MA-53G Intr. a la Criptografía | **Semestre Otoño, 1998**

Cátedra No. 2 : 17 de Marzo

Transcriptor: Rodrigo Meza[1]

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 el conjunto y determinar $d_K(y)$ para todas las claves $K \in \mathcal{K}$. Muchas veces, por contexto, podemos determinar cual texto puro $d_K(y)$ es el único que tiene sentido. A continuación determinaremos $|\mathcal{K}|$ para el cifrado afín.

Definición 1 *El número de enteros en $\mathcal{Z}_m$ que son relativamente primos a m es $\phi(m)$ donde ϕ 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

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*

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

Dem: Por la propiedad multiplicativa de ϕ 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 1 y 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 conocido 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 eficientemente p y q.*

[1] Estos apuntes están basados en la transcripción de Marcos Kiwi (6/8/96)

Dem: Por el lema antes visto, sabemos que

$$\begin{aligned}\phi(m) &= (p-1)(q-1)\\ &= pq-p-q+1.\end{aligned}$$

Luego, conocidos p y q se puede calcular $\phi(m)$ con un costo esencialmente equivalente al de multiplicar p y q.

Por otro lado:

$$\begin{aligned}p+q &= m-\phi(m)+1\\ pq &= m.\end{aligned}$$

De la misma forma, p y q se pueden calcular conociendo $\phi(m)$ y m con un costo similar al cálculo de una ra'iz cuadrada. Este cálculo es la operación más costosa y domina el tiempo involucrado en la ejecución de las otras operaciones requeridas.

□

1 Criptosistemas Poli-alfabéticos

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

1.1 Cifrado de Hill

En este caso $\mathcal{K}$ está definido sobre el conjunto de matrices invertibles de $n \times n$ cuyas coordenadas estan en $\mathcal{Z}_m$, es decir,

$$\mathcal{K} \;=\; \{(n,m,A)\,|\,n,m \in N^* \; y \; A \in M_n(\mathcal{Z}m)\}\,.$$

y para $k=(n,m,A)$ se cumple que $\mathcal{P}_k=\mathcal{C}_k=(\mathcal{Z}m)^n$.
Además, para todo $x \in \mathcal{P}$, $y \in \mathcal{C}$

$$\begin{aligned}e_k(x) &= Ax,\\ d_k(y) &= A^{-1}y\,.\end{aligned}$$

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 invertibilidad.

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

- $\mathrm{mcd}(\mathit{det}(A), m) = 1$,
- *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 está 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: $(\mathcal{Z}_m)^n \to (\mathcal{Z}_m)^n$ es una biyección, en particular es inyectiva.

Si A: $(\mathcal{Z}_m)^n \to (\mathcal{Z}_m)^n$ es inyectiva entonces, de un resultado básico del álgebra lineal, se tiene que $\ker(A) = \{x \in \mathcal{Z}_m \mid Ax = 0\} = \{(0,\ldots,0)\} \subseteq (\mathcal{Z}_m)^n$.

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.

$\square$

2 Cifrados de Flujo

En los criptosistemas que hemos estudiado hasta ahora, hemos encriptado el texto puro utilizando la misma clave K de forma que el texto cifrado $y = y_1 y_2 \ldots = e_K(x_1) e_K(x_2) \ldots$. Los criptosistemas que se obtienen utilizando esta forma de encriptar se conocen como *cifrados en bloque.*[2]

En este curso nos remitiremos principalmente al estudio de este tipo de criptosistemas. Sin embargo hay otras alternativas. Por completitud discutiremos una de ellas en esta sección: los *cifrados de flujo.*[3]

La idea básica de este tipo de cifrados es generar una secuencia de claves $K = z_1 z_2 \ldots$, y usarla para encriptar el texto puro $x = x_1 x_2 \ldots$, como sigue:

$$y \;=\; y_1 y_2 \ldots \;=\; e_{z_1}(x_1) e_{z_2}(x_2) \ldots$$

Formalmente,

Definición 2 *Un cifrado de flujo es una tupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{F}, \mathcal{E}, \mathcal{D})$ tal que:*

- *$\mathcal{P}$ es un conjunto de posibles textos puros.*
- *$\mathcal{C}$ es un conjunto de posibles textos cifrados.*
- *$\mathcal{K}$ es un conjunto de posibles claves.*
- *$\mathcal{L}$ es un conjunto denominado alfabeto de claves de flujo.*
- *$\mathcal{F} = (f_1, f_2, \ldots)$ es tal que $\forall\, i \geq 1$, $f_i \colon \mathcal{K} \times \mathcal{P}^{i-1} \rightarrow \mathcal{L}$.*
- *Para cada $z \in \mathcal{L}$, hay una* función de encripción *$e_z \in \mathcal{E}$ y una correspondiente* función de decripción *$d_z \in \mathcal{D}$, donde $e_z \colon \mathcal{P} \rightarrow \mathcal{C}$, $d_z \colon \mathcal{C} \rightarrow \mathcal{P}$ y $d_z(e_z(x)) = x$, cualquiera sea $x \in \mathcal{P}$.*

A continuación discutimos la forma en que Alicia y Roberto emplean un criptosistema como el anterior.

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 puro $x = x_1 x_2 \ldots$, $x_i \in \mathcal{P}$, $i = 1, 2, \ldots$, esta determina $z_i = f_i(K, x_1, \ldots, x_{i-1})$, y envía $y_i = e_{z_i}(x_i)$. En general, Alicia determinará $z_1, y_1, z_2, y_2, \ldots$ secuencialmente. (Es importante notar, que la encripción de x_i depende no sólo de K sino que también de $x_1 x_2 \ldots x_{i-1}$.) Una vez que Roberto recibe el texto cifrado $y = y_1 y_2 \ldots$, este obtiene el texto puro calculando secuencialmente $z_1, x_1, z_2, x_2, \ldots$ determinando primero $z_i = f_i(K, x_1, \ldots, x_{i-1})$ y luego $x_i = d_{z_i}(y_i)$.

Claramente, los cifrados en bloque son un caso especial de los cifrados de flujo donde $z_i = K$, para todo $i \geq 1$.

La utilidad de los cifrados de flujo radica en que usualmente se pueden implementar a nivel de hardware en forma muy eficiente.

[2] *Block chiphers.*
[3] *Stream ciphers.*

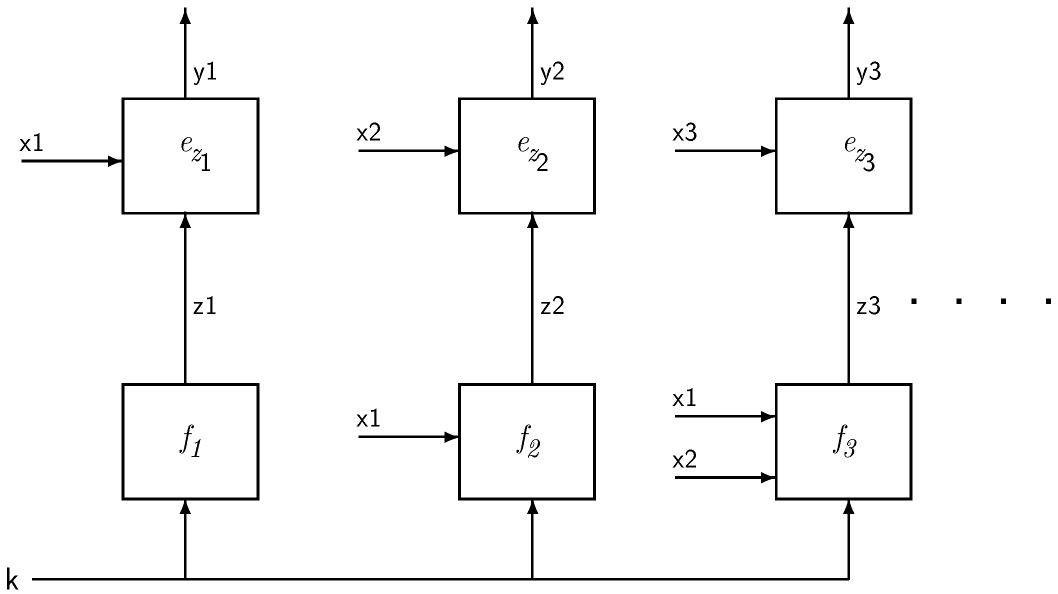

Figura 1: Método de encripción por cifrado de flujo.

Veamos un ejemplo de este tipo de cifrados. Consideremos $\mathcal{P} = \mathcal{C} = \mathcal{L} = \mathcal{Z}_2$ y $\mathcal{K} = (\mathcal{Z}_2)^m \setminus \{(0, \ldots, 0)\}$. Supongamos que comenzamos con $K = (z_1, \ldots, z_m) \in \mathcal{K}$ y hacemos que

$$z_{i+m} \quad = \quad (\sum_{j=0}^{m-1} c_j \, z_{i+j}) \bmod 2 \,,$$

donde $c_0, \ldots, c_{m-1} \in \mathcal{Z}_2$ estan fijos. Finalmente hacemos

$$\begin{aligned} e_z(x) &= (x + z) \bmod 2 \,, \\ d_z(y) &= (y - z) \bmod 2 \,. \end{aligned}$$

Más adelante en el curso, cuando estudiemos DES (*Data Encryption Standard*), veremos otros ejemplos del tipo de encripción discutido en esta sección.

3 Algunos otros métodos

Los métodos de encriptación monoalfabéticos han sido bastamente usados a través de la historia. Al finalizar esta sección, queremos entregar algunas de las técnicas criptográficas monoalfabéticas más usadas.

3.1 Cifrado de Cesar

Esta es una de las técnicas monoalfabéticas más simples. Debe su nombre a Julio Cesar de quien se dice la ocupaba para escribir a sus colaboradores más cercanos. El método es simple, y consiste en que cada letra del alfabeto es reemplazada por la letra ubicada a tres espacios más adelante en el alfabeto en el alfabeto, y donde el alfabeto se considera circular, es decir, las letras x, y y z se codifican como a, b y c respectivamente. Esta técnica corresponde a los llamados cifrados por corrimiento ya analizados, usando como constantes $a = 3\,, m = 26$.
En la literatura se puede encontrar que a los cifrados por corrimiento en general se les llama también cifrados de Cesar.

3.2 Atbash

El cifrado Atbash es otra técnica monoalfabética. Tiene origen jud'io y consiste en invertir el orden de las letras en el abecedario. De esta forma, la Z representa a la A, la Y reemplaza a la B, etcétera.
La tabla de reemplazos es la siguiente:

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

El Atbash es aún más sencillo de descifrar que los criptosistemas por corrimiento, pues existe sólo una solución a intentar.

3.3 Playfair

A diferencia de los sistemas que ya hemos visto, el *Play fair* es un criptosistema poli-alfabético.
La forma en que trabaja consiste en generar una matriz $M \in M_{55}$ con las letras del abecedario. como las letras son 26, la i y la j se ponen juntas, pues el contexto nos es suficiente para determinar cual usar.

La forma de generar esta matriz puede variar. Una de las más conocidas es generarla a partir de una palabra clave, y luego poner las letras resultantes en forma horizontal, eliminando las repeticiones y poner las letras restantes bajo ella. Por ejemplo, usando la palabra *computador*, tenemos lo siguiente:

C	O	M	P	U	T	A	D	R
B	E	F	G	H	I	K	L	N
Q	S	V	W	X	Y	Z	-	-

Figura 2: Algunos de los bailarines del cuento de Edgard Allan Poe

Luego, se leen las letras por columnas y se genera la matriz.

C	B	Q	O	E
S	M	F	V	P
G	W	U	H	X
T	IJ	Y	A	K
Z	D	L	R	N

Para codificar cualquier texto, es necesario separarlo en grupos de dos caracteres. Luego, para cada par de letras, se considera la submatriz que contiene ambas letras como vértices y en un orden predeterminado, se escriben las otras letras que son vértices de esta submatriz.
Por ejemplo, para codificar el par de letras *hm*, se codifica como *wv*, pues son los vértices opuestos en la submatriz que forman.

3.4 El caso de los bailarines

Entre los cifrados por sustitución de s'imbolos existen muchis'imos. En la literatura se pueden encontrar algunos famosos, como en "el caso de los danzarines" donde Allan Poe pone a su personaje Sherlock Holmes en el dilema de descifrar la correspondencia entre cada bailar'in como los de la Figura 3.4 y los caracteres del alfabeto. En general este y todos los cifrados de sustitución monoalfabéticos tienen la desventaja de ser muy fáciles de decriptar, analizando la frecuencia de los signos y asociándola a las letras del alfabeto.

4 Quebrando los códigos cl'asicos

En general los códigos cl'asicos como los que aqu'i hemos descrito, han sido bastamente analizados, y es as'i como los métodos para quebrarlos estan bastante bien descritos en la literatura.
Las técnicas se basan fundamentalmente en:

- Como en general los criptosistemas monoalfabéticos se basan en claves con $|\mathcal{K}|$ muy peque'no, es fácil iterar sobre todas las llaves posibles y basándose en el contexto, decidir cual es la clave

a	7.81	h	5.85	o	8.21	v	1.00
b	1.28	i	6.77	p	2.15	w	1.49
c	2.93	j	0.23	q	0.14	x	0.30
d	4.11	k	0.42	r	6.64	y	1.51
e	13.05	l	3.60	s	6.46	z	0.09
f	2.88	m	2.62	t	9.02		
g	1.39	n	7.28	u	2.77		

Tabla 1: Distribución de frecuencia (en porcentajes) de las letras en el idioma inglés

a	13	h	1.2	'n	0.2	u	4.3
b	1.6	i	6.3	o	9.6	v	1.1
c	4	j	0.6	p	2.6	w	0.01
d	4.3	k	0.3	q	1.1	x	0.2
e	13.3	l	5.3	r	6.0	y	1.2
f	0.5	m	3.9	s	7.2	z	0.4
g	1.1	n	6.6	t	4.3		

Tabla 2: Distribución de frecuencia (en porcentajes) de las letras en el idioma espa'nol

utilizada.

- Otro m'etodo un poco m'as elaborado consiste en, teniendo una gran cantidad de texto cifrado, analizar la frecuencia de cada uno de los caracteres que en el aparecen. Los lenguajes guardan una frecuencia por cada letra muy precisa, y por lo tanto basta asociar cada letra con la frecuencia correspondiente, y obtendremos el texto puro.
  Este método es aplicable a todos los sistemas de sustitución, e incluso a algunos de cifrado por bloque, como el Play Fair, ya que las frecuencias de pares de letras también se encuentran tabuladas.

  En las tablas 1 y 2 se puede apreciar la distribución de frecuencias de caracteres para los idiomas ingles y espa'nol respectivamente.