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

Cátedra No. 1 : 16 de Marzo

Transcriptor: Marcos Kiwi[1]

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. Estos conceptos los iremos definiendo y estudiando a través del curso.

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 típicamente 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, ondas radiales, el telegrafo, etc.

La información que Alicia quiere enviarle a Roberto la llamaremos *texto puro* o *texto plano*. Para evitar que Eva comprenda lo que Alicia le quiere decir a Roberto, Alicia encripta el texto puro, 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 puro.

Formalmente tenemos la siguiente

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

- $\mathcal{K}$ *es un conjunto de posibles claves.*
- $\mathcal{E} = (e_K)_{K\in\mathcal{K}}$ *es una lista de funciones de encripción y* $\mathcal{D} = (d_K)_{K\in\mathcal{K}}$ *es una lista de funciones de decripción.*
- *Para toda clave* $K \in \mathcal{K}$, $e_K\colon \mathcal{P}_K \to \mathcal{C}_K$, $d_K\colon \mathcal{C}_K \to \mathcal{P}_K$ *y* $d_K(e_K(x)) = x$, *cualquiera sea* $x \in \mathcal{P}_\mathcal{K}$.

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

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 puro $x = x_1 \dots x_n$, $x_i \in \mathcal{P}_K$, $i = 1, \dots, n$, esta determina $y_i = e_K(x_i)$, $i = 1, \dots, n$ y envía $y = y_1, \dots, y_n$. Una vez que Roberto recibe el texto cifrado y, este obtiene el texto puro x utilizando la función de decripción d_K, *i.e.* calcula $x_i = d_K(y_i)$, $i = 1, \dots, n$.

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

Observación 1 *Por su modo de empleo, el criptosistema definido más arriba se denomina* criptosistema de bloque.[2] *El nombre se debe a que cualquier mensaje a ser enviado debe romperse en bloques cada uno de los que debe pertenecer al dominio de la función de encripción que se este utilizando.*

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

- Debe ser posible elegir un elemento K en $\mathcal{K}$ en forma computacionalmente eficiente. Formalmente, dado un parámetro de seguridad, debe ser posible elegir una clave por una máquina de Turing probabilista en tiempo polinomial.
- Las funciones de encripción e_K y decripción d_K deben poder calcularse en forma computacionalmente eficiente. Formalmente, deben poder ser calculadas por una máquina de Turing probabilista en tiempo polinomial.
- A un adversario que conoce el texto cifrado le debe ser difícil determinar la clave K o el texto puro x tal que $e_K(x) = y$.

La última 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. Pero antes identificaremos algunos conceptos con los que ya nos hemos topado.

1.1 Terminología y Conceptos Básicos

PARTICIPANTES EN LA COMUNICACIÓN: Una *entidad* o *parte* es un ente que envía, recive, o manipula información. Alicia y Roberto, mencionados anteriormente, son entidades. Una entidad puede ser una persona, pero también un terminal de computador, etc. Un *emisor* es una entidad en una comunicación que es la legítima originadora de la información que se envía, como por ejemplo Alicia mencionada anteriormente. Un *receptor* es una entidad en una comunicación que es un legítimo destinatario de información, como por ejemplo Roberto mencionada anteriormente. Un *adversario* es una entidad que participa en la comunicación, que no es ni emisor ni receptor, y que trata de burlar

[2] Block cipher.

el servicio de transmisión de información que esta siendo proveido entre el emisor y el destinatario. Otros sinónimos de adversario son: enemigo, atacante, oponente, intruso, etc. Frecuentemente un adversario tratará de jugar el rol de un legítimo emisor o receptor.

CANALES: Un *canal* es un medio de transmisión de información entre entidades. Un *canal físicamente seguro* es aquel que no puede ser accesado físicamente por un adversario. Un *canal inseguro* es aquel en que una entidad distinta a aquellas con las autorizaciónes adecuadas puede leer, borrar, insertar, o re–enviar mensajes. Un *canal seguro* es aquel en que ningúna entidad distinta a aquellas con las autorizaciónes adecuadas puede leer, borrar, insertar, o re–enviar mensajes. Un canal seguro no es necesariamente un canal físicamente seguro. En efecto, la seguridad de un canal puede ser garantizada por medios distintos a los físicos. En este curso nos abocaremos al estudio de los mecanismos que permiten asegurar un canal por medios que no son físicos.

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 puro.

2.1 Cifrados de Substitución

En estos casos $|\mathcal{P}_K| = |\mathcal{C}_K|$, para todo $K \in \mathcal{K}$. De hecho, a menudo $\mathcal{P}_K = \mathcal{C}_K$. Típicamente $\mathcal{P}_K$, $\mathcal{C}_K$ 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 $\mathcal{P}_K$ y $\mathcal{C}_K$, 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 substitución son algunos de los criptosistemas utilizados por la masonería, uno de los cuales se ilustra en la Figura 2.1. (Observar que en este ejemplo, sólo existe una clave, luego toda la seguridad del criptosistema se basa en mantenerlo secreto.)

A continuación estudiaremos otros dos códigos de substitución.

2.2 Cifrado por Corrimiento

En el cifrado por corrimiento[3] $\mathcal{K} = \{(a,m) \,|\, m \in \mathbb{N}^*, a \in \mathcal{Z}_m\}$, para todo $K = (k,m) \in \mathcal{K}$ se tiene que $\mathcal{P}_K = \mathcal{C}_K = \mathcal{Z}_m$, y para todo $x \in \mathcal{P}_K$, $y \in \mathcal{C}_K$

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

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

Típicamente $m = 27$ 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

[3] *Shift cipher.*

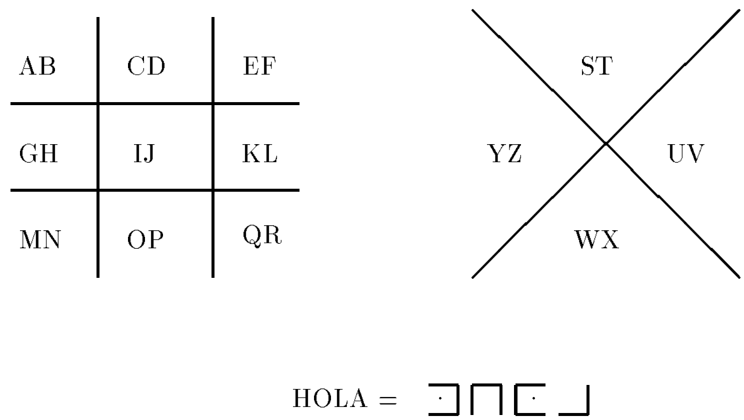

Figure 1: Cifrado de la masonería.

a menudo utilizado para obscurecer el contenido de mensajes enviados a newsgroups y que pueden ser ofensivos para algunas personas. Uno de los criptosistemas más antiguos conocidos, el de Julio Cesar, es también un código de substitución que consistía en substituir cada letra del alfabeto por aquella tres posiciones más adelante.

2.3 Cifrado Afín

En este caso

$$\mathcal{K} \quad = \quad \{(a,b,m) \mid m \in \mathbb{N}^*, a, b \in \mathcal{Z}_m,\ \text{y } \operatorname{mcd}(a,m) = 1\}\,,$$

y para $K = (a,b,m) \in \mathcal{K}$, $\mathcal{P}_K = \mathcal{C}_K = \mathcal{Z}_m$. Equivalentemente, $\mathcal{K}$ es el conjunto de tuplas (a,b,m) de números tales que $a, b \in \mathcal{Z}_m$ y a y m son primos relativos. Luego, de un resultado básico de la aritmética modular[4] sigue que a tiene un inverso multiplicativo en $\mathcal{Z}_m$, denotado a^{-1}. Si $K = (a,b,m) \in \mathcal{K}$, para todo $x \in \mathcal{P}_K$, $y \in \mathcal{C}_K$

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

Típicamente $m = 27$ está fijo, 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 puro $d_K(y)$ es el único que tiene sentido. La próxima cátedra determinaremos $|\mathcal{K}|$ para el cifrado afín en el caso que m este fijo. Este problema es interesante desde un punto de vista matemático. Más

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

aun, dado que un adversario que ve suficiente texto cifrado, encriptado utilizando el criptosistema afín, puede facilmente deducir el valor de m. En efecto, si el texto plano encriptado se distribuye uniformemente en $\mathcal{Z}_m$, se puede probar que si N es el mayor número de k textos cifrados, entonces $N+1 \leq m \leq N+c$ con probabilidad al menos $1-(c/m)^k$.