# Cátedra No. 1 : 6 de Agosto

*Transcriptor: Marcos Kiwi*

Tradicionalmente, la criptografía ha consistido en el estudio de métodos que permitan el envío de mensajes entre dos partes interesadas, a través de un canal inseguro monitoreado por un adversario o espía, y de forma que sólo aquellos a los cuales los mensajes van dirijidos puedan entender lo que se esta diciendo.

El dramático aumento en la capacidad y la interconectividad de los computadores modernos ha llevado a una redefinición de los objetivos y el ámbito de la criptografía. La criptografía moderna aborda temas como la autentificación, verificación de integridad, no-repudiación, firmas digitales, dinero electrónico, etc.

Comenzamos este curso presentando, brevemente, nociones básicas de criptografía clásica. Esto lo hacemos por razones históricas, y porque nos permitirá introducir ciertos conceptos importantes sin entrar en mayores complicaciones técnicas.

## 1 Criptografía Clásica

La criptografía clásica tipicamente considera el escenario en que dos partes interesadas, que llamaremos Alicia y Roberto, quieren comunicarse a través de un canal inseguro. Este canal inseguro esta monitoriado por un adversario o espía que llamaremos Eva. Ejemplos típicos de canales inseguros son: una línea telefónica, una red computacional, el correo, etc.

La información que Alicia quiere enviarle a Roberto la llamaremos *texto plano*. Para evitar que Eva comprenda lo que Alicia le quiere decir a Roberto, Alicia encripta el texto plano, utilizando una clave, y obtiene el *texto cifrado* el cual envia a Roberto. Roberto, que asumimos conoce la clave que se usó en la encripción, puede descifrar el mensaje, pero Eva que sólo ve el texto cifrado no debería ser capaz de determinar el texto plano.

Formalmente tenemos la siguiente

**Definición 1** *Un criptosistema es una tupla* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *tal que:*

- $\mathcal{P}$ *es un conjunto de posibles textos planos.*

- *$\mathcal{C}$ es un conjunto de posibles textos cifrados.*
- *$\mathcal{K}$ es un conjunto de posibles claves.*
- *Para toda clave $K \in \mathcal{K}$, hay una* función de encripción $e_K \in \mathcal{E}$ *y una correspondiente* función de decripción $d_K \in \mathcal{D}$, *donde* $e_K \colon \mathcal{P} \to \mathcal{C}$, $d_K \colon \mathcal{C} \to \mathcal{P}$ *y* $d_K(e_K(x)) = x$, *cualquiera sea* $x \in \mathcal{P}$.

A continuación discutimos la forma en que Alicia y Roberto emplean un criptosistema. Primero eligen una clave $K \in \mathcal{K}$ (cuando no pueden ser observados por Eva). Más tarde, cuando Alicia quiere enviar a Roberto el texto plano $x = x_1 \ldots x_n$, $x_i \in \mathcal{P}$, $i = 1, \ldots, n$, esta determina $y_i = e_K(x_i)$, $i = 1, \ldots, n$ y envía $y = y_1, \ldots, y_n$. Una vez que Roberto recibe el texto cifrado $y$, este obtiene el texto plano $x$ utilizando la función de decripción $d_K$, i.e. calcula $x_i = d_K(y_i)$, $i = 1, \ldots, n$.

Para que la decripción no sea ambigua, se debe tener que $e_K$ debe ser una función inyectiva cualquiera sea $K \in \mathcal{K}$. Más aun, en el caso que $\mathcal{P} = \mathcal{C}$ (como usualmente se da), se tiene que $e_K$ debe ser una permutación de $\mathcal{P}$, para todo $K \in \mathcal{K}$.

Si un criptosistema ha de ser de alguna utilidad, entonces debe satisfacer ciertas propiedades básicas. Entre ellas:

- Las funciones de encripción $e_K$ y decripción $d_K$ deben poder calcularse en forma computacionalmente eficiente.[1]
- A un adversario que conoce el texto cifrado y desconoce la clave $K$ le debe ser difícil determinar $K$ o el texto plano $x$ tal que $e_K(x) = y$.

La segunda de estas propiedades intenta capturar de forma muy vaga la noción de *seguridad*. A medida que el curso progrese iremos precisando este concepto.

En las secciones que siguen veremos algunos ejemplos concretos de criptosistemas cuyo interés es más que nada de caracter histórico.

# 2 Criptosistemas Mono-alfabéticos

En este caso las funciones de encripción corresponden a transformaciones de los caracteres alfabéticos de los cuales puede consistir el texto plano.

[1] Formalmente, deben poder ser calculadas por una máquina de Turing probabilista en tiempo polinomial.

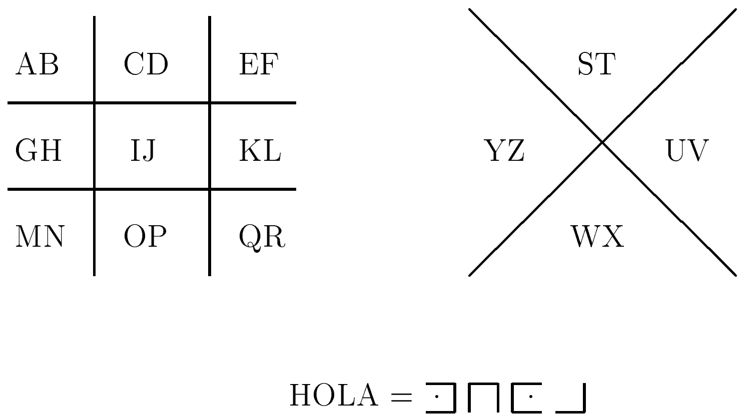


Figure 1: Cifrado de la masonería.

## 2.1 Cifrados de Sustitución

En estos casos $|\mathcal{P}| = |\mathcal{C}|$. De hecho, a menudo $\mathcal{P} = \mathcal{C}$. Tipicamente $\mathcal{P}$, $\mathcal{C}$ corresponden al alfabeto, a un conjunto de números, un conjunto de símbolos, etc. En estos criptosistemas cada función de encripción $e_K$ corresponde a una biyección entre $\mathcal{P}$ y $\mathcal{C}$, y la correspondiente función de decripción $d_K$ es la inversa de $e_K$ (que existe pues $e_K$ es biyección).

Ejemplos de códigos de sustitución son algunos de los criptosistemas utilizados por la masonería, uno de los cuales se ilustra en la Figura 2.1.

A continuación estudiaremos otros dos códigos de sustitución.

## 2.2 Cifrado por Corrimiento

En el cifrado por corrimiento[2] $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{Z}_m$, y para todo $x \in \mathcal{P}$, $y \in \mathcal{C}$

$$\begin{aligned} e_K(x) &= (x + K) \bmod m\,, \\ d_K(y) &= (y - K) \bmod m\,, \end{aligned}$$

donde $a \bmod b$, $|b| \geq 1$, denota el único número $r \in \{0, \ldots, |b|-1\}$ tal que $a = kb + r$ para algun entero $k$ (i.e. si $a$ y $b$ son positivos, $a \bmod b$ es el resto que se obtiene de dividir $a$ por $b$).

[2] *Shift cipher.*

Tipicamente $m = 27$ y $j \in \mathcal{Z}_m$ representa la $j$-ésima letra del alfabeto (es decir 0 representa $A$, 1 representa $B$, ..., 26 representa $Z$). ROT13 es un ejemplo de este tipo de criptosistemas el cual es a menudo utilizado para obscurecer el contenido de mensajes enviados a newsgroups y que pueden ser ofensivos para algunas personas.

## 2.3 Cifrado Afín

En este caso $\mathcal{P} = \mathcal{C} = \mathcal{Z}_m$, y

$$\mathcal{K} = \{(a, b) \in \mathcal{Z}_m \times \mathcal{Z}_m \mid \mathrm{mcd}(a, m) = 1\}.$$

Equivalentemente, $\mathcal{K}$ es el conjunto de tuplas $(a, b)$ de números en $\mathcal{Z}_m$ tales que $a$ y $m$ son primos relativos. Luego, de un resultado básico de la aritmética modular[3] sigue que $a$ tiene un inverso multiplicativo, denotado $a^{-1}$, en $\mathcal{Z}_m$. Si $K = (a, b) \in \mathcal{K}$, para todo $x \in \mathcal{P}$, $y \in \mathcal{C}$

$$\begin{aligned} e_K(x) &= (a\,x + b) \bmod m\,, \\ d_K(y) &= a^{-1}\,(y - b) \bmod m\,. \end{aligned}$$

Tipicamente $m = 27$ y $j \in \mathcal{Z}_m$ representa la $j$-ésima letra del alfabeto (es decir 0 representa $A$, 1 representa $B$, etc.).

La seguridad de un criptosistema radica, en parte, en el tamaño del conjunto de claves $\mathcal{K}$. Si la cardinalidad de $\mathcal{K}$ es demasiado pequeña entonces es posible ciclar sobre todo $\mathcal{K}$ y determinar $d_K(y)$ para todas las claves $K \in \mathcal{K}$. Muchas veces, por contexto, podemos determinar cual texto plano $d_K(y)$ es el único que tiene sentido. A continuación determinaremos $|\mathcal{K}|$ para el cifrado afín.

**Definición 2** *El número de enteros en $\mathcal{Z}_m$ que son relativamente primos a $m$ es $\phi(m)$ donde $\phi$ es la función-phi de Euler.*

Más adelante probaremos que la función-phi de Euler es multiplicativa, es decir,

**Proposición 1** *$\phi(m\,n) = \phi(m)\,\phi(n)$, si $m, n$ son enteros positivos relativamente primos.*

Luego podemos concluir el siguiente

[3] La próxima cátedra repasaremos conceptos relacionados con aritmética modular y discutiremos la complejidad de cálculo de algunas operaciones en $\mathcal{Z}_m$.

**Lema 1** *Si $m$ es tal que $m = \prod_{i=1}^{n} p_i^{e_i}$, donde los $p_i$ son números primos distintos, y los $e_i$ son enteros positivos, entonces*

$$\phi(m) \;=\; \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i-1}) \,.$$

**Dem:** Por la propieda multiplicativa de $\phi$ sigue que $\phi(m) = \prod_{i=1}^{n} \phi(p_i^{e_i})$. Pero si $p$ es primo, y $e$ es un entero positivo es fácil ver que los únicos números en $\{1, \ldots, p^e - 1\}$ que no son primos relativos con $p^e$ son los múltiplos de $p$, de los cuales hay $p^{e-1}$. Luego, $\phi(p^e) = p^e - p^{e-1}$, de donde se conluye el resultado buscado. $\square$

Luego, el número de claves del cifrado afín sobre $\mathcal{Z}_m$ es $(m\,\phi(m))$. Observar que conocida la factorización de $m$ es fácil calcular $\phi(m)$. De hecho no se conoce un algoritmo eficiente para determinar $\phi(m)$ desconocida la factorización de $m$. El siguiente resultado sugiere que de existir dicho algoritmo no va a ser fácil encontrarlo.

**Proposición 2** *Si $m$ es el producto de dos primos $p$ y $q$ distintos, entonces la determinación de $p$ y $q$ es equivalente a la determinación de $\phi(m)$. Más precisamente, uno puede calcular eficientemente $\phi(m)$ conocidos $p$ y $q$, y conocido $\phi(m)$ se puede determinar eficientement $p$ y $q$.*

**Dem:** Como $\phi(m) = (p-1)(q-1) = m + 1 - (p+q)$, si $p$ y $q$ son conocidos entonces $\phi(m)$ se obtiene como el resultado de un par de sumas.

Si $\phi(m)$ es conocido, $p$ y $q$ se obtienen resolviendo el sistema $pq = m$ y $\phi(m) = m + 1 - (p+q)$, lo que requiere el cálculo de una raiz cuadrada. El cálculo de la raiz cuadrada es la operación más costosa y domina el tiempo involucrado en la ejecución de las otras operaciones requeridas. $\square$

# 3 Criptosistemas Poli-alfabéticos

En estos criptosistemas cada caracter alfabético del que esta compuesto el texto plano puede ser encriptado de distintas maneras.

## 3.1 Cifrado de Hill

En este caso $\mathcal{P} = \mathcal{C} = (\mathcal{Z}_m)^n$, y $\mathcal{K}$ es el conjunto de matrices invertibles de $m \times m$ cuyas coordenadas estan en $\mathcal{Z}_m$, es decir

$$\mathcal{K} \;=\; \{K \in M_n(\mathcal{Z}_m) \,|\, K \text{ es invertible } \}\,.$$

Además, para todo $x \in \mathcal{P}$, $y \in \mathcal{C}$

$$\begin{aligned} e_K(x) &= Kx, \\ d_K(y) &= K^{-1}y\,. \end{aligned}$$

donde todas las operaciones se realizan sobre $\mathcal{Z}_m$.

Tipicamente $m = 27$, $j \in \mathcal{Z}_m$ representa la $j$-ésima letra del alfabeto (es decir 0 representa $A$, 1 representa $B$, etc.), y cada elemento de $\mathcal{P}$ representa una secuencia de $n$ letras.

Ponemos término a esta sección dando algunas caracterizaciones equivalentes de invertivilidad.

**Proposición 3** *Sea $A \in M_n(\mathcal{Z}_m)$, las siguientes afirmaciones son equivalentes:*

- $\mathrm{mcd}(\det(A), m) = 1$,
- *$A$ es invertible,*
- *la transformación que a $x \in (\mathcal{Z}_m)^n$ le asocia $A\,x \in (\mathcal{Z}_m)^n$ es inyectiva.*
- *si $x \in (\mathcal{Z}_m)^n$ es tal que $x \neq \vec{0}$ entonces $A\,x \neq \vec{0}$,*

**Dem:** Si $D = \mathrm{mcd}(\det(A), m) = 1$, entonces $D$ tiene inverso multiplicativo en $\mathcal{Z}_m$ y la inversa de la matriz $A$ exise y esta dada por $B \in M_n(\mathcal{Z}_m)$ tal que $B_{j,i} = D^{-1}\,(-1)^{i+j}\det(A_{i,j})$ (observar que los índices se invierten), y donde $A_{i,j} \in M_{n-1}(\mathcal{Z}_m)$ es la matriz que se obtiene de $A$ al eliminar la $i$-ésima fila y la $j$-ésima columna.

Si $A$ es invertible entonces $A\colon (\mathcal{Z}_m)^n \to (\mathcal{Z}_m)^n$ es una biyección, en particular es inyectiva.

Si $A\colon (\mathcal{Z}_m)^n \to (\mathcal{Z}_m)^n$ es inyectiva entonces, de un resultado básico del álgebra lineal, se tiene que $\mathrm{Ker}(A) \stackrel{\text{def}}{=} \{x \in \mathcal{Z}_m \,|\, Ax = 0\} = \{(0, \ldots, 0)\} \subseteq (\mathcal{Z}_m)^n$.

Demostraremos que la última afirmación implica la primera para el caso en que $n = 2$. La generalización es directa pero tediosa. Sea entonces

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Supongamos que $D = \det A$ y $m$ no son primos relativos, i.e. $d = \mathrm{mcd}(D, m) > 1$. Sea $m' = m/d$. La demostración se descompone en tres casos. (En lo que sigue todas las operaciones aritméticas son sobre $\mathcal{Z}_m$.)

**Caso 1:** Si todas las componentes de $A$ son divisibles por $d$ y $x = \begin{pmatrix} m' \\ m' \end{pmatrix}$ sigue que $Ax = 0$ lo que constituye una contradicción.

**Caso 2:** Si $a$ y $b$ no son ambos divisibles por $d$. Haciendo $x = \begin{pmatrix} -bm' \\ am' \end{pmatrix}$ y dado que $D = ac - bd$ sigue que $Ax = \begin{pmatrix} 0 \\ Dm' \end{pmatrix}$, contradicción.

**Caso 3:** Si $c$ y $d$ no son ambos divisibles por $d$ se procede como en el caso anterior.

$\square$