Fundamentos de criptografía

Josep Domingo Ferrer
Jordi Herrera Joancomartí

PID_00214915
Módulo 2

UOC
Universitat Oberta de Catalunya

Índice

Introducción

En este módulo presentamos las bases para entender las técnicas criptográficas modernas, y lo hacemos siguiendo el esquema siguiente:

1) Empezamos tratando detalladamente los **criptosistemas históricos**, es decir, los que se usaban antes de la aparición de los ordenadores. En muchos casos, estos criptosistemas han servido de base a los actuales.

2) A continuación veremos los **conceptos básicos de la teoría de la información**, sobre la cual se ha construido la criptografía moderna.

En términos de la teoría de la información formularemos las **definiciones de secreto perfecto y de autenticidad perfecta**. Veremos que en la práctica es difícil, si no imposible, conseguir el secreto y la autenticidad perfectos. Sin embargo, estos conceptos tienen que servir de guía en el diseño de los criptosistemas.

Para finalizar, introduciremos dos conceptos básicos en el criptoanálisis: la **suposición de Kerckhoffs** y la **distancia de unicidad**, y finalmente ilustraremos con un ejemplo cómo se puede criptoanalizar un criptosistema concreto.

Objetivos

En los materiales didácticos asociados a este módulo hallaréis las herramientas y los contenidos necesarios para alcanzar los objetivos siguientes:

1. Conocer las técnicas históricas de cifrado.

2. Adquirir un conocimiento operativo de los conceptos básicos de la teoría de la información.

3. Hacerse cargo de la relevancia de la teoría de la información para la criptografía y el criptoanálisis modernos.

4. Captar los principios elementales del criptoanálisis.

5. Darse cuenta de la debilidad de los criptosistemas históricos.

6. Entender las definiciones de *secreto* y de *autenticidad perfectos*.

1. Criptosistemas históricos

Occultas seu furtivas notas politioris literature viri eas literas appellant, quae artificio huiusmodi confictae sunt, ut non possint ab alio, quam ab eo, cui literi destinatur, interpretari.
G.B. Porta

Hay dos tipos de cifras elementales, las basadas en el principio de transposición y las basadas en el principio de sustitución. Pues bien, todas las cifras históricas (anteriores a la Segunda Guerra Mundial) se basan en uno de estos dos principios, o en una combinación de ambos.

Recordad que hemos visto las cifras de transposición y las de sustitución en el subapartado 1.1 del módulo "Introducción a la criptografía" de esta asignatura.

1.1. Criptosistemas de transposición

Las cifras o criptosistemas de transposición reordenan los caracteres de acuerdo con ciertas reglas.

Normalmente, la reordenación de los caracteres se hacía con la ayuda de alguna figura geométrica. Este cifrado se efectuaba en dos pasos:

1) El texto en claro se escribía en la figura siguiendo un determinado *camino de entrada*.

2) Siguiendo un determinado *camino de salida*, se extraía el texto cifrado de la figura.

Transposiciones espartanas

Los espartanos empleaban un bastón como figura para hacer una cifra de transposición. Se preparaban dos bastones gruesos, exactamente del mismo diámetro. El emisor se quedaba uno y el otro se entregaba al receptor como paso previo al envío de mensajes. Para cifrar un mensaje, el emisor enrollaba una cinta de pergamino en espiral en torno a su bastón. A continuación, escribía el mensaje en la cinta en líneas a lo largo del bastón, después retiraba la cinta y se la enviaba al receptor. Por el camino, la cinta de pergamino no era más que una sucesión de letras griegas colocadas en un orden ininteligible. Cuando el receptor enrollaba la cinta recibida en torno a su bastón, podía leer el mensaje original. Observad que el grosor del bastón actuaba como clave (con un bastón más delgado o más grueso no podía recuperarse el mensaje inicial).

Esparta...

... era una ciudad estado de la Grecia clásica que durante el siglo V a.C. tuvo una larga rivalidad con Atenas. Los espartanos eran fuertemente militaristas y utilizaban el cifrado para las comunicaciones militares.

Muchas cifras de transposición permutan los caracteres del texto en claro con un periodo fijado de d. Sean $\mathbb{Z}_d$ los enteros de 1 hasta d, y sea f: $\mathbb{Z}_d \to \mathbb{Z}_d$ una permutación sobre $\mathbb{Z}_d$. La clave para la cifra viene dada por la pareja $K = (d,f)$. Los bloques sucesivos de d caracteres se cifran permutando los caracteres según f. De esta manera, un mensaje en claro como el siguiente:

$$M = m_1 \dots m_d\, m_{d+1} \dots m_{2d} \dots$$

queda cifrado como:

$$E_K(M) = m_{f^{-1}(1)} \dots m_{f^{-1}(d)} m_{d+f^{-1}(1)} \dots m_{d+f^{-1}(d)} \dots$$

El descifrado utiliza la permutación inversa como f.

Transposición con periodo fijo

Consideramos $d = 3$ y tomemos la permutación f tal que $f(1) = 2$, $f(2) = 3$ y $f(3) = 1$. Entonces el mensaje:

$$M = \text{CRIPTOGRAFIA}$$

queda cifrado como:

$$E_K(M) = \text{ICROPTAGRAFI}$$

1.2. Criptosistemas de sustitución

Hay cuatro tipos de cifras de sustitución: simple, homofónica, polialfabética y poligráfica. A continuación explicamos cada uno de estas cifras.

1.2.1. Sustitución simple

Una **cifra o criptosistema de sustitución simple** cambia cada carácter de un alfabeto en claro ordenado, denotado por $\mathcal{A}$, por la letra correspondiente de un alfabeto cifrado, denotado por $\mathcal{C}$.

Más formalmente lo podemos expresar de la manera siguiente:

- $\mathcal{A} = \{a_0, a_1, ..., a_{n-1}\}$,
- $\mathcal{C} = \{f(a_0), f(a_1), ..., f(a_{n-1})\}$,

donde f: $\mathcal{A} \to \mathcal{C}$ es una aplicación biyectiva que hace corresponder a cada carácter de $\mathcal{A}$ un carácter de $\mathcal{C}$. La clave de la cifra está determinada por la función f, de manera que un mensaje en claro como éste:

$$M = m_1 m_2 \dots$$

queda cifrado como:

$$E_K(M) = f(m_1) f(m_2) \dots$$

La **cifra de César** es una cifra de sustitución simple, donde $\mathcal{A} = \mathcal{C}$ y la clave es $f(a) = (a + k) \bmod 26$, con k entre 0 y 25. De hecho, César utilizaba $k = 3$.

Recordad que vimos la cifra del César en el subapartado 1.1 del módulo "Introducción a la criptografía" de esta asignatura.

1.2.2. Sustitución homofónica

Las sustituciones simples tienen el inconveniente de que preservan las frecuencias del texto en claro en el texto cifrado, lo cual facilita mucho los ataques criptoanalíticos.

Frecuencias del texto

Imaginemos que queremos cifrar mensajes en castellano con una cifra de César con $k = 3$. Entonces la frecuencia de la letra D en el texto cifrado es la misma que la frecuencia de la letra A en el texto en claro. Como las frecuencias de las letras en castellano son conocidas, el criptoanalista puede deducir, viendo sólo el texto cifrado, que la D se descifra como A y que, por lo tanto, la clave es $k = 3$.

Una **cifra o criptosistema de sustitución homofónica** tiene como objetivo disimular las frecuencias de los caracteres del texto en claro. La idea es hacer corresponder a cada carácter a del alfabeto de texto en claro no uno, sino un conjunto $f(a)$ de símbolos de texto cifrado denominados *homófonos*.

Homófono

El término de raíz griega *homófono* quiere decir 'que tiene el mismo sonido'. En criptografía, los símbolos homófonos corresponden al mismo carácter en claro.

Por lo tanto, si utilizamos una cifra de sustitución homofónica la correspondencia entre el texto en claro y el texto cifrado tiene la forma $f: \mathcal{A} \to 2^{\mathcal{C}}$. De manera que un mensaje en claro como el siguiente:

$$M = m_1 m_2 \ldots$$

queda cifrado como sigue, donde cada c_i se escoge al azar dentro del conjunto de homófonos $f(m_i)$:

$$C = c_1 c_2 \ldots$$

Para ocultar las frecuencias del texto en claro y evitar ataques criptoanalíticos como el mencionado al hablar de la sustitución simple, una buena estrategia es que el conjunto de homófonos $f(a)$ tenga un cardinal proporcional a la frecuencia relativa del carácter en claro a. Así se consigue que las frecuencias de los símbolos en el texto cifrado sean prácticamente uniformes.

Homofonía italiana

El primer uso conocido de una cifra homofónica en Europa remonta en 1401, concretamente a la correspondencia entre el Ducado de Mantua y Simeone de Crema.

Durante más de un siglo, criptoanalistas aficionados trataron de descifrar un texto que, según se decía, indicaba la situación de un tesoro enterrado en el estado americano de Virginia por un grupo de aventureros bajo el mando de T.J. Beale. Ahora se sabe que el texto era cifrado con una cifra homofónica llamada **cifra de Beale** que tiene como clave la declaración de independencia de

los Estados Unidos de América. Beale numeró las palabras de dicha declaración y para cifrar una letra del texto en claro, la sustituía por el número de alguna palabra que empezara por la letra que había que cifrar.

Por ejemplo, la letra *W* se podía cifrar con los números 1, 19, 40, 66, 72, 290 y 459 (éstos son los homófonos de *W*). Como el número de palabras que empiezan por *W* en un texto inglés un poco largo es aproximadamente proporcional a la frecuencia relativa de *W* en inglés, la cifra de Beale consigue uniformizar las frecuencias de los símbolos del texto cifrado si el texto en claro está en inglés.

1.2.3. Sustitución polialfabética

Hemos visto que la sustitución homofónica intenta ocultar la distribución de frecuencias de los símbolos del texto en claro asignando diversos símbolos de texto cifrado a cada carácter del texto en claro.

Italia otra vez

Al igual que la sustitución homofónica, la sustitución polialfabética está documentada por primera vez en Italia. La primera cifra de este tipo fue publicada por L.B. Alberti en 1568.

La **sustitución polialfabética** persigue la misma finalidad que la homofónica, pero aplica diversos criterios de sustitución en vez de uno sólo.

La mayoría de criptosistemas polialfabéticos son cifras de sustitución periódica basadas en un periodo *d*. Sean $\mathcal{C}_1, ..., \mathcal{C}_d$ alfabetos de texto cifrado; sea $f_i: \mathcal{A} \rightarrow \mathcal{C}_i$ una aplicación del alfabeto de texto en claro $\mathcal{A}$ en el *i*-ésimo alfabeto de texto cifrado $\mathcal{C}_i$, para $1 \leq i \leq d$. Un mensaje en claro como el siguiente:

$$M = m_1 \dots m_d m_{d+1} \dots m_{2d} \dots$$

se cifra repitiendo la secuencia de aplicaciones $f_1, ..., f_d$ cada *d* caracteres, con lo cual se obtiene:

$$C = E_K(M) = f_1(m_1) \dots f_d(m_d) f_1(m_{d+1}) \dots f_d(m_{2d}) \dots$$

La llamada **cifra de Vigenère** es un criptosistema atribuido indebidamente al criptógrafo francés del siglo XVI Blaise de Vigenère. La clave está determinada por una secuencia de letras *K* o, mejor dicho, por los números de orden de estas letras:

$$K = k_1 \dots k_d,$$

donde k_i ($i = 1, ..., d$) indica la cantidad de desplazamiento en el *i*-ésimo alfabeto, es decir:

$$f_i(a) = (a + k_i) \bmod n.$$

Ejemplo de cifrado con el criptosistema de Vigenère

Tomamos $n = 26$ y $d = 4$. Sean los alfabetos $\mathcal{A}$, $\mathcal{C}_1$..., $\mathcal{C}_4$ iguales al alfabeto latino; si la clave es K = TREN = {19, 17, 4, 13}, el texto en claro ESTACIÓN queda cifrado como XJXNVZSA.

La denominada **cifra de Beaufort** se atribuye al almirante inglés Sir Francis Beaufort, pero fue propuesta primero por el italiano G. Sestri en 1710. La única diferencia respecto a la cifra de Vigenère es que las funciones de sustitución son:

$$f_i(a) = (a - k_i) \bmod n,$$

para $i = 1, \ldots, d$.

Las **máquinas de rotores** implementan cifras polialfabéticas con un periodo largo. Una máquina de rotores consiste en un banco de rotores o ruedas. El perímetro de cada rotor tiene 26 contactos eléctricos (uno para cada letra) tanto en la cara de delante como en la de detrás. Cada contacto de la cara de delante se encuentra conectado a un contacto de la cara de detrás para implementar una aplicación f_i de letras del texto en claro a letras del texto cifrado. Los rotores pueden rodar y colocarse en 26 posiciones diferentes, con el fin de alterar la aplicación. La cara del detrás del rotor i-ésimo se encuentra conectada a la cara del delante del rotor i+1-ésimo. Una letra en claro en forma de señal eléctrica entra en el primer rotor, atraviesa todos los rotores en secuencia y sale del último rotor.

Durante la Segunda Guerra Mundial...

... los alemanes utilizaron una máquina de rotores llamada Enigma e inventada por A. Scherbius.

El cableado entre rotores y las posiciones iniciales de los rotores determinan la clave inicial. Cada vez que se cifra una letra de texto en claro, unos o más rotores cambian de posición, con lo cual la clave cambia. Una máquina con t rotores no vuelve a la posición inicial hasta pasados $d = 26^t$ cifrados.

La **cifra de Vernam** puede ser vista como una cifra de sustitución polialfabética donde la clave es aleatoria y el periodo d es mayor que la longitud del texto en claro.

1.2.4. Sustitución poligráfica

Las tres sustituciones anteriores cifran una sola letra de texto en claro cada vez.

Las **cifras de sustitución poligráfica** cifran bloques grandes de letras, con lo cual dificultan ataques criptoanalíticos basados en las frecuencias individuales de las letras del texto en claro.

La clave de la **cifra de Hill** es una matriz K de d filas y d columnas. Para cifrar, se toman bloques sucesivos de d caracteres del texto en claro como si

fuesen vectores. Cada vector de texto en claro se multiplica por K para obtener un vector de texto cifrado (también con d caracteres). Los productos son módulo n, donde n es el cardinal del alfabeto de texto cifrado. El proceso de cifrado de un vector M se puede describir como:

$$C = E_K(M) = K \cdot M \bmod n.$$

2. Fundamentos de la teoría de la información

En 1949 C.E. Shannon proporcionó una base teórica a la criptografía basada en la teoría de la información que él mismo había elaborado el año anterior. Es importante conocer los fundamentos teóricos de la criptografía porque eso es lo que eleva esta disciplina a la condición de ciencia. Para entender la formulación de Shannon necesitamos unos conceptos básicos de la teoría de la información que daremos en este apartado.

Una **variable aleatoria** se puede definir informalmente como una variable que adopta un valor entre un conjunto de valores posibles, de manera que cada valor posible tiene una cierta probabilidad no nula de ser adoptado. Si el conjunto de valores que puede tomar la variable es discreto, entonces se dice que la variable aleatoria es discreta. Así, pues, tenemos que:

- Un mensaje *M* es visto por el criptoanalista como una variable aleatoria discreta que puede tomar como valores unos textos concretos.

- Una clave *K* también es vista por el criptoanalista como una variable aleatoria discreta. El criptoanalista querría saber qué valor toma la variable *K*, pero en principio sólo puede conocer (como mucho) la distribución de probabilidades de la clave, es decir, las probabilidades que tiene la clave de adoptar cada uno de los valores posibles. Si la clave es aleatoria en el sentido de la cifra de Vernam, la probabilidad de cada uno de los valores posibles es la misma.

Por ejemplo...

... imaginemos un mensaje "Comando Unix" enviado por *telnet*; en un 50% de los casos (probabilidad 0,5) se trata del mandato *ls*, en un 20% de los casos (probabilidad 0,2) se trata del mandato *vi*, etc.

Sea X una variable aleatoria discreta y x uno de los valores posibles de X. Denominamos **función de probabilidad de la variable X** a la función $p(x) = P(X = x)$.

Para cada valor de x, $p(x)$ indica la probabilidad de que la variable X tome el valor x. Si definimos $\sup(X) = \{x \mid P(X = x) \neq 0\}$ se cumple:

$$\sum_{x \in \sup(X)} p(x) = 1.$$

A partir de la función de probabilidad de una variable aleatoria X, la **entropía de Shannon** mide en bits la incertidumbre sobre X o, dicho de otro modo, la información que nos aporta el hecho de saber que X ha tomado tal o cual valor. Claramente, no obtenemos la misma información al saber el valor que ha tomado una variable que sólo tiene uno posible que al saber el que ha tomado otra variable que puede adoptar cincuenta valores diferentes con la misma probabilidad.

La **entropía de una variable aleatoria *X***, $H(X)$, es la esperanza matemática del logaritmo en base 2 de su función de probabilidad, con el signo cambiado:

$$H(X) = -\sum_x p(x) \log_2 p(x),$$

donde el sumatorio se extiende para $x \in \sup(X)$. Podemos expresar la misma relación de manera equivalente:

$$H(X) = \sum_x p(x) \log_2 \left(\frac{1}{p(x)}\right). \qquad (2.1)$$

Es importante recordar que la entropía se mide en bits.

Cálculo de la entropía del campo *Sexo*

El campo *Sexo* de una base de datos puede ser visto como una variable aleatoria que puede tomar dos valores: hombre y mujer. Si ambos valores se consideran equiprobables, el cálculo de la entropía es el siguiente:

$$H(sexo) = \frac{1}{2}(\log_2 2) + \frac{1}{2}(\log_2 2) = 1 \text{ bit.}$$

Así, pues, el campo *Sexo* contiene 1 bit de información bajo la hipótesis que los dos sexos tienen la misma probabilidad.

Intuitivamente, cada término $\log_2[1/p(x)]$ en la ecuación (2.1) representa el número de bits necesarios para codificar el valor x con una codificación óptima, es decir, una codificación que minimice el número esperado de bits para transmitir o almacenar. Visto de esta manera, $H(X)$ sería la longitud media ponderada de las codificaciones óptimas de los valores de X (la ponderación se hace según la probabilidad de cada valor). Los códigos de Huffman sirven para construir la codificación óptima mencionada y se usan en compresión de datos.

Lecturas recomendadas

Podéis ver con detalle los códigos de Huffman en el libro:

J. Rifó, L. Huguet (1991). *Comunicación digital*. Barcelona: Masson.

Cálculo de la información contenida en un mensaje

Supongamos un mensaje X que puede tomar n valores $x_1, \ldots, x_n$, todos con la misma probabilidad $p(x_i) = 1/n$, para $i = 1, \ldots, n$. Entonces:

$$H(X) = n\left(\frac{1}{n}\log_2 n\right) = \log_2 n \text{ bits.}$$

Así pues, saber qué valor ha tomado X aporta $\log_2 n$ bits de información. También podemos decir que la codificación óptima de cada uno de los n posibles valores requiere $\log_2 n$ bits.

Si en este ejemplo hacemos $n = 1$ y $p(x_1) = 1$, tenemos que $H(X) = \log_2 1 = 0$ bits. En una variable que no es tal, sino que toma un valor constante, no hay información.

En el ejemplo anterior hemos visto dos casos extremos. De hecho, la entropía máxima se da cuando hay incertidumbre máxima, es decir, cuando todos los n valores posibles de una variable son equiprobables y la entropía mínima se

da cuando sólo hay un valor posible y entonces vale 0. Formalmente, podemos recoger esta idea en la proposición que expresamos a continuación:

Proposición 1: si X tiene n posibles valores, entonces $0 \leq H(X) \leq \log_2 n$.

Además de la entropía, para el estudio teórico de la criptografía es relevante el concepto de *entropía condicionada*. Esta entropía mide la incertidumbre que nos queda sobre una variable X cuando conocemos el valor tomado por otra variable Y.

La **entropía de la variable X condicionada a la variable Y** se denota por $H(X|Y)$ y se calcula de la manera siguiente:

$$H(X|Y) = -\sum_x \sum_y p(x,y) \log_2 p(x|y) = \sum_y p(y) \sum_x p(x|y) \log_2 \left(\frac{1}{p(x|y)}\right), \qquad (2.2)$$

donde $p(x,y) = p(X = x, Y = y)$ es la función de probabilidad conjunta de X y de Y*, y $p(x|y) = p(X = x|Y = y) = p(X = x, Y = y)/p(Y = y)$ es la función de probabilidad de X condicionada a Y**.

* Probabilidad de que X valga x y al mismo tiempo Y valga y.
** Probabilidad de que X valga x si sabemos que Y vale y.

Cálculo de la entropía condicionada de un mensaje

Sea X un mensaje que puede tomar cuatro valores, todos con la misma probabilidad 1/4; por lo tanto, $H(X) = \log_2 4 = 2$ bits; y sea Y un mensaje que puede tomar cuatro valores, también todos con probabilidad 1/4. Supongamos que cada valor de Y restringe la elección de X a dos de los cuatro valores posibles, según las reglas siguientes:

- Si sale $Y = y_1$, entonces $X = x_1$ o $X = x_2$.
- Si sale $Y = y_2$, entonces $X = x_2$ o $X = x_3$.
- Si sale $Y = y_3$, entonces $X = x_3$ o $X = x_4$.
- Si sale $Y = y_4$, entonces $X = x_4$ o $X = x_1$.

De la primera regla resulta $p(x_1|y_1) = p(x_2|y_1) = 1/2$ y $p(x_3|y_1) = p(x_4|y_1) = 0$. Análogamente, las otras reglas dan lugar a dos probabilidades condicionadas iguales a 1/2 y dos nulas. Aplicando el último miembro de la ecuación (2.2) resulta:

$$H(X|Y) = 4 \cdot \left[\frac{1}{4} \cdot 2 \cdot \left(\frac{1}{2} \cdot \log_2 2\right)\right] = \log_2 2 = 1.$$

Vemos cómo el conocimiento de Y reduce la incertidumbre sobre X a un solo bit, mientras que inicialmente eran dos.

Puede pasar que X e Y sean variables que no tienen nada que ver entre sí*. En este caso, se dice que X e Y son independientes y entonces se verifica lo siguiente:

* Por ejemplo, la latitud y la longitud de un punto del planeta escogido al azar.

- $H(X|Y) = H(X)$.
- $H(Y|X) = H(Y)$.

Conocer el valor que toma una variable no reduce la incertidumbre sobre la otra. La proposición siguiente explica la relación general entre $H(X|Y)$ y $H(X)$.

Proposición 2: el conocimiento de una variable Y sólo puede reducir la incertidumbre sobre otra variable X, es decir:

$$0 \leq H(X|Y) \leq H(X). \tag{2.3}$$

En caso de que Y determine X, la incertidumbre sobre X baja a cero (igualdad izquierda). En el caso que X e Y sean independientes, no se reduce nada la incertidumbre sobre X, que continúa siendo $H(X)$ (igualdad derecha).

La **entropía conjunta de dos variables *X* e *Y***, $H(X,Y)$, es la incertidumbre sobre la combinación de valores que tomarán ambas variables, es decir, el valor que tomará el vector de variables (X,Y):

$$H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y). \tag{2.4}$$

Intuitivamente, la incertidumbre sobre el comportamiento conjunto de X y de Y se descompone en la incertidumbre en cuanto al valor que tomará X más la incertidumbre sobre el que tomará Y sabiendo qué valor ha tomado X (se podría decir lo mismo si intercambiáramos X e Y).

Proposición 3: si X, Y y Z son variables aleatorias, se cumplen unas cuantas igualdades que no nos tendrían que sorprender si tenemos en cuenta que la entropía de Shannon es básicamente el logaritmo de una probabilidad:

- $H(X,Y,Z) = H(X) + H(Y|X) + H(Z|X,Y)$.
- $H(X,Y|Z) = H(X|Z) + H(Y|X,Z) = H(Y|Z) + H(X|Y,Z)$.
- $0 \leq H(X|Y,Z) \leq H(X|Y)$.
- $H(X) \leq H(X,Y)$.
- $H(X|Z) \leq H(X,Y|Z)$.

Un concepto importante para la definición de secreto perfecto es el de información mutua. La **información mutua entre dos variables aleatorias *X* e *Y***, $I(X,Y)$, se define de la manera siguiente:

$$I(X,Y) = H(X) - H(X|Y) = H(Y) - H(Y|X).$$

Teniendo en cuenta la proposición 2, queda claro que $I(X,Y)$ siempre es positiva o nula. Intuitivamente, la información mutua entre X e Y es la reducción en la incertidumbre que tenemos sobre X cuando sabemos el valor que ha tomado Y (se podría decir lo mismo si intercambiáramos X e Y).

3. Secreto perfecto y autenticidad perfecta

El *secreto* y la *autenticidad* son conceptos diferentes, y por ello los trataremos de manera independiente.

3.1. Secreto perfecto

Shannon midió el **secreto teórico de una cifra** como la incertidumbre sobre el texto en claro una vez se ha interceptado el texto cifrado correspondiente. Si, con independencia de la cantidad de texto cifrado interceptado, no se puede saber nada del texto en claro, entonces la cifra ofrece un secreto perfecto. La definición siguiente formaliza este concepto en términos de entropía.

Si M es un texto en claro y C es el texto cifrado correspondiente obtenido con un determinado criptosistema, decimos que el criptosistema proporciona un secreto perfecto si $H(M|C) = H(M)$; o equivalentemente: $I(M,C) = 0$. Intuitivamente, la incertidumbre sobre el valor del texto en claro M cuando el criptoanalista ve el texto cifrado C es la misma que tendría si no lo hubiera visto.

El problema del secreto perfecto, como en la mayoría de cosas perfectas, es que es difícil de conseguir. En su artículo de 1949, Shannon utilizó las propiedades de la entropía para demostrar que si M, C y K son el texto en claro, el texto cifrado y la clave, respectivamente, entonces tenemos:

$$H(M|C) \leq H(M,K|C) = H(K|C) + H(M|C,K) = H(K|C) \leq H(K) \qquad (3.1)$$

En esta desigualdad se ha utilizado que $H(M|C,K) = 0$, es decir, que no hay incertidumbre sobre el texto en claro una vez conocidos el texto cifrado correspondiendo y la clave utilizada.

Combinando la definición de secreto perfecto y la desigualdad (3.1) obtenemos como resultado el **teorema de la cota fundamental de Shannon para el secreto perfecto**, que establece lo siguiente: en un criptosistema perfectamente secreto, la incertidumbre de la clave secreta K tiene que ser al menos tan grande como la incertidumbre del texto en claro que pretende ocultar. Formalmente podemos expresar la cota de Shannon de la manera siguiente:

$$H(M) \leq H(K). \qquad (3.2)$$

Esta cota fundamental tiene consecuencias "trágicas" con respecto a la longitud de clave necesaria para mantener el secreto perfecto. En efecto, hemos visto que un mensaje X con incertidumbre $H(X)$ requiere como mínimo $H(X)$ bits por término medio para codificar los valores posibles.

En resumen, la cota de Shannon nos dice que en un criptosistema perfectamente secreto, la clave K requiere tantos o más bits que el texto en claro M, es decir, la clave secreta tiene que ser más larga que el texto que se pretende cifrar.

La **cifra de Vernam** es la única conocida que ofrece un secreto perfecto. Recordamos que:

- La cifra de Vernam consiste en sumar una clave K al texto en claro M para obtener el texto cifrado C.
- M, C y K adoptan valores en {0, 1} y la suma es módulo 2, es decir, $C = M \oplus K$.
- La clave es aleatoria y sólo se utiliza una vez, es decir, cada bit de texto en claro se cifra con un nuevo bit de clave elegido al azar.

La última condición implica que la clave K es al menos tan larga como el texto en claro, es decir, $|K| \geq |M|$. Como K es aleatoria (cada bit vale 0 ó 1 con probabilidad 1/2), resulta que $H(K) = |K|$. Por otra parte, $H(M) \leq |M|$ (la igualdad sólo se produce si M es un mensaje aleatorio). Por lo tanto:

$$H(M) \leq |M| \leq |K| = H(K),$$

y se cumple la condición de secreto perfecto.

El criptosistema de Vernam puede parecer inútil a primera vista: se puede pensar que, puestos a hacer llegar al receptor de manera segura una clave secreta de un sólo uso más larga que el mensaje en claro, daría igual enviar directamente el mensaje en claro por el mismo canal seguro por donde se quiere enviar la clave. No obstante, hay que tener en cuenta que si la clave es enviada al receptor en circunstancias más favorables que las que tendremos a la hora de enviar el mensaje cifrado, tiene sentido pasar una clave secreta más larga que el mismo mensaje en claro; por ejemplo, una buena estrategia es pasar grandes longitudes de clave antes de un conflicto armado para poder enviar mensajes cifrados durante el conflicto.

One-time pad

En inglés, la cifra de Vernam se conoce también como *one-time pad*, porque se utilizó poco antes, durante y después de la Segunda Guerra Mundial por parte de espías de diferentes países que recibían una hoja de papel (*pad*) con la clave secreta aleatoria y las instrucciones de utilizarla sólo para un sólo cifrado (*one-time*).

3.2. Autenticidad perfecta

La criptografía pretende asegurar el secreto y la autenticidad de los mensajes. Sin embargo, sólo recientemente la gente se ha dado cuenta de que *secreto* y

autenticidad son atributos independientes. Si Ana comparte una clave con Bernardo y Ana recibe un criptograma que se descifra bien con la clave compartida, ¿puede estar segura de que el criptograma fue enviado por Bernardo? La respuesta es no. G.J. Simmons publicó en 1984 el artículo "Authentication theory/coding theory", que presenta una teoría de la autenticidad análoga en muchos aspectos a la teoría del secreto publicada por Shannon en 1949.

Como Shannon, Simmons supone que la clave de cifrado se utiliza una sola vez. En en escenario supuesto por Simmons, el criptoanalista enemigo se halla entre el emisor y el receptor y genera un criptograma fraudulento $\tilde{C}$ como bueno. Hay dos tipos de ataque:

1) Suplantación: el criptoanalista genera un criptograma fraudulento $\tilde{C}$. El ataque tiene éxito si el receptor acepta $\tilde{C}$ como bueno. Llamamos P_{sup} a la probabilidad de éxito de un ataque de suplantación.

2) Sustitución: el criptoanalista cambia un criptograma auténtico C enviado por el emisor por un criptograma fraudulento $\tilde{C}$. Este tipo de ataque tiene éxito si el receptor acepta $\tilde{C}$ como bueno y $\tilde{C} \neq C$. Denominamos P_{sub} a la probabilidad de éxito de un ataque de sustitución.

Suponiendo que el criptoanalista enemigo escogerá el tipo de ataque que le resulte más favorable, se define la **probabilidad de engaño**, P_e, como:

$$P_e = \max(P_{sub}, P_{sup}).$$

Llamamos $\#C$ al número de criptogramas c que tienen una probabilidad no nula de aparecer, es decir, tales que $P(C = c) \neq 0$ de manera análoga, llamamos $\#M$ y $\#K$ al número de mensajes en claro y de claves, respectivamente, con una probabilidad no nula de aparecer. Entonces para cada clave k tiene que haber $\#M$ criptogramas con probabilidad no nula: son los criptogramas resultantes de cifrar con k los $\#M$ mensajes en claro que tienen una probabilidad no nula.

Por lo tanto, si el criptoanalista enemigo inicia un ataque de suplantación y elige al azar uno de los $\#C$ criptogramas que tienen una probabilidad no nula, su probabilidad de éxito será:

$$P_{sup} \geq \frac{\#M}{\#\mathrm{C}}. \qquad (3.3)$$

Como $P_e \geq P_{sup}$, la desigualdad (3.3) muestra que no es posible conseguir una protección total contra el engaño. Una buena manera de luchar contra el engaño es que el conjunto de criptogramas posibles sea mucho mayor que el conjunto de textos en claro posibles, es decir, tomar $\#C \gg \#M$.

Por ser la protección total imposible, Simmons definió la **autenticidad perfecta** como la máxima protección posible contra el engaño. Hay que admitir que esta definición presenta algunos "casos patológicos", ya que cuando $\#M = \#C$ tendremos que considerar perfectamente auténtico un sistema con $P_e = 1$, porque la desigualdad (3.3) indica que, a la fuerza, $P_{sup} = 1$.

La autenticidad perfecta se define en términos de información mutua. Para ello, necesitamos conocer el **teorema de la cota de Simmons**, que establece que, si P_{sup} es la probabilidad de suplantación con éxito, se cumple:

$$P_{sup} \geq 2^{-I(C,K)}. \tag{3.4}$$

Lectura complementaria

Podéis encontrar la demostración del teorema de la cota de Simmons en el artículo de J. Massey "An Introduction to Contemporary Cryptology" en la obra siguiente:

G.J. Simmons (1992). *Contemporary Cryptology: The Science of Information Integrity*. Nueva York: IEEE Press.

Paradójicamente, para reducir la cota (3.4) hace falta que $I(C,K)$ sea grande, es decir, de que un criptograma dé mucha información sobre la clave utilizada. Eso tiene sentido, porque el hecho de que $I(C,K)$ sea grande quiere decir que el criptograma C difícilmente puede ser producido por alguien que no sepa la clave K; en otras palabras, por alguien diferente del emisor legítimo. Claramente, secreto y autenticidad son, como mínimo, independientes.

De hecho, reducir la cota (3.3) haciendo crecer $\#C$ en relación con $\#M$ implica también reducir la cota (3.4). En efecto, si $\#M \lll \#C$, quiere decir que ver a uno de los $\#M$ criptogramas válido da bastante información sobre la clave utilizada para producirlo; por lo tanto, $I(C,K)$ es grande y la cota (3.4) es pequeño. Para entender este razonamiento, pensemos en el caso opuesto: si $\#M = \#C$, entonces un criptograma puede aparecer con cualquier clave (sea cual sea la clave escogida, tiene que haber $\#M = \#C$ criptogramas válidos); por lo tanto, ver un criptograma no dice nada sobre la clave utilizada, con lo cual $I(C,K) = 0$ y la cota (3.4) es máxima ($P_e = P_{sup} = 1$).

Un criptosistema tiene la propiedad de autenticidad perfecta si P_e toma el mínimo valor posible, es decir, si $P_e = 2^{-I(C,K)}$.

3.3. Ejemplos de independencia entre el secreto y la autenticidad

En este subapartado recogemos cinco ejemplos propuestos por J. Massey para ilustrar la afirmación de que secreto y autenticidad son dos propiedades independientes de un criptosistema. En los criptosistemas de los ejemplos, el texto en claro es siempre un solo dígito binario M, el criptograma consiste en dos dígitos binarios $C = [C_1, C_2]$ y la clave K es aleatoria y consiste en uno o dos bits. Al ser aleatoria la clave, su entropía $H(K)$ es igual a su longitud.

3.3.1. Criptosistema no secreto ni auténtico

Consideremos $M = \{0, 1\}$, K = {0, 1} y $C = \{00, 01, 10, 11\}$. La transformación de cifrado se indica en la tabla siguiente:

K	$M = 0$	$M = 1$
0	$C = 00$	$C = 10$
1	$C = 01$	$C = 11$

En este caso, claramente no hay secreto, dado que el primer bit del texto cifrado es igual al texto en claro.

Analicemos su autenticidad:

1) La probabilidad de suplantación con éxito es $P_{sup} = 1/2$, porque sólo dos de los cuatro criptogramas serán aceptados por el receptor (que sabe la clave) y porque no hay ningún criptograma que valga con las dos claves.

2) Si el criptoanalista enemigo ve un criptograma, sabe que puede invertir el primer bit y que el criptograma alterado será aceptado sea cual sea la clave. En efecto, si $K = 0$, valen $C = 00$ y $C = 10$; si $K = 1$, valen $C = 01$ y $C = 11$. Por lo tanto, la probabilidad de tener éxito en una sustitución es $P_{sub} = 1$, con lo cual $P_e = 1$.

3) Calculemos la cota de Simmons. Tenemos $H(K) = 1$ bit y, por otra parte, $H(K|C) = 0$, dado que la clave queda determinada por el segundo bit del criptograma. Por lo tanto, $I(C,K) = H(K) - H(K|C) = 1$. La cota es $2^{-I(C,K)} = 2^{-1} < P_e$. Así, pues, el criptosistema no proporciona una autenticidad perfecta.

En este caso, el ataque de sustitución es más peligroso que el ataque de suplantación.

3.3.2. Criptosistema no secreto y trivialmente auténtico

Consideremos $M = \{0, 1\}$, $K = \{0, 1\}$ y $C = \{00, 01, 10, 11\}$. Introduzcamos un parámetro R aleatorio para aleatorizar el cifrado. La transformación de cifrado viene determinada por la tabla siguiente:

K	R	$M = 0$	$M = 1$
0	0	$C = 00$	$C = 10$
0	1	$C = 01$	$C = 11$
1	0	$C = 00$	$C = 11$
1	1	$C = 01$	$C = 10$

En este caso tampoco hay secreto, dado que el primer bit del texto cifrado es igual al texto en claro.

Analicemos su autenticidad:

1) La probabilidad de suplantación con éxito es $P_{sup} = 1$, porque los cuatro criptogramas son válidos sea cual sea el valor de la clave (el receptor los aceptará como buenos).

2) Si el criptoanalista enemigo ve un criptograma, se encuentra ante dos alternativas equiprobables a la hora de intentar sustituirlo. Por ejemplo, no sabe si cambiar $C = 00$ por $C = 10$ o bien por $C = 11$ (tendría que saber la clave secreta para decidirlo con seguridad). Por lo tanto, la probabilidad de sustitución con éxito es $P_{sub} = 1/2$ y entonces $P_e = \max(P_{sup},P_{sub}) = 1$.

3) Calculemos la cota de Simmons. Tenemos $H(K) = 1$ bit y, por otra parte, $H(K|C) = 1$, dado que para cualquier texto cifrado los dos valores de la clave son equiprobables. Por lo tanto, $I(C,K) = H(K) - H(K|C) = 0$. La cota es $2^{-I(C,K)} = 1 = P_e$. Así, pues, el criptosistema proporciona una autenticidad perfecta de manera trivial; pero la autenticidad perfecta no tiene ninguna gracia si la probabilidad de engaño es 1.

De hecho, este ejemplo y el anterior muestran que el ataque de sustitución puede ser más peligroso que el de suplantación o al revés, en función de cada caso particular.

3.3.3. Criptosistema no secreto y perfectamente auténtico

Consideremos el mismo esquema presentado en el subapartado anterior, pero ahora K y R son los dos bits de la clave (K_1 y K_2) y, por lo tanto, los dos serán conocidos por el receptor legítimo. La nueva tabla de cifrado es la siguiente:

K_1	K_2	$M = 0$	$M = 1$
0	0	$C = 00$	$C = 10$
0	1	$C = 01$	$C = 11$
1	0	$C = 00$	$C = 11$
1	1	$C = 01$	$C = 10$

En este caso sigue sin haber secreto, dado que el primer bit del texto cifrado es igual al texto en claro.

Analicemos su autenticidad:

1) Para cada uno de los cuatro valores de la clave sólo hay dos criptogramas válidos y cada criptograma sólo es válido con dos de los cuatro valores de la

clave. Por lo tanto, la probabilidad de que un criptograma escogido al azar sea válido es 1/2 y entonces $P_{sup} = 1/2$.

2) Si el criptoanalista enemigo ve un criptograma, se halla ante dos alternativas equiprobables a la hora de intentar sustituirlo. Por ejemplo, no sabe si cambiar $C = 00$ por $C = 10$ o bien por $C = 11$; tendría que saber la clave secreta para decidirlo con seguridad. Por lo tanto, la probabilidad de sustitución con éxito es $P_{sub} = 1/2$ y entonces $P_e = \max(P_{sup},P_{sub}) = 1/2$.

3) Calculamos la cota de Simmons. Tenemos $H(K) = 2$ bits y, por otra parte, $H(K|C) = 1$ bit, dado que al ver un texto cifrado el criptoanalista duda sólo entre dos de las cuatro claves (por ejemplo, $C = 00$ sólo puede aparecer con las claves $K = 00$ y $K = 10$). Por lo tanto, $I(C,K) = H(K) - H(K|C) = 1$. La cota es $2^{-I(C,K)} = 1/2 = P_e$. Así, pues, el criptosistema proporciona una autenticidad perfecta conseguida de una manera no trivial.

3.3.4. Criptosistema perfectamente secreto y no auténtico

Consideremos el esquema de cifrado siguiente:

K_1	K_2	$M = 0$	$M = 1$
0	0	$C = 00$	$C = 11$
0	1	$C = 01$	$C = 10$
1	0	$C = 10$	$C = 01$
1	1	$C = 11$	$C = 00$

Si analizamos su secreto podemos ver que cada mensaje en claro posible puede ser cifrado con la misma probabilidad como uno de los cuatro criptogramas posibles (según la clave); es decir, $P(C = c|M = m) = 1/4$ para cualquier par (m, c). Otra manera de decirlo es que al ver un criptograma, no tenemos ninguna pista sobre cuál es el mensaje en claro. Por lo tanto, hay un secreto perfecto.

Analicemos su autenticidad:

1) Para cada uno de los cuatro valores de la clave sólo hay dos criptogramas válidos y cada criptograma sólo es válido con dos de los cuatro valores de la clave. Por lo tanto, la probabilidad de que un criptograma escogido al azar sea válido es 1/2 y entonces $P_{sup} = 1/2$.

2) Si el criptoanalista enemigo ve un criptograma, sabe que puede invertir los dos bits y que el receptor aceptará como válido el criptograma resultante. Por lo tanto, $P_{sub} = 1$ y entonces $P_e = \max(P_{sup},P_{sub}) = 1$.

3) Calculamos la cota de Simmons. Tenemos $H(K) = 2$ bits y, por otra parte, $H(K|C) = 1$ bit, dado que, al ver un texto cifrado, el criptoanalista duda sólo entre dos de las cuatro claves (por ejemplo, $C = 00$ sólo puede aparecer con las claves $K = 00$ y $K = 11$). Por lo tanto, $I(C,K) = H(K) - H(K|C) = 1$. La cota es $2^{-I(C,K)} = 1/2 < P_e$. Así, pues, no hay una autenticidad perfecta.

3.3.5. Criptosistema perfectamente secreto y perfectamente auténtico

Consideremos el esquema de cifrado siguiente:

K_1	K_2	$M = 0$	$M = 1$
0	0	$C = 00$	$C = 10$
0	1	$C = 01$	$C = 00$
1	0	$C = 11$	$C = 01$
1	1	$C = 10$	$C = 11$

Analicemos su secreto. Cada posible mensaje en claro puede ser cifrado con la misma probabilidad como uno de los cuatro criptogramas posibles (según la clave); es decir, $P(C = c|M = m) = 1/4$ para cualquier par (m, c). Otra manera de decirlo es que al ver un criptograma, no tenemos ninguna pista sobre cuál es el mensaje en claro. Por lo tanto, hay un secreto perfecto.

Analicemos su autenticidad:

1) Para cada uno de los cuatro valores de la clave sólo hay dos criptogramas válidos y cada criptograma sólo es válido con dos de los cuatro valores de la clave. Por lo tanto, la probabilidad de que un criptograma escogido al azar sea válido es 1/2 y entonces $P_{sup} = 1/2$.

2) Si el criptoanalista enemigo ve un criptograma, se encuentra ante dos alternativas equiprobables a la hora de intentar sustituirlo. Por ejemplo, no sabe si cambiar $C = 00$ por $C = 10$ o bien por $C = 01$; tendría que saber la clave secreta para decidirlo con seguridad. Por lo tanto, la probabilidad de sustitución con éxito es $P_{sub} = 1/2$ y entonces $P_e = \max(P_{sup},P_{sub}) = 1/2$.

3) Calculemos la cota de Simmons. Tenemos $H(K) = 2$ bits y, por otra parte, $H(K|C) = 1$ bit, dado que al ver un texto cifrado, el criptoanalista duda sólo entre dos de las cuatro claves (por ejemplo, $C = 00$ sólo puede aparecer con las claves $K = 00$ y $K = 01$). Por lo tanto, $I(C,K) = H(K) - H(K|C) = 1$. La cota es $2^{-I(C,K)} = 1/2 = P_e$. Así, pues, hay una autenticidad perfecta conseguida de una manera no trivial.

4. Criptoanálisis elemental

En este apartado revisaremos dos conceptos básicos en el criptoanálisis: la suposición de Kerckhoffs y la distancia de unicidad. Por otro lado, veremos un ejemplo práctico de criptoanálisis rompiendo un cifrado de Vigenière con el criptoanálisis de frecuencias.

4.1. Suposición de Kerckhoffs

Una suposición casi universal en criptografía es que el criptoanalista enemigo tiene acceso al criptograma. Casi tan universal es la suposición de Kerckhoffs, formulada por el holandés A. Kerckhoffs (1835-1903), según la cual la seguridad de la cifra tiene que residir totalmente en la clave secreta.

La **suposición de Kerckhoffs** establece que el criptoanalista enemigo conoce todo el mecanismo de cifrado excepto el valor de la clave secreta.

No deja de sorprender que la suposición de Kerckhoffs sea a menudo ignorada en criptografía militar e incluso en aplicaciones civiles como la telefonía móvil. Los diseñadores de criptosistemas caen fácilmente en la tentación de pensar que si el mecanismo de cifrado se mantiene secreto, la seguridad de la cifra es más alta. Eso no es necesariamente cierto por las razones siguientes:

1) Un mecanismo de cifrado público puede ser sometido al examen de toda la comunidad científica. De este modo se puede comprobar su fortaleza o debilidad. Un mecanismo de cifrado secreto sólo ha pasado el examen de un grupo reducido de criptógrafos que, por su propia contribución al diseño, corren el riesgo de pasar por alto eventuales deficiencias de seguridad.

Secreto de dos

La sabiduría popular dice: "Secreto de uno, secreto seguro; secreto de dos, encomiéndate a Dios; secreto de tres, ya no lo es". Eso puede explicar la dificultad de mantener en secreto un mecanismo de cifrado diseñado por un grupo de criptógrafos.

2) A la larga, es muy difícil mantener en secreto un mecanismo de cifrado, incluso si los diseñadores firman un contrato de no revelación. Como ejemplo, actualmente se conocen casi del todo los mecanismos de seguridad usados en telefonía móvil GSM, que en teoría tendrían que ser secretos. Es más realista suponer, como hace Kerckhoffs, que lo único secreto es la clave.

4.2. Redundancia y distancia de unicidad

De la suposición de Kerckhoffs y de la desigualdad (3.1) se deduce que puede utilizarse $H(K|C)$ para medir el secreto de una cifra. La magnitud $H(K|C)$ se llama **ambigüedad de clave** y representa la incertidumbre que queda sobre la clave una vez se conoce un criptograma. Si $H(K|C) = 0$, no hay incertidumbre

y la cifra se puede romper, en teoría, si se dispone de recursos de cálculo suficientes. Normalmente, $H(K|C)$ decrece a medida que aumenta la longitud N del criptograma conocido C.

La **distancia de unicidad de una cifra** es la menor longitud N de criptograma que aproxima más $H(K|C)$ a cero. Dicho de otro modo, es la cantidad de texto cifrado que hace falta para que la clave quede determinada de manera única.

Shannon denominó *criptosistemas idealmente secretos* a aquéllos que, a pesar de no proporcionar un secreto perfecto, son irrompibles porque no dan suficiente información para determinar la clave.

La mayoría de criptosistemas son demasiados complejos para hallar su distancia de unicidad. Shannon formuló un modelo llamado *modelo de cifra aleatoria* que permite hallar en algunos casos una distancia de unicidad aproximada. Veamos cómo funciona dicho modelo. Antes, necesitemos algunas definiciones.

Para un lenguaje determinado, consideramos el conjunto de todos los mensajes de N caracteres de longitud. La **tasa del lenguaje para mensajes X de longitud N**, r, se define como:

Según diversos estudios, la tasa del inglés para valores grandes de N está entre 1,0 y 1,5 bits/letra.

$$r = H(X)/N,$$

es decir, el número medio de bits de información por carácter.

La **tasa absoluta de un lenguaje**, R, se define como el número máximo de bits de información que pueden ser codificados en cada carácter suponiendo que todas las secuencias de caracteres son equiprobables. Si hay L caracteres en el alfabeto, la tasa absoluta es:

La tasa absoluta del inglés (y del español) es de $R = \log_2 26 = 4{,}7$ bits/letra.

$$R = \log_2 L$$

La **redundancia de un lenguaje** con tasa r y tasa absoluta R se define como $D = R - r$.

Para el inglés...

... $D = 4{,}7 - 1{,}5 = 3{,}2$ bits/letra. Del cociente D/R se ve que el inglés es aproximadamente redundante en un 79%. Ello quiere decir que si ciframos un texto en claro en inglés, la distancia de unicidad no puede ser muy grande.

Supongamos que cada texto en claro y cada mensaje cifrado vienen de un alfabeto finito de L símbolos. Entonces hay 2^{RN} posibles mensajes de longitud N, donde $R = \log_2 L$, que se pueden dividir en un conjunto de 2^{rN} **mensajes con sentido** y un conjunto de $2^{RN} - 2^{rN}$ **mensajes sin sentido**, donde r es la tasa del lenguaje.

Se supone que todos los mensajes con sentido tienen la misma probabilidad de aparición $1/2^{rN} = 2^{-rN}$, mientras que los mensajes sin sentido tienen probabilidad cero. Supondremos también que hay $2^{H(K)}$ claves, todas equiprobables, donde $H(K)$ es la entropía de la clave (número de bits de la clave). La probabilidad de todas las claves k es:

$$P(K = k) = 1/2^{H(K)} = 2^{-H(K)}.$$

Una **cifra aleatoria** es aquélla en la cual el criptoanalista ve el descifrado $D_{k(c)}$, para cada clave k y para cada texto cifrado c, como una variable aleatoria independiente (de otros $D_{k'(c')}$) y distribuida uniformemente sobre todos los 2^{RN} mensajes, con o sin sentido.

Consideramos el texto cifrado $c = E_{k(m)}$ para k y m dados. Es un **descifrado espurio** cuando el cifrado bajo otra clave k' puede dar c; es decir, $c = E'_k(m)$ para el mismo mensaje m, o bien $c = E'_k(m')$ para otro mensaje con sentido m'. Un criptoanalista que intercepte c no podrá decidir si la clave correcta es k o bien k'.

Ahora bien, por cada descifrado correcto de un determinado texto cifrado hay $2^{H(K)} - 1$ claves restantes, cada una con la misma probabilidad q de generar un descifrado espurio, que es el número de mensajes con sentido dividido por el número de mensajes posibles:

$$q = 2^{rN}/2^{RN} = 2^{(r-R)N} = 2^{-DN}.$$

Si con F denotamos el número esperado de descifrados espurios obtenidos a partir de una de las claves, tenemos:

$$F = (2^{H(K)} - 1) \cdot q = (2^{H(K)} - 1) \cdot 2^{-DN} \approx 2^{H(K)-DN}.$$

A causa del decrecimiento rápido que F experimenta cuando N crece, se toma $\log_2 F = H(K) - DN = 0$ como el punto donde el número de soluciones falsas es lo suficientemente pequeño para que la cifra se pueda romper. Por lo tanto, la distancia de unicidad, N, es decir, la cantidad de texto necesaria para romper la cifra es la siguiente:

$$N = \frac{H(K)}{D}.$$

Si el criptoanalista dispone de N caracteres y de una capacidad de cálculo ilimitada, entonces podrá hallar la única clave que puede generar los N caracteres cifrados. Observad que si el texto en claro no tuviera redundancia (es decir, si consistiera en una secuencia aleatoria de bits), la distancia de unicidad sería infinita.

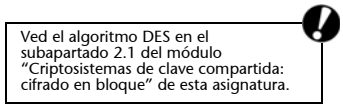
En la **cifra de Vernam**, el número de claves posibles para cada N es tan grande como el número de mensajes posibles. Luego $H(K) = \log_2 (2^{RN}) = RN$ y tenemos:

$$H(K) - DN = (R - D) \cdot N = rN \neq 0,$$

lo cual implica que la cifra de Vernam es irrompible en teoría, como ya habíamos mencionado.

Seguridad del algoritmo DES

El algoritmo DES cifra bloques de 64 bits (8 caracteres) y utiliza claves de 56 bits. Este algoritmo encaja razonablemente con el modelo de cifra aleatoria. Si se utiliza para cifrar un texto en claro en inglés, entonces $H(K) = 56$ y $D = 3{,}2$, con la cual la distancia de unicidad en caracteres es:



Ved el algoritmo DES en el subapartado 2.1 del módulo "Criptosistemas de clave compartida: cifrado en bloque" de esta asignatura.

$$N = \frac{56}{3{,}2} = 17{,}5\ .$$

Por lo tanto, en teoría basta con algo más de dos bloques de texto cifrado para que la clave DES utilizada quede determinada únicamente. Ahora bien, que quede determinada únicamente no quiere en absoluto decir que al criptoanalista le sea fácil encontrarla. A modo de analogía, podemos saber que un atraco ha sido cometido por una sola persona, pero entre llegar a esa conclusión e identificar a dicha persona hay mucho trabajo.

4.3. Criptoanálisis de Kasiski para el cifrado de Vigenère

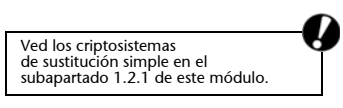
El año 1863, el oficial prusiano W. F. Kasiski consiguió romper el criptosistema de Vigenère a partir del análisis de las repeticiones de grupos de símbolos en el texto cifrado y el análisis de frecuencias.

En la realización de un criptoanálisis de Kasiski se establecen dos etapas. En la primera se determina la longitud de la clave, y en la segunda se calcula su valor exacto.

La longitud de la clave de cifrado del criptograma se calcula a partir del análisis de las repeticiones de grupos de caracteres. Para entender bien el proceso, vamos a empezar al revés. Supongamos que la longitud de la clave que queremos hallar es 5. Si el criptograma está formado por una secuencia de m caracteres $C_1, C_2,..., C_{m-1}, C_m$ y lo escribimos en 5 columnas tenemos:

$$\begin{array}{lllll} C_1 & C_2 & C_3 & C_4 & C_5 \\ C_6 & C_7 & C_8 & C_9 & C_{10} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ C_{m-4} & C_{m-3} & C_{m-2} & C_{m-1} & C_m \end{array}$$

El método de cifrado de Vigenère con una clave de 5 caracteres cifra cada columna con el mismo elemento de la clave. Es decir, los caracteres de cada columna corresponden a un criptosistema de sustitución simple utilizando el carácter i-ésimo de la clave. Por lo tanto, dos o más caracteres iguales de una



Ved los criptosistemas de sustitución simple en el subapartado 1.2.1 de este módulo.

columna provendrán de caracteres iguales de texto en claro. Como todos los idiomas presentan una alta redundancia, posiblemente habrá conjuntos de caracteres característicos (por ejemplo, en inglés los conjuntos: *the*, *ing*, *ght*; en castellano: *ando*, *ado*, *ción*), que quedarán cifrados con la misma porción de la clave y darán lugar a cadenas de texto cifrado repetidas en el criptograma.

La probabilidad de que estas repeticiones de cadenas se den de forma aleatoria es más baja cuanto más larga sea la longitud de la cadena que se repite. De hecho, conjuntos de tres o cuatro caracteres repetidos más de una vez indican una alta probabilidad de que la distancia entre las cadenas sea un múltiplo de la clave utilizada para cifrar. Por ejemplo, si ciframos el mensaje:

$$M = \text{TOBEORNOTTOBETHATISTHE...}$$

Con la clave $K = \text{HAM}$ obtenemos el criptograma resultante siguiente:

$$C = \textbf{AONL}\text{ODUOFA}\textbf{AONL}\text{TTHTTZTTL...}$$

Observamos que la distancia entre las dos secuencias de caracteres AONL es igual a 9, y puesto que 9 es un múltiplo de la longitud de la clave, la longitud de la clave será 3 o 9. Además, la secuencia TT se encuentra separada por 6 espacios, lo cual confirma que la longitud de la clave es efectivamente 3. Es decir, el máximo común divisor de las distancias entre conjuntos de caracteres iguales tiene que ser un múltiplo de la longitud de la clave.

Hasta aquí hemos visto la parte del criptoanálisis que nos permite obtener la longitud de la clave a partir del texto cifrado. A continuación veremos cómo podemos obtener su valor concreto una vez hallada su longitud.

Simplificaciones

Del texto en claro se han eliminado los acentos, los signos de puntuación y los espacios para que el análisis sea más simple.

Para entender el funcionamiento criptoanalizaremos un ejemplo particular. Partiremos del siguiente texto cifrado de 404 caracteres, correspondiente a un texto en claro en castellano:

```
C =  PBVRQ VICAD SKAÑS DETSJ PSIED BGGMP SLRPW RÑPWY EDSDE ÑDRDP
     CRCPQ MNPWK UBZVS FNVRD MTIPW UEQVV CBOVN UEDIF QLONM WNUVR
     SEIKA ZYEAC EYEDS ETFPH LBHGU ÑESOM EHLBX VAEEP UÑELI SEVEF
     WHUNM CLPQP MBRRN BPVIÑ MTIBV VEÑID ANSJA MTJOK MDODS ELPWI
     UFOZM QMVNF OHASE SRJWR SFQCO TWVMB JGRPW VSUEX INQRS JEUEM
     GGRBD GNNIL AGSJI DSVSU EEINT GRUEE TFGGM PORDF OGTSS TOSEQ
     OÑTGR RIVLP WJIFW XOTGG RPQRR JSQET XRNBL ZETGG NEMUO TXJAT
     ORVJH RSFHV NUEJI BCHAS EHEUE UOTIE FFGYA TGGMP IKTBW UEÑEN
     IEEU
```

Hemos resaltado en negrita algunas de las cadenas largas que se repiten, que son:

- 3 cadenas GGMP separadas por 256 y 104 caracteres
- 2 cadenas YEDS separadas por 72 caracteres

- 2 cadenas HASE separadas por 156 caracteres
- 2 cadenas VSUE separadas por 32 caracteres

El máximo común divisor de todas estas distancias debería ser un múltiplo de la longitud de la clave. Así, en este caso, mcd (256,104,72,156,32) = 4, de modo que la clave podría tener longitud 4.

Hay que procurar no escoger cadenas demasiado cortas, ya que podría ser que se repitieran de forma aleatoria. Por ejemplo, las cadenas VR y RR (subrayadas en el criptograma anterior), se repiten dos veces la primera (VR), con una separación de 65 y 31, y también dos veces la segunda (RR), con distancias de 142 y 19. Si hubiéramos procedido al cálculo del máximo común divisor con estos valores, claramente habrían desvirtuado el valor 4 que hemos obtenido a partir de las cadenas de cuatro caracteres.

Para hallar el valor exacto de la clave, efectuaremos las siguientes manipulaciones:

1) Una vez calculada la longitud de la clave, que en nuestro ejemplo vale 4, dividiremos el texto cifrado en tantos trozos como longitud tiene la clave, en este caso 4.

2) Denominaremos *subcriptograma* a cada una de las cadenas C_A, C_B, C_C y C_D resultantes de dicha división. Para calcular dichos subcriptogramas (cuyas longitudes pueden ser diferentes), colocamos el texto cifrado en filas de longitud igual a la de la clave:

$$\begin{array}{cccc} C_1 & C_2 & C_3 & C_4 \\ C_5 & C_6 & C_7 & C_8 \\ C_9 & C_{10} & C_{11} & C_{12} \\ \ldots & \ldots & \ldots & \ldots \\ C_{401} & C_{402} & C_{403} & C_{404} \end{array}$$

Tomad cada una de las columnas resultantes como un subcriptograma, es decir:

$$C_A = C_1\ C_5\ C_9 \ldots C_{397}\ C_{401}$$
$$C_B = C_2\ C_6\ C_{10} \ldots C_{398}\ C_{402}$$
$$C_C = C_3\ C_7\ C_{11} \ldots C_{399}\ C_{403}$$
$$C_D = C_4\ C_8\ C_{12} \ldots C_{400}\ C_{404}$$

En nuestro ejemplo, los subcriptogramas quedarán constituidos por los siguientes caracteres:

C_A = PQAAEPDMRÑEEDCNUSRIECNIONSAAETLUOLAUIEULMNIIEAAOOLU
MNARSOMRSISERNAISIRTMDTOORLIORRENENOAVSNIAEOFAMTEI

C_B = BVDÑTSBPPPDÑPPPBFDPQBUFNUEZCDFBÑMBEÑSFNPBBÑBÑNMKDPF
QFSJFTBPUNJMBNGDUNUFPFSSÑRPFTPJTBTETTJFUBSUTFTPBÑE

C_C = VISSSIGSWWSDCQWZNMWVOEQMVIYESPHEEXEEEWMQRPMVISTMSWO
MOEWQWJWEQEGDISSETEGOOSETYWWGQSXLGMXOHHECEEIGGIWEE

C_D = RCKDJEGLRYDRRMKVVTUVVDLWRKEYEHGSHVPLVHCPRVTVDJJDEIZ
VHSRCVGVXRUGGLJVEGEGRGTQGVJXGRKRZGUJRRVGHHUEYGKUNU

A continuación, se aplica a cada uno de los subcriptogramas un criptosistema de sustitución simple que utilice como clave el correspondiente carácter de ésta. Para obtener el valor de cada elemento de la clave aplicaremos el **método de coincidencia múltiple**, basado en la observación de las frecuencias relativas de los caracteres de cada subcriptograma. Se trata de determinar los tres (o pueden ser más) caracteres con frecuencias más altas en el lenguaje del texto en claro que criptoanalizamos, y hallar las distancias entre ellos en el alfabeto del idioma. A continuación, determinamos los tres caracteres con frecuencias más altas en cada uno de los subcriptogramas y también analizamos sus distancias. La clave resultará de la relación de estas dos distancias.

Dado que el texto cifrado de nuestro ejemplo corresponde a un texto en claro en español, tomaremos como caracteres más frecuentes la 'A', la 'E' y la 'O'. Si en el alfabeto español la letra 'A' se halla en la posición $p(\mathrm{A}) = 0$ y la letra Z, en la posición $p(\mathrm{Z}) = 25$, las distancias entre estas letras son:

$$\begin{aligned}(p(\mathrm{A}) + 4) \bmod 27 &= p(\mathrm{E})\\ (p(\mathrm{E}) + 11) \bmod 27 &= p(\mathrm{O})\\ (p(\mathrm{O}) + 12) \bmod 27 &= p(\mathrm{A})\end{aligned} \qquad (1)$$

Y puesto que el cifrado dentro de cada subcriptograma es de sustitución simple, algún carácter del texto cifrado tendrá aproximadamente la frecuencia característica de la 'A', otro la de la 'E', y un tercero, la de la 'O'. Además, estos valores con estas tres frecuencias altas tendrán que estar separados por una relación de distancias constantes igual a la descrita en (1). Efectivamente, si calculamos la tabla de frecuencias de los diferentes caracteres en cada subcriptograma de nuestro ejemplo:

Tabla de frecuencias

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
C_A	**11**	0	2	3	**12**	1	0	0	11	0	0	5	6	9	1	**10**	2	1	9	7	4	5	1	0	0	0	0
C_B	0	**14**	1	6	4	**12**	1	0	0	4	1	0	3	6	8	6	**14**	2	1	6	9	7	1	0	0	0	1
C_C	0	0	1	2	**18**	0	7	3	7	1	0	1	7	1	0	0	2	6	1	**12**	3	0	3	12	3	2	1
C_D	0	0	3	5	7	0	**12**	6	1	7	5	4	1	1	0	6	2	1	**13**	2	3	7	**14**	0	2	3	2

Si nos fijamos, con los valores más frecuentes (marcados en negrita) para cada subcriptograma se cumplen en buena medida las distancias indicadas en (1), es decir:

$$\begin{aligned}(m_A + 4) \bmod 27 &= m_E\\ (m_E + 11) \bmod 27 &= m_O\\ (m_O + 12) \bmod 27 &= m_A\end{aligned} \qquad (2)$$

donde m_A, m_E y m_O son las posiciones de los caracteres con mayor frecuencia relativa en el subcriptograma.

Así, utilizamos C_A para calcular el primer carácter de la clave. La única solución que cumple con la ecuación (2) es la de las letras 'AEO', que tienen frecuencias (11, 12, 10), que curiosamente corresponde a cuando el texto cifrado coincide con el texto en claro.

Escribimos las ecuaciones del criptosistema de sustitución simple:

$$\begin{array}{lll} p(\mathrm{A}) + K = p(\mathrm{A}) & 0 + K = 0 & \\ p(\mathrm{E}) + K = p(\mathrm{E}) & 5 + K = 5 & K = 0 \\ p(\mathrm{O}) + K = p(\mathrm{O}) & 15 + K = 15 & \end{array}$$

De donde podemos deducir que la primera letra de la clave pueda ser la 'A'.

Para C_B, la relación de las tres letras con frecuencia más alta y que cumple (2) corresponde a 'BFP', con frecuencias (14, 12, 14). En este caso, las ecuaciones serán:

$$\begin{array}{lll} p(\mathrm{A}) + K = p(\mathrm{B}) & 0 + K = 1 & \\ p(\mathrm{E}) + K = p(\mathrm{F}) & 5 + K = 6 & K = 1 \\ p(\mathrm{O}) + K = p(\mathrm{P}) & 15 + K = 16 & \end{array}$$

La clave podría ser la 'B'.

Para C_C, la cosa no está tan clara porque las frecuencias más altas son (18, 12, 12), pero un análisis más detallado nos permite asegurar que la terna correcta es (18, 7, 12), correspondiente a la cadena 'EIS', que requiere la letra 'E' como el tercer valor de la clave.

Finalmente, para C_C, la relación de las tres letras con frecuencia más alta y que cumple (2) corresponde a 'RVG', con frecuencias (13, 14, 12), que determinan la 'R' como último valor de la clave. Luego, hemos obtenido que la clave es K = 'ABER'.

Si ahora utilizamos un algoritmo de descifrado de Vigenère con el criptograma inicial C y la clave obtenida K, obtendremos el siguiente texto en claro:

M= PARA QUE LA COSA NO ME SORPRENDA COMO EN OTROS AÑOS, HE COMENZADO YA CON UNOS SUAVES EJERCICIOS DE PRECALENTAMIENTO; MIENTRAS DESAYUNABA HE CONTEMPLADO UNA BOLA PLATEADA I UNA TIRA DE ESPUMILLÓN Y MAÑANA ME INICIARÉ EN EL AMOR AL PRÓJIMO CON LOS QUE LIMPIEN EL PARABRISAS EN LOS SEMÁFOROS. ESTA GIMNASIA DEL CORAZÓN METAFÓRICO ES TAN IMPORTANTE COMO LA DEL OTRO CORAZÓN PORQUE LOS RIESGOS CORONARIOS ESTÁN AHÍ

Como vemos, el método de criptoanálisis de Kasiski es estadístico; no es, pues –ni mucho menos– totalmente exacto o infalible. Por ejemplo, puede suceder que al buscar la longitud de la clave se repitan por azar cadenas de caracteres cuya separación no sea un múltiplo de la clave; o peor, que sea un número primo, con lo que el máximo común divisor sería 1. Para evitar estas situaciones necesitaremos criptogramas de textos largos (de varios centenares de caracteres) y buscaremos repeticiones de cadenas de al menos 3 elementos que aparezcan más de dos veces. Por otra parte, puede ocurrir que si los subcriptogramas son pequeños, no se conserve la rotación modular de las letras de frecuencia más alta, de modo que la clave no sea tan simple de obtener en un primer análisis.

Resumen

En este módulo hemos presentado los fundamentos de la criptografía desde cuatro aspectos diferentes:

1) Los **criptosistemas históricos**, basados en los principios de transposición y de sustitución, que se utilizaban antes de la aparición de los ordenadores. De todos modos, las cifras de transposición y de sustitución se continúan utilizando como bloques constituyentes de muchas de las cifras actuales.

2) Los **fundamentos de la teoría de la información** y, de una manera especial, el concepto de **entropía de Shannon**, que proporcionan un marco teórico para cuantificar la seguridad de los criptosistemas, tanto con respecto al secreto como a la autenticidad.

3)El **secreto perfecto** y la **autenticidad perfecta**, que son dos propiedades independientes y difícilmente alcanzables en la práctica. Sirven como guía de lo que se debería tender a conseguir al diseñar criptosistemas. La teoría de la información permite formular ambas propiedades con precisión.

4) Las **bases del criptoanálisis elemental**, en particular, dos conceptos:

a) La **suposición de Kerckhoffs**, según la cual los algoritmos de cifrado y de descifrado han de ser públicos y el único parámetro secreto tiene que ser la clave.

b) La **distancia de unicidad**, que está relacionada con la redundancia del texto en claro y es la cantidad de texto cifrado que un criptoanalista tiene que obtener para que haya una sola clave que pueda producir este texto cifrado a partir de un texto en claro con sentido. Con todo, el hecho de que la clave quede determinada de manera única no quiere decir que sea computacionalmente fácil de hallar.

Actividades

1. Implementad la cifra de Beale utilizando como clave cualquier texto bastante largo.

2. Escribid un programa que simule una máquina de 10 rotores.

3. Tomad un texto lo bastante largo e intentad determinar la tasa r y la redundancia D del español. Debéis seguir son los siguientes:
a) Considerad sólo las letras del texto y no distingáis entre mayúsculas y minúsculas. Contad la letra 'ñ' como si fuera una 'n'. No contéis espacios ni los signos de puntuación.
b) Escribid un programa que calcule la frecuencia relativa de cada una de las 26 letras en el texto.
c) Calculad la entropía de un carácter del texto; utilizad las frecuencias calculadas como si fueran probabilidades de aparición de las letras en español. Esta entropía ofrece una aproximación de r.
d) Obtened $D = R - r = 4{,}7 - r$. Calculad la proporción de redundancia como D/R.

Ejercicios de autoevaluación

1. Suponed que la frecuencia relativa de aparición de la letra 'a' en un texto en claro sea 0,1. ¿Si se utiliza una cifra de transposición, habrá necesariamente alguna letra en el texto cifrado que tenga la misma frecuencia? ¿Si el digrama 'ch' aparece con una frecuencia 0,02 al texto en claro, habrá algún digrama en el texto cifrado con la misma frecuencia?

2. Descifrad el texto cifrado siguiente con la cifra de César utilizando $k = 3$.

HVWRHVIDFLO

3. Considerad los textos cifrados siguientes:
- XXXXX.
- VWXYZ.
- RKTIC.
- JZQAT.

¿Cuáles de estas palabras podrían ser el resultado de cifrar palabras de cinco letras utilizando:
a) Una cifra de sustitución simple, no necesariamente del tipo César?
b) Cualquier cifra de transposición?

4. Sea X una variable aleatoria entera representada por 32 bits. Suponed que la probabilidad de que X caiga dentro del intervalo $[0, 2^8 - 1]$ sea 1/2, con todos los valores del intervalo equiprobables; la probabilidad de que X caiga dentro del intervalo $[2^8, 2^{32} - 1]$ también sea 1/2 y también con todos los valores del intervalo equiprobables. A partir de esta información, calculad $H(X)$.

5. Sea M uno de los seis mensajes A, B, C, D, E, F donde $p(A) = p(B) = p(C) = 1/4$, $p(D) = 1/8$, $p(E) = p(F) = 1/16$. Calculad $H(M)$.

6. Demostrad que si M puede tomar dos valores, $H(M)$ es máxima para $p_1 = p_2 = 1/2$. Generalizadlo para cualquier n, es decir, probad que si M puede tomar n valores, $H(M)$ es máxima cuando todos los valores son equiprobables.

7. Explicad por qué una cifra puede ser computacionalmente segura aunque tenga una distancia de unicidad pequeña.

Solucionario

Ejercicios de autoevaluación

1. En una cifra de transposición se conserva la distribución de frecuencias. Así, pues, la letra cifrada correspondiente a la 'a' tendrá exactamente la misma frecuencia 0,1. En cambio, dos letras contiguas en el texto en claro no tienen por qué serlo en el texto cifrado. En particular, el digrama 'ch' no tendrá ningún digrama correspondiente al texto cifrado y, por lo tanto, no se conservará la frecuencia.

2. El resultado del descifrado es el texto en claro siguiente:

ESTOESFACIL

3. La palabra cifrada XXXXX no se puede obtener como resultado de invertir las letras de una palabra (no hay ninguna palabra en el diccionario que conste de cinco letras iguales). Por la misma razón, XXXXX no puede ser obtenida con una cifra de sustitución simple. El resto de palabras se pueden obtener por una sustitución simple, pero no por transposición.

4. Cada uno de los 2^8 valores del intervalo $[0, 2^8 - 1]$ se toman con probabilidad 2^{-9}. Cada uno de los $2^{32} - 2^8$ valores restantes se toman con probabilidad:

$$\frac{1}{2 \cdot (2^{32} - 2^8)} = \frac{1}{2^{33} - 2^9}$$

Por lo tanto, la entropía de X será:

$$H(X) = 2^8 \cdot (2^{-9} \log_2 2^9) + (2^{32} - 2^8) \cdot \left(\frac{1}{2^{33} - 2^9} \cdot \log_2(2^{33} - 2^9)\right) \approx \frac{9}{2} + \frac{1}{2} 33 = 21 \text{ bits.}$$

Así, pues, vemos que el contenido informativo de la variable es bastante menor que los 32 bits usados para representarla.

5. La entropía de M es la siguiente:

$$H(M) = 3 \cdot \frac{1}{4} \cdot \log_2 4 + \frac{1}{8} \cdot \log_2 8 + 2 \cdot \frac{1}{16} \cdot \log_2 16 = 6/4 + 3/8 + 8/16 = 2.375 \text{ bits.}$$

6. Con dos valores posibles para X, la probabilidad del segundo valor es $p_2 = 1 - p_1$. Luego:

$$H(X) = H(p_1) = p_1 \log_2\left(\frac{1}{p_1}\right) + (1 - p_1) \log_2\left(\frac{1}{1 - p_1}\right).$$

Si derivamos respecto a p_1 e igualamos a cero, obtenemos un máximo de $H(p_1)$ en $p_1 = 1/2$. En el caso de n valores posibles, se trata de hallar el máximo de la función $H(p_1,...,p_n)$ sujeta a la siguiente restricción:

$$\sum_{i=1}^{n} p_i = 1.$$

Por el método de los multiplicadores de Lagrange, obtenemos el máximo para $p_1 = ... = p_n = 1/n$.

7. Si la distancia vale d y damos como entrada a un ordenador d caracteres de texto cifrado, tarde o temprano el ordenador hallará una única clave que pueda producir los d caracteres. Ahora bien, puede suceder que el ordenador necesite un tiempo demasiado largo (años o incluso siglos, según el algoritmo de cifrado), incluso para un valor de d pequeño.

Glosario

ambigüedad de clave *f* Incertidumbre que queda sobre el valor de la clave tras conocer un criptograma.

autenticidad perfecta *f* Propiedad que posee una cifra cuando la probabilidad de engaño del receptor con éxito por parte de un criptoanalista es mínima.

criptosistema histórico *m* Criptosistema utilizado antes de la aparición de los ordenadores.

descifrado espurio *m* decodificación que existe cuando, dado un texto cifrado $c = E_k(m)$, el cifrado bajo otra clave k' puede dar c; es decir, $c = E_{k'}(m)$ para el mismo mensaje m, o bien $c = E_{k'}(m')$ para otro mensaje con sentido m'.

distancia de unicidad *f* Número mínimo de caracteres de texto cifrado tal que existe una única clave que produce estos caracteres de texto cifrado a partir de un texto en claro con sentido.

entropía de Shannon *f* Entropía de una variable aleatoria que mide, en bits, la incertidumbre sobre el valor que tomará la variable.

probabilidad de engaño *f* Probabilidad de que un criptoanalista enemigo consiga engañar al receptor y hacerle aceptar como bueno un mensaje modificado o un mensaje insertado.

suposición de Kerckhoffs *f* Suposición según la cual los algoritmos de cifrado y de descifrado de un criptosistema son públicos y el secreto queda restringido a la clave utilizada.

teoría de la información *f* Teoría introducida por Shannon que mide la información desde un punto de vista cuantitativo.

variable aleatoria *f* Variable que toma un valor entre un grupo de valores posibles, de modo que cada valor posible tiene una cierta probabilidad no nula de ser adoptado.

Bibliografía

Bibliografía básica

Denning, D. E. (1982). *Cryptography and data security*. Reading: Addison-Wesley.

Kahn, D. (1967). *The codebreakers*. Nueva York: Macmillan.

Rifó, J.; Huguet, L. (1991). *Comunicación digital*. Barcelona: Masson.

Simmons, G. J. (1992). *Contemporary cryptology: the science of information integrity*. Nueva York: IEEE Press.

Stinson, D. (1995). *Cryptography: theory and practice*. Boca Raton: CRC Press.

Referencias bibliográficas

Porta, G. B. (1593). *De occultis literarum* (libro 1, capítulo 1). Edición facsímil (1996). Zaragoza: Universidad de Zaragoza.