.

   b) El algoritmo de desplazamiento (César) para mensajes de tamaño uno sobre el alfabeto `ABC...Z` de 26 letras.

   c) One-time pad para mensajes de longitud ℓ, usando únicamente llaves distintas de $k = 0^\ell$. Esto es para evitar que un mensaje cifrado sea exactamente el mensaje claro.

3. Definimos Π como una versión modificada de one-time pad, donde $\mathcal{M} = \{0, 1\}^\ell$, pero ahora $\mathcal{K}$ son las cadenas de ℓ bits con un número par de unos; el cifrado y descifrado son iguales que en one-time pad. Construye un adversario $\mathcal{A}$ tal que $\Pr[\mathsf{PrivK}_{\mathcal{A},\Pi} = 1] = 1$, es decir, un adversario que siempre gana el juego $\mathsf{PrivK}_{\mathcal{A},\Pi}$.

4. Sea Π el esquema de Vigenère, donde $\mathcal{M} = \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}^3$, la clave se genera escogiendo aleatoriamente un número $t \in \{1, 2, 3\}$ y luego se escoge una clave aleatoria de tamaño t.

   En el juego $\mathsf{PrivK}_{\mathcal{A},\Pi}$ un adversario $\mathcal{A}$ entrega $m_0 = \mathtt{aab}$ y $m_1 = \mathtt{abb}$. Cuando se le da un texto cifrado $c = c_1c_2c_3$, devuelve 0 si $c_1 = c_2$ y 1 en caso contrario.

   Construye un mejor adversario que $\mathcal{A}$, es decir, un adversario $\mathcal{A}'$ tal que $\Pr[\mathsf{PrivK}_{\mathcal{A}',\Pi} = 1] > \Pr[\mathsf{PrivK}_{\mathcal{A},\Pi} = 1]$.

5. Como hemos visto, un archivo cifrado normalmente está formado por bytes que no tienen una representación como texto. Una forma muy común de almacenar bytes arbitrarios como una cadena de texto consiste en usar la codificación Base64.

Recuerda que no es lo mismo cifrar (encriptar) que codificar, pues la codificación solamente sirve para representar de distintas formas la información, no tiene el propósito de ocultarla o proteger su integridad.

Para usar Base64 existen programas o bibliotecas en cualquier lenguaje de programación. Busca alguno y decodifica el siguiente contenido, que originalmente es una imagen en formato PNG.

```
iVBORw0KGgoAAAANSUhEUgAAAFEAAAAzCAIAAABgOXMwAAAAAXNSROIArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAAn5SURBVGhD5ZoHVFRXGsfvvW/eMHQUBRUrYjTL
GkuMGNfusa/ILpYYG8paWAvrMWuOOUYl6AaNikmM5WStMa6KGLtYYhdjY1UELERZK9gow8zAvHL3
m3l3hFFmIIODcvI7R+Z+990n7z/3fuXeB45NvIN+ZxD2+XuCIIpZs5oBz00ppgjDP1MbetiV8sBf
JGaZb6hmYE5KWru0UPuIw0SWJXeNpnfEbMy7s8t2wfMTMynimPXWA5Mj6J/vWj6jMPtKWtpSjv7K
IS8qS3oq9un1Qz5pMnhyHO/uw0bbADTfokjFrLcbWMMHNi3rHHT3n9EfenmJ2DoYwdWLFx9vO/Dw
QoZ333GzsG2frTbzDDO8c8U8P+OxXXujcGk5ijZwagWKJNmr34TzPYZ9jnHZuqpN3C549qDrB893
7YtC1vO3YPF5mUjMADBSqQrC2qGivBzW8wrVRvPJjdFxn/cEvcRqltHqFfsItV7kFE2aGLx5yWhb
Kal6aE7/5cjo8GAsGaAtybjBu1/GLTmvXCoWpXMpxsXxpynilR6AEEkjGDCSmWONaK4GiSr1+NZJ
kX9U2lHRCWmXpn30cTeCasDDh4d39vGUIsa1+Oqb08oAhcNH59zNvMwMa4hA1Kz5tkJFQ6dOgRQz
p+OUOmzrtqxpO74T5WfgvgOC/JoG+Xt5+EhGrTJAoYZn3uXj+5hhDY7ZkUXAA95isrPS+7U41ruz
L7Mpuv8gj1PhunW8wdLpBTc3NSzjAm2xl6dGGWKCku7DM/pGzmVmKaqBPxuK9JgWMgPAqH59HOUw
4O7Gm+tIbCXYjK2ZrAaaKQRqWnYOUoABMqdjhgXKawS56vIz5YiQfQ+qQtHyXVfKdzQu3i6u9ZiB
kCjjgkJNOs/XU9MfmUsRPC9mf/jQHWk3n7IRZo6dymnXdSAzrCGVehxrVKKUtO7L/8RGXFk+t8vD
zAdrFm6cM3xD7Dg3XExlx38PRkV7diUzw5Sr3CZMSfT25qdM24EQr9MZebVrwuYRiT9dEcWS5TAx
clOd5m2YYc1rqDOh8Rfr806umu2nO8XOGNHArbZgmVgOY5FK4zfGuHfv4/GHrvWCgpX+CkNz7t8W
MhbGx/VWEVg1JmSKW7ZZnnZ58tNclPLfzE4dGsWvTunWse6vd4SRQwMJMdUhj3NOgyLPhOWvLHMh
cz2GTavMCpcwepB+8v6e9cs6DB7WorMH71ba8OwrD+HQVt0bFdNtW77lmjT18a3LrpUHodKz25eb
kh2zZ3YEZ2G98B9i1DI4oFEjr3xd7qVf7oWENPb388x5lN/mPd+aNV1hgIxxwtYrvu1m866eyi0v
Ucl5lh/euHBtddzuMTFUthdmAK1eOzcvtemAvzPbLsUG3d7v53UKzl4a19+8kpDOgARR8PFkxRaG
uEVEImNqKTyhh5qSLr1z98HYT7V9I+ZiUvZcQq/jnqaS8fP9P24ZPLNcwYCnm6fvtdtigc3S3wKE
YSk1KW56hGbJot6ghWIh/utTE2demfpZ+pzYw0oNDfKwxLOQDJgFo7MXMnv229q6+8e2BAOOzzMU
8Kum9708aoGqwrdDlA369m/R685h27cUPr975oe5R/YMIFjU6aWneU9HRe5uP2Be7eadKaZJa2KG
9y8O7dnU189Dbb3rz9cW5RYW9RpOfMzc9bz65VxdGsfPPWFVNz51NLJt75c2OnYgCK+4+XNuzyFe
tRqwrlJgJB5P+Casi35wWLMli5IMxdSgap4rNfQLbBfQpLl5CEWyfPtasqR96u+eaXhyDeIZz1FB
hE+ilevpuNbt+wyFZGYebBPHz8Ou7vl3jHdgHc+azK4YOqMu6nlaSL8JzLYAS2DB2HYL5w+Z98V2
TDw+WXFQgPISHozaXBEC4dWSSIkgQ8lCECcTbHtwaSCOOyJYhYtrpaW+EAxZfn3KQWi89A3D+t95
oyS1ApwEpUoZngYju/914m0aGr3y9D9WHROJGoOv2tXAy4Lp3JOqCOVVEl9BwYBNR7dP3OSxs/uP
ZAbURgRtun5S/bJklGcoXH1uLzPMaNxdR7btyAxrPgwd79vgXcK5MNtpOKKZIMlTynItKrmXUHxg
dGyxyeGsqKHx2BcxnxlmOIou7YT66U3ikGajfuv4f2GruEl5sWw3IeBqpZAgpchGZNkMvxEc0Xz2
RJJ/EWy6HQkEJiRBKnWOU/XYOyxKxUumDryw73tmv4AaTFsmR5FVSEWNzHgT2NRsNGpvr51/deKc
cL10IznRdJpoAfKCY9FeQYZ8iqwClanwStmffvYnJBawLmdiU7MnLZjUrIOHwA8K+hN37SwuKjlt
8qa8qdJ3FDXiYP/ADDOp5w8My86bruMSFO2GKpr1Og2bml2oXN/HDxoykuI/GJN8aJPSDymx8zst
vL3YOUxpJDVZfW73rDOrP9u/elzCooiEhTEHN7ySvyCvyrjUKTwsGZ+LydODgoN8GOr3HpEKp1mH
salZJ+Az6SlKW5bFPoHvKW1ORlf3biZlnQGoBDqhY+j8sKgFg6LWDJu5fujMmD5jXnWCdwIaY67k
9/4YP2v0+91gW2wyJNirlL9dqSQ2NedR1OeGPKUNW//s4OckyDEmJGQoLnNlm/c6UGkhLMgYnpya
fryKm4t7yeslJOnunA1W+ytGkUmw45GigtjUDN+3xLGMAoUhJiI2O6GR8DaOVJwSVRnnDq7vOVm2
BEijmsrOT2M2NXt5+uYFBjADoYZuvoLeFMbgBnjASs2FZZLhQ8h/HFSvoWLCpt9bVaMKDtttaoa5
PZN1EOpFhb+O7rItPhoaLpws4kq9r37hF+AJLZ/keqjYXjfl3q2QjyKVtlOxs7YJ715Lh1nxAAlG
zsmSREEw6r1dKvW6p3FAQyqazrf0+VpZV5ICr+Xdd2vajhnOxI5m1HXQqE8Or1WmBeb7xJSVKccT
jmz+alLHP5v7HKSWq0/qoW2wCVwbOyIqhB1Bw25UU6u2C18VNak9zUjlcTTjPG95W+9ahN6/dyv7
yIkanIfS4xjeourg9q/PbF++JWyqClzIjITxujsZHj6Wl1LOxK5mhNqHT0198j9mIDS11aBzOcsc
312YgdvTJ6wMzS9qq/F/kbNkTpZd+DJT4GunHM2tug05mplS8iim19ivIbC6EH54217UfP6uELp0
xsCIT0sFOCdSjmYJC7DqKi/SPiDOPqdFKtOJfBVQzt8Bumg8Ant0c/qXj7Go9oaoxkwnQ+xKRoTj
N1xIhmqB2c5hbObylCWbnL6cLJR/7ikTdTkOUGlyC59pBadvp15QvpyWnfpvvH7KqRMt1PJX8fbe
PLxeytdcs2HzGXu/A79nthM4oyt0ca1Uzv9NlK8Z3Cw8anG6/jGzXzewIX8sGypz8PJbqZCrBnXs
eyjV6nXEa0TSqKhlm1EVIPR/XQXt9t25L+8AAAAASUVORK5CYII=
```

También podemos escribir la representación hexadecimal de los bytes originales. Entre Base64 y la representación hexadecimal ¿cuál ocupa más espacio? ¿Por qué?

6. Para cifrar un mensaje usando One-time pad necesitamos una cadena aleatoria de bytes. Supongamos que Bartolo quiere enviar un archivo a Alicia, entonces Juan Aleatorio le proporciona el archivo `cinta_aleatoria.txt`, que contiene una cadena de bytes k en Base64. Bartolo usa k como llave para cifrar el archivo `imagen.png` y envía el resultado c a Alicia.

   Alicia, que también posee k, al recibir el mensaje cifrado c revisa los primeros bytes y nota algo extraño: c no parece algo aleatorio, sino que es un mensaje de un formato muy particular.

   Cuando Alicia descifra c obtiene el mensaje correcto (el archivo `imagen.png`), y entonces se da cuenta de que la llave no es una cadena tan arbitraria de bytes, al parecer Juan Aleatorio conocía el mensaje que Bartolo quería enviar.

   a) Cifra `imagen.png` con la cadena contenida en `cinta_aleatoria.txt` (revisa que esta llave tiene la misma longitud que el mensaje) para obtener el mensaje c y descubre por qué Alicia notó algo extraño.

   b) Suponiendo que k efectivamente es una cadena aleatoria de bytes, ¿cuál es la probabilidad de que $m \oplus k$ sea el c que recibió Alicia?

   c) ¿Qué hizo Juan Aleatorio para crear el archivo `cinta_aleatoria.txt`?