Criptografía

Profesores del curso:

Ronald Mass [1]

Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

1 de septiembre de 2020

Tabla de contenidos

Transformaciones de ciframiento y desciframiento

Una **transformación de ciframiento** (o función de ciframiento) es una función biyectiva $E_e : \mathcal{M} \to \mathcal{C}$ donde la clave $e \in \mathcal{K}$ determina de forma única E_e que actúa sobre los mensajes de **texto plano** $M \in \mathcal{M}$ para obtener el **mensaje cifrado** $c = E_e(m) \in \mathcal{C}$.

Una **transformación de desciframiento** (o función de desciframiento) es una función biyectiva $D_d : \mathcal{C} \to \mathcal{M}$ el cual es únicamente determinado por la clave $d \in \mathcal{K}$ que actúa sobre un **mensaje cifrado** $c \in \mathcal{C}$ para obtener el **mensaje plano** $m = D_d(m) \in \mathcal{M}$.

Criptosistema

Un **criptosistema** está compuesto de un conjunto $\{E_e \,/\, e \in \mathcal{K}\}$ consistiendo de transformaciones de cifrado y el correspondiente conjunto $\{E_e^{-1} \,/\, e \in \mathcal{K}\} = \{D_d \,/\, d \in \mathcal{K}\}$ de transformaciones de descifrado. En otras palabras, para cada $e \in \mathcal{K}$ existe un único $d \in \mathcal{K}$ tal que $D_d = E_e^{-1}$ de modo que $D_d(E_e(m)) = m$ para todo $m \in \mathcal{M}$.

Observaciones

1. El caso donde $e = d$ o cuando uno de ellos puede ser **fácilmente determinado** a partir del otro, es llamado **cifrado de clave simétrica**. Este tipo de cifrado es de los más simples y tienen una mayor historia. También son llamados de **clave simple** y **convencional**.
2. Por convención se usan **letras minúsculas** para el texto plano y **letras mayúsculas** para el texto cifrado.

Tabla de contenidos

Cifrados afines

Sea
$\mathcal{M} = \mathcal{C} = \mathbb{Z}_n,\ n \in \mathbb{N},\ \mathcal{K} = \{(a, b) \,/\, a, b \in \mathbb{Z}_n \quad \wedge \quad mcd(a, n) = 1\}$
y para $e, d \in \mathcal{K}$ y $m, c \in \mathbb{Z}_n$ defina:

$$E_e(m) \equiv (am + b)\, mod\, n \quad \text{y} \quad D_d(c) \equiv a^{-1}(c - b) mod\, n.$$

Ejemplo:
El **cifrado de Julio César** está basado en desplazar 3 letras a la derecha de un alfabeto dado. La siguiente tabla da el cifrado de Julio César para el alfabeto en español:

Texto plano:	a	b	c	d	e	f	g	h	i	j	k	l
Texto cifrado:	D	E	F	G	H	I	J	K	L	M	N	O
Texto plano:	m	n	o	p	q	r	s	t	u	v	w	x
Texto cifrado:	P	Q	R	S	T	U	V	W	X	Y	Z	A
Texto plano:	y	z										
Texto cifrado:	B	C										

Asignando números a cada letra del cifrado de Julio César, se obtiene la siguiente tabla:

Texto plano	a	b	c	d	e	f	g	h	i	j	k	l
	0	1	2	3	4	5	6	7	8	9	10	11
Texto cifrado	D	E	F	G	H	I	J	K	L	M	N	O
	3	4	5	6	7	8	9	10	11	12	13	14
Texto plano	m	n	o	p	q	r	s	t	u	v	w	x
	12	13	14	15	16	17	18	19	20	21	22	23
Texto cifrado	P	Q	R	S	T	U	V	W	X	Y	Z	A
	15	16	17	18	19	20	21	22	23	24	25	1
Texto plano	y	z										
	24	25										
Texto cifrado	B	C										
	2	3										

Por tanto, de lo descrito, el cifrado de Julio César define una transformación afin E_e únicamente determinado por la clave $e = 3$, es decir:

$$E_3(m) = c \equiv m + 3 (mod\, 26)$$

donde $m \in \mathcal{M}$ es el equivalente numérico del texto plano según la tabla anterior.
Análogamente, $D_3(c)$ es la transformación de desciframiento únicamente determinado por la clave $d = 3$, el cual se obtiene por sustracción modular de 3 módulo 26, es decir:

$$D_3(c) = m \equiv c - 3 (mod\, 26)$$

donde $c \in \mathcal{C}$ es el equivalente numérico del texto cifrado según la tabla anterior.

Ejemplo:

Cifre el texto: " dinero " usando:

$$E_5(m) = 5m + 9(mod\, 26).$$

Además determine la función de descriframiento D_d.

Solución:
Usando la función de ciframiento E_5 sobre la tabla de Julio César, se obtiene:

Texto plano	d	i	n	e	r	o
	3	8	13	4	17	14
Texto cifrado						

Para determinar la función de desciframiento, necesitamos calcular $5^{-1}(mod\, 26)$ (Ejercicio).

Cifrado de Hill

- Expliquemos en qué consiste el cifrado de Hill. En primer lugar, se asocia cada letra del alfabeto con un número. La forma más sencilla de hacerlo es con la asociación natural ordenada, aunque podrían realizarse otras asociaciones diferentes. Además, en este ejemplo solamente vamos a utilizar las letras dadas para el alfabeto en español utilizada en el ciframiento de Julio César.

¿Cómo funciona?

1. Supongamos que tenemos una matriz invertible $A_{n\times n}$ (la matriz de codificación) y un texto que queremos **cifrar** M.
2. **Transformamos** el texto (M) a una secuencia de números, dando a cada carácter un valor numérico único; a continuación, formamos una matriz mediante la agrupación de los números en columnas de acuerdo al orden de la matriz $A_{n\times n}$. Llamemos a esta matriz $T_{n\times k}$ (la matriz plana), es decir

   El mensaje M se transfoma a la matriz numérica $T_{n\times k}$

3. Multiplicando la matriz A por la matriz T, se obtiene la **matriz cifrada** $C_{n\times k}$, es decir

$$C = A \cdot T.$$

¿Cómo funciona? (cont.)

4. Para **descifrar el mensaje**, sólo debe multiplicarse $A^{-1}C = T$.
5. El texto plano original se puede hallar nuevamente tomando la matriz resultante y uniendo sus vectores columna, de manera que formen una secuencia, para luego convertir los números en los caracteres respectivos.

Example 1

Dada la matriz de codificación $A = \begin{pmatrix} 3 & 2 & 5 \\ 0 & 9 & -1 \\ 2 & 3 & 4. \end{pmatrix}$, se tiene el texto $M =$"COVIDDIECINUEVE" a cifrar. Luego,

- Transforme el mensaje M a la matriz numérica T
- Halle la matriz cifrada C
- Descifre el mensaje, es decir, halle $A^{-1}C$