Índice general

Capítulo 1

Criptosistemas simétricos o de clave privada

1.1. Criptografía

La *criptografía* es la ciencia de representar información de forma opaca para que sólo los agentes autorizados (personas o dispositivos diversos) sean capaces de desvelar el mensaje oculto. El proceso de ocultar la información se llama *cifrado*, pero a menudo también se llama *encriptado* por influencia del inglés. El proceso de desvelarla se llama *descifrado* o *desencriptado*. El concepto de criptosistema modela los procesos de cifrado y descifrado.

Un *criptosistema simétrico*, también llamado *de clave privada*, está formado por un conjunto K, cuyos elementos llamamos *claves* o *llaves*, y una regla que asocia dos aplicaciones a cada clave $k \in K$:

$$c_k : M_k \longrightarrow C_k, \quad d_k : C_k \longrightarrow M_k$$

de forma que

$$d_k(c_k(x)) = x, \text{ para todo } x \in M_k$$

En la práctica el protocolo criptográfico también incluye un algoritmo generador de claves, es decir, uno que tiene como salida un elemento de K, pero nosotros no vamos a tener en cuenta esta parte del criptosistema.

Extendemos las aplicaciones c_k a $M_k^\infty = \cup_{n\geq 1} M_k^n$ y d_k a $C_k^\infty = \cup_{n\geq 1} C_k^n$ poniendo

$$c_k(x_1 \dots x_n) = c_k(x_1) \cdots c_k(x_n), \quad x_1, \dots, x_n \in M_k$$
$$d_k(y_1 \dots y_n) = d_k(y_1) \cdots d_k(y_n), \quad y_1, \dots, y_n \in C_k$$

Obsérvese que representamos los elementos de M^n como concatenación de elementos de M.

Utilizaremos la siguiente terminlogía para una clave $k \in K$:

- Elementos de M_k^∞: *Mensajes en claro.*
- Elementos de C_k^∞: *Mensajes en cifrados o encriptados.*
- Elementos de c_k: *Función de cifrado o función de encriptado.*
- Elementos de d_k: *Función de descifrado o función de desencriptado.*

Un mensaje en claro o cifrado diremos que es *básico* si tiene longitud 1. Sin embargo, en muchas situaciones diremos mensajes para referirnos a mensajes básicos, bien en claro o cifrados.

Frecuentemente M_k es el mismo conjunto para todas las claves y lo mismo ocurre con los C_k. En este caso ponemos $M = M_k$ y $C = C_k$.

Ejemplo 1.1. *Criptosistemas.*
Sea A un conjunto finito y denotemos por S_A el conjunto de permutaciones de los elementos de A.

(1) *Sustitución.* Tomamos como conjunto de claves $K = S_A$, como conjuntos de mensajes básicos $M = C = A$ y como funciones de cifrado y descifrado:

$$c_\sigma(x) = \sigma(x) \quad \text{y} \quad d_\sigma(y) = \sigma^{-1}(y)$$

(2) *Reordenamiento.* Ponemos $K = \cup_{n\geq 2} S_n$, donde $S_n = S_{\{1,\ldots,n\}}$. Si la clave σ está en S_n entonces ponemos $M_\sigma = C_\sigma = A^n$ y ciframos reordenando las posiciones de los símbolos de los mensajes en claro. Más precisamente:

$$c_\sigma(x_1 \cdots x_n) = x_{\sigma(1)} \cdots x_{\sigma(n)} \quad \text{y} \quad d_\sigma(y_1 \cdots y_n) = x_{\sigma^{-1}(1)} \cdots x_{\sigma^{-1}(n)}$$

En la práctica casi todos los protocolos criptográficos son combinaciones de los del ejemplo 1.1. Sin embargo, en estos criptosistemas no se dice nada sobre las permutaciones elegidas. La naturaleza de estas permutaciones es lo que hace un criptosistema bueno o malo. La bondad de un criptosistema depende de que satisfaga las siguientes condiciones:

- *Rapidez de los cálculos.* Es importante disponer de un algoritmo eficiente (polinomial, con exponente pequeño) para calcular $c_k(x)$ y $d_k(y)$.
- *Seguridad.* Debe ser difícil descubrir un valor concreto de x a partir del valor de $c_k(x)$ sin conocer k.

Las nociones de "algoritmo eficiente", "difícil de calcular" y "tiempo razonable" son ambiguas. Más adelante daremos conceptos más precisos. De momento, veamos ejemplos concretos.

Criptosistema de César

Vamos a identificar las 27 letras mayúsculas del alfabeto español asignando a cada una de ellas un número del 0 al 26, de forma que estamos identificando los elementos de A con los de $\mathbb{Z}_{27}$ usando la siguiente tabla

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	0	10	11	12	13
$\tilde{N}$	O	P	Q	R	S	T	U	V	W	X	Y	Z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

(1.1)

Ponemos $K = M = C = \mathbb{Z}_{27}$ y

$$c_k(x) = (x + k \mod 27)$$
$$d_k(x) = (x - k \mod 27)$$

Por ejemplo, supongamos que la clave es la letra W, que corresponde con el número 23 y que queremos cifrar el mensaje "ésta es la primera vez que vamos a cifrar un mensaje". En primer lugar obsérvese que nuestro alfabeto sólo contiene letras mayúsculas sin acentuar, con lo que el mensaje a cifrar es:

ESTAESLAPRIMERAVEZQUEVAMOSACIFRARUNMENSAJE

Ahora tenemos que convertir el mensaje en una lista de números de acuerdo a la tabla anterior:

$$4, 19, 20, 0, 4, 19, 11, 0, 16, 18, 8, 12, 4, 18, 0, 22, 4, 26, 17, 21,$$
$$4, 22, 0, 12, 15, 19, 0, 2, 8, 5, 18, 0, 18, 21, 13, 12, 4, 13, 19, 0, 9, 4$$

Después tenemos que sumar a cada uno de estos números la clave, es decir, sumamos 23 módulo 27, o lo que es lo mismo restamos 4 módulo 27.

$$0, 15, 16, 23, 0, 15, 7, 23, 12, 14, 4, 8, 0, 14, 23, 18, 0, 22, 13, 17,$$
$$0, 18, 23, 8, 11, 15, 23, 25, 4, 1, 14, 23, 14, 17, 9, 8, 0, 9, 15, 23, 5, 0$$

Finalmente tenemos que sustituir los números por las letras correspondientes y obtendremos el mensaje cifrado.

AOPWAOHWMÑEIAÑWRAVNQARWILOWYEBÑWÑQJIAJOWFA

Criptosistema de Vigenère

Es similar al de César con el alfabeto español identificado con $\mathbb{Z}_{27}$, pero $K = \mathbb{Z}_{27}^{\infty}$ y si $k \in \mathbb{Z}_{27}^{d}$ entonces $M_k = C_k = \mathbb{Z}_{27}^{d}$ y

$$c_{k_1 \cdots k_d}(x_1 \cdots x_d) = [x_1 + k_1]_{27} \cdots [x_d + x_k]_{27}$$
$$d_{k_1 \cdots k_d}(y_1 \cdots y_d) = [y_1 - k_1]_{27} \cdots [y_d - y_k]_{27}$$

Es decir se divide el mensaje en bloques de longitud d y se trabaja como en el Criptosistema de César usando la clave k_i para los símbolos en posiciones con $j \equiv i \mod d$.

En realidad el criptosistema de César y Vigenére se pueden considerar como casos particulares de otros más generales. Simplemente hemos restringido la presentación a 27 símbolos para hacer más simple la explicación. Sin embargo el conjunto de símbolos puede ser cualquiera (letras mayúsculas y minúsculas, comas, espacios, etc), y podemos siempre identificar el conjunto de símbolos con $\mathbb{Z}_n$ donde n es el cardinal del conjunto de símbolos. De esta forma podemos obtener versiones del Criptosistema de César y del de Vigenère con un conjunto mayor de símbolos. Por otro lado, se puede cambiar $\mathbb{Z}_n$ por cualquier otro grupo sin que cambie de forma esencial la naturaleza de estos dos criptosistemas. Nos referiremos a este grupo como plataforma. Por ejemplo, en lugar de identificar los símbolos del alfabeto con los elementos de $\mathbb{Z}_n$ los podemos identificar con los elementos de un grupo finito y utilizar la operación del grupo para hacer las operaciones. No es esencial que la aplicación que asocia a un símbolo un elmenento del grupo plataforma sea sobreyectiva, aunque si que es necesario que sea inyectiva.

Por otro lado, los símbolos pueden no ser elementos de un alfabeto natural sino combinaciones de varios símbolos. Es decir, podemos elegir una cierta longitud, pongamos n, e identificar listas de n símbolos en nuestro alfabeto, con el grupo aditivo $\mathbb{Z}_{b^n}$, donde b es el cardinal del alfabeto. Por ejemplo, supongamos que utilizamos el mismo alfabeto de antes, es decir, las letras mayúsculas del alfabeto en español y que las queremos agrupar en bloques de longitud cuatro. Entonces podemos identificar estas sucesiones con los elementos de $\mathbb{Z}_{27^4}$ mediante la siguiente regla:

$$AAAA = 0, AAAB = 1, \ldots, AAAZ = 26, AABA = 27, AABB = 28, \ldots, ZZZZ = 27^4 - 1$$

Obsérvese que el bloque $X_1X_2X_3X_4$ se identificará con

$$x_1 \cdot 27^3 + x_2 \cdot 27^2 + x_3 \cdot 27 + x_4 \cdot 27^0$$

donde x_i es el número identificado con la letra X_i. Por ejemplo, "MESA" se identificaría con

$$12 \cdot 27^3 + 4 \cdot 27^2 + 19 \cdot 27 + 0 \cdot 27^0 = 239625$$

De esta forma $M = C = \mathbb{Z}_{27^4}$ y podríamos utilizar cualquiera de los criptosistemas anteriores de forma similar.

En resumen, podemos establecer diferentes formas de asociar los mensajes básicos con los elementos de un grupo G. Todo esto no tiene ninguna naturaleza criptográfica, es simplemente la codificación de la información, de forma que podemos identificar el grupo plataforma G con los tres conjuntos fundamentales del protocolo criptográfico: $K \equiv M \equiv C \equiv G$. Lo que tiene la naturaleza criptográfica son las funciones de cifrado y descifrado, que en este caso toma la forma,

$$c_k(x) = kx, \quad \text{y} \quad d_k(y) = k^{-1}y$$

Otra cosa importante, es que la naturaleza del grupo plataforma no es indiferente, pues para que podamos considerar el criptosistema como tal, necesitamos disponer de algoritmos eficientes para calcular las funciones de cifrado y descifrado y queremos que, sin el conocimiento de la clave sea difícil descifrar. Así por ejemplo $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n^*, \cdot)$ y los grupos aditivo y multiplicativo de un cuerpo finito o el grupo aditivo de un espacio vectorial sobre un cuerpo finito cumplen la primera condición pues la aritmética en estos grupos es sencilla.

Veamos un último ejemplo de criptosistema sencillo.

1.2. Entropía

Teorema 1.1. *Una función continua definida sobre el conjunto de funciones de distribución de longitud n que cumpla las condiciones:*

(1) $H\left(\frac{1}{n}, \ldots, \frac{1}{n}\right) < H\left(\frac{1}{n+1}, \ldots, \frac{1}{n+1}\right)$

(2) $H\left(\frac{1}{n}, \ldots, \frac{1}{n}\right) = H\left(\frac{k_1}{n}, \ldots, \frac{k_m}{n}\right) + \sum_{i=1, k_i \neq 0}^{m} \frac{k_i}{n} H\left(\frac{1}{k_i}, \ldots, \frac{1}{k_i}\right)$ *siempre que* $\sum_{i=1}^{m} k_i = n$

es de la forma

$$H(p_1, \ldots, p_n) = \sum_{i=1, p_i \neq 0}^{n} p_i \log_b\left(\frac{1}{p_i}\right) = -\sum_{i=1, p_i \neq 0}^{n} p_i \log_b p_i$$

para algún $b > 1$.

Demostración. Si $m|n$, entonces

$$H\left(\frac{1}{n}, \ldots, \frac{1}{n}\right) = H\left(\frac{m}{n}, \ldots, \frac{m}{n}\right) + \sum_{i=1}^{n/m} \frac{m}{n} H\left(\frac{1}{m}, \ldots, \frac{1}{m}\right) =$$
$$= H\left(\frac{m}{n}, \ldots, \frac{m}{n}\right) + H\left(\frac{1}{m}, \ldots, \frac{1}{m}\right)$$

En particular, si $n = m^s$, entonces

$$H\left(\frac{1}{m^s}, \ldots, \frac{1}{m^s}\right) = H\left(\frac{1}{m^{s-1}}, \ldots, \frac{1}{m^{s-1}}\right) + H\left(\frac{1}{m}, \ldots, \frac{1}{m}\right)$$

Sea $g(n) = H\left(\frac{1}{n}, \ldots, \frac{1}{n}\right)$, entonces

$$g(m^s) = g(m^{s-1}) + g(m)$$

y por inducción sobre s, se obtiene que

$$g(m^s) = sg(m)$$

La condición (1), implica que g es estrictamente creciente y, por tanto, para todo $m > 1$ tenemos $g(m^s) < g(m^{s+1})$, es decir, $sg(m) < (s+1)g(m)$. Por tanto $g(m)$ es positivo.

Sean n, k y m enteros mayores a 1 y sea s

$$s = \text{máx}\left\{j \in \mathbb{Z} : j \geq 0, m^j \leq n^k\right\}$$

entonces $m^s \leq n^k < m^{s+1}$. Como g es estrictamente creceinte, $g(m^s) \leq g(n^k) \leq g(m^{s+1})$, o equivalentemente

$$sg(m) \leq kg(n) \leq (s+1)g(m)$$

Como log también es una función creciente también tenemos

$$s\log(m) \leq k\log(n) \leq (s+1)\log(m)$$

Por tanto,

$$\frac{s}{k} \leq \frac{g(n)}{g(m)} \leq \frac{s+1}{k} \quad \text{y} \quad \frac{s}{k} \leq \frac{\log(n)}{\log(m)} \leq \frac{s+1}{k}$$

luego

$$\left|\frac{g(n)}{g(m)} - \frac{\log(n)}{\log(m)}\right| \leq \frac{1}{k}$$

Como k es arbitrario,

$$\frac{g(n)}{g(m)} = \frac{\log(n)}{\log(m)}$$

es decir,

$$\frac{g(n)}{\log(n)} = \frac{g(m)}{\log(m)} = C$$

Luego $g(n) = C\log(n)$ para algún número postivo C. Por tanto, si elegimos una base b adecuada, tendremos que $g(n) = \log_b n$.

Supongamos ahora que $(p_1, \ldots, p_k)$ es una distribución de probabilidad formada por números racionales. Poniéndolos con común denominador podemos suponer que $p_i = \dfrac{b_i}{n}$ y, de la propiedad (2) tenemos,

$$H(p_1, \ldots, p_k) = H\left(\frac{b_1}{n}, \ldots, \frac{b_k}{n}\right) = g(n) - \sum_{i=1, b_i \neq 0}^{k} \frac{b_i}{n} g(b_i) = \log_b n - \sum_{i=1, b_i \neq 0}^{k} \frac{b_i}{n} \log_b b_i =$$

$$= \sum_{i=1, b_i \neq 0}^{k} \frac{b_i}{n} \log_b \frac{n}{b_i} = \sum_{i=1, p_i \neq 0}^{k} p_i \log_b \frac{1}{p_i}$$

Como H es continua, entonces

$$H(p_1, \ldots, p_k) = \sum_{i=1, p_i \neq 0}^{k} p_i \log_b \frac{1}{p_i}$$

para toda $k-$upla $(p_1, \ldots, p_k)$ de números reales en el dominio de H. □

Definición 1.1. Sea b un número real mayor que 1. Se llama *entropía* en base b de una distribución de probabilidad $P = (p_1, \ldots, p_k)$ a

$$H_b(p_1, \ldots, p_k) = \sum_{i=1}^{k} p_i \log_b \frac{1}{p_i}$$

La entropía de una variable aleatoria discreta es la entropía de su distribución de probabilidad.

La base b en la que se calcule la función de entropía sólo implica un cambio de escala debido a la igualdad $\log_b x = \log_{b'} x \cdot \log_b b'$ que implica

$$H_b(X) = H_{b'}(X) \cdot \log_b b'$$

Proposición 1.1. *Sea $(p_1, \ldots, p_n, q_1, \ldots, q_m)$ una distribución de probabilidad. Si $a = \sum_{i=1}^{n} p_i$, con $0 < a < 1$ entonces*

$$H(p_1, \ldots, p_n, q_1, \ldots, q_m) = H(a, 1-a) + aH\left(\frac{p_1}{a}, \ldots, \frac{p_n}{a}\right) + (1-a)H\left(\frac{q_1}{1-a}, \ldots, \frac{q_m}{1-a}\right)$$

Demostración.

$$\begin{aligned}
H(p_1, \ldots, p_n, q_1, \ldots, q_m) &= \sum_{i=1}^{n} p_i \log \frac{1}{p_i} + \sum_{i=1}^{m} q_i \log \frac{1}{q_i} = \sum_{i=1}^{n} p_i \log \frac{a}{ap_i} + \sum_{i=1}^{m} q_i \log \frac{1-a}{(1-a)q_i} = \\
&= \sum_{i=1}^{n} p_i \left(\log \frac{a}{p_i} + \log \frac{1}{a}\right) + \sum_{i=1}^{m} q_i \left(\log \frac{1-a}{q_i} + \log \frac{1}{1-a}\right) = \\
&= \sum_{i=1}^{n} p_i \log \frac{a}{p_i} + \sum_{i=1}^{n} p_i \log \frac{1}{a} + \sum_{i=1}^{m} q_i \log \frac{1-a}{q_i} + \sum_{i=1}^{m} q_i \log \frac{1}{1-a} = \\
&= a \log \frac{1}{a} + (1-a) \log \frac{1}{1-a} + \sum_{i=1}^{n} p_i \log \frac{a}{p_i} + \sum_{i=1}^{m} q_i \log \frac{1-a}{q_i} = \\
&= H(a, 1-a) + a \sum_{i=1}^{n} \frac{p_i}{a} \log \frac{a}{p_i} + (1-a) \sum_{i=1}^{m} \frac{q_i}{1-a} \log \frac{1-a}{q_i} = \\
&= H(a, 1-a) + aH\left(\frac{p_1}{a}, \ldots, \frac{p_n}{a}\right) + (1-a)H\left(\frac{q_1}{1-a}, \ldots, \frac{q_m}{1-a}\right)
\end{aligned}$$

□

Vamos ahora a ver cual es el rango de la función de entropía. Más concretamente vamos a demostrar el siguiente.

Teorema 1.2. *Sea X una variable aleatoria discreta con n sucesos posibles. Entonces*

$$0 \leq H_b(X) \leq \log_b n$$

Además $H_b(X) = 0$ precisamente si $P(X = x) = 1$ para algún suceso x y $H_b(X) = \log_b n$ si y sólo si la distribución de probabilidad de X es uniforme.

Para demostrar el Teorema 1.2 necesitaremos dos lemas. El primero es bien conocido:

Lema 1.1. *Para todo número real positivo x se verifica $\log x \leq x - 1$ y la igualdad se verifica precisamente si $x = 1$.*

El segundo es un poco más complicado:

Lema 1.2. *Sea* $P = (p_1, \ldots, p_n)$ *una distribución de probabilidad y* $Q = (q_1, \ldots, q_n) \in \mathbb{R}^n$ *con* $0 \leq q_i \leq 1$ *y* $\sum_{i=1}^n q_i \leq 1$. *Entonces*

$$\sum_{i=1, p_i \neq 0}^{n} p_i \log \frac{1}{p_i} \leq \sum_{i=1, q_i \neq 0} p_i \log \frac{1}{q_i}$$

Además la igualdad se verifica precisamente si $p_i = q_i$ *para todo* i.

Demostración. Del lema 1.1 se tiene que si $p \neq 0$ y $q \neq 0$ entonces

$$\log \frac{q}{p} \leq \frac{q}{p} - 1$$

y, por tanto,

$$p \log \frac{1}{p} \leq p \log \frac{1}{q} + q - p$$

Puesto que $\sum_{i=1}^n q_i \leq 1 = \sum_{i=1}^n p_i$, se tiene

$$\sum_{i=1, p_i \neq 0}^{n} p_i \log \frac{1}{p_i} \leq \sum_{i=1, p_i \neq 0, q_i \neq 0}^{n} \left(p_i \log \frac{1}{q_i} + q_i - p_i \right) \leq \sum_{i=1, q_i \neq 0}^{n} p_i \log \frac{1}{q_i}$$

Supongamos que se da la igualdad, esto es,

$$\sum_{i=1, p_i \neq 0}^{n} p_i \log \frac{1}{p_i} = \sum_{i=1, q_i \neq 0} p_i \log \frac{1}{q_i}$$

Entonces,

$$p_i \log \frac{1}{p_i} = p_i \log \frac{1}{q_i} + q_i - p_i$$

para todo i con $p_i \neq 0$ y $q_i \neq 0$, o equivalentemente,

$$\log \frac{q_i}{p_i} = \frac{q_i}{p_i} - 1$$

Pero del lema 1.1, esto equivale a que $p_i = q_i$ para todo i.

□