Glosario de términos usados en el curso

- Enc: función de cifrado o encriptación
- Dec: función de descifrado o desencriptación
- $c = Enc(k, m)$: m es el mensaje o texto plano, k es la clave o llave, y c es el texto cifrado
- A y B: Alice y Bob, dos participantes que quieren comunicarse de manera segura
- E: Eve, quien quiere atacar a los protocolos criptográficos (descifrar mensajes, hacerse pasar por otro participante, etc.)
- M: espacio de todos los mensajes posibles
- C: espacio de todos los mensajes cifrados posibles
- K: espacio de todas las claves posibles
- h: función de hash
- H: espacio de posibles valores para una función de hash
- Para denotar la probabilidad de un evento utilizaremos Pr[evento]. Para referirnos al espacio de casos posibles usaremos la notación de *underset* vista en clases. Por ejemplo, dados un mensaje m y un texto cifrado c, la probabilidad de que al ver c el mensaje original haya sido m se define como la cantidad de llaves k tales que $Enc(k, m) = c$ dividido por la cantidad total de llaves. La notación para esta probabilidad es la siguiente:

$$\underset{k \leftarrow K}{\Pr}[Enc(k, m) = c]$$

- Tipos de ataques:
  - solo texto cifrado: el adversario solo tiene un texto cifrado c
  - texto plano: el adversario tiene un texto plano m y su texto cifrado c
  - texto plano elegido: el adversario elige textos planos m_1, m_2, ..., m_r, y le son entregados sus textos cifrados c_1, c_2, ..., c_r
  - texto cifrado elegido: el adversario elige textos planos m_1, m_2, ..., m_r, y le son entregados sus textos cifrados c_1, c_2, ..., c_r, y además elige textos cifrados c'_1, c'_2, ..., c'_s, y les son entregados sus textos planos m'_1, m'_2, ..., m'_s
- Propiedades de una función de hash $h : M \to H$:
  - h es resistente a preimagen: no existe un algoritmo eficiente (de tiempo polinomial) que dado $x \in H$, calcule $m \in M$ tal que $h(m) = x$
  - h es resistente a colisiones: no existe un algoritmo eficiente (de tiempo polinomial) que pueda encontrar dos mensajes distintos $m_1, m_2 \in M$ tales que $h(m_1) = h(m_2)$

- Función despreciable: una función $f : \mathbb{N} \to [0,1]$ es despreciable si para todo polinomio $p(n)$, existe $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$:

$$f(n) \quad \leq \quad \frac{1}{p(n)}.$$

- Sistema (o esquema) de cifrado simétrico: dados espacios M, K y C de mensajes, claves y textos cifrados, respectivamente, (Gen, Enc, Dec) es un sistema de cifrado simétrico sobre M, K y C si:
  - $Gen : \{1\}^* \to K$ es un algoritmo aleatorizado de tiempo polinomial que dado 1^n genera una clave $k \in K$.
  - $Enc : K \times M \to C$ es un algoritmo de tiempo polinomial que corresponde a la función de cifrado.
  - $Dec : K \times C \to M$ es un algoritmo de tiempo polinomial que corresponde a la función de descifrado. Se debe tener que $Dec(k, Enc(k, m)) = m$ para todo $k \in K$ y $m \in M$.
- Sistema (o esquema) de cifrado simétrico de largo fijo $\ell(n)$: (Gen, Enc, Dec) debe satisfacer la definición de sistema de cifrado simétrico sobre M, K y C junto con la siguiente propiedad adicional. Para cada k generado por la invocación $Gen(1^n)$, se tiene que $Enc(k, m)$ está definido solo para mensajes $m \in M$ de largo $\ell(n)$.
- Generador pseudo-aleatorio: Sea $G : \{0,1\}^* \to \{0,1\}^*$ un algoritmo de tiempo polinomial que dado $s \in \{0,1\}^n$, construye $G(s) \in \{0,1\}^{p(n)}$, donde $p(n)$ es un polinomio fijo. G es un generador pseudo-aleatorio si satisface las siguientes propiedades:
  - Expansión: para cada n, se tiene que $p(n) > n$
  - Pseudo-aleatoriedad: para cada algoritmo $D : \{0,1\}^* \to \{0,1\}$ de tiempo polinomial, existe una función despreciable $f(n)$ tal que:

$$\left| \Pr_{r \leftarrow \{0,1\}^{p(n)}}[D(r) = 1] - \Pr_{s \leftarrow \{0,1\}^n}[D(G(s)) = 1] \right| \quad \leq \quad f(n)$$