Clase 17

Criptografía de Clave Secreta

- El escenario que estudia la criptografía, en un esquema de clave secreta, es el siguiente:
- ✦ Alicia quiere enviar un mensaje X a Bernat
- ✦ Oscar ha interceptado la señal del canal de comunicaciones
- ✦ Alicia y Bernat comparten una clave (secreta) K
- ✦ Alicia encripta X usando K y obtiene el mensaje encriptado Y
- ✦ Alicia envía Y a Bernat
- ✦ Bernat desencripta Y usando K y recupera X

- El objetivo es proteger el mensaje X de Oscar, quien intercepta Y pero (en principio) no puede recuperar X. Por supuesto, esto implica en particular que Oscar no tiene acceso a la clave secreta K, ni puede deducirla a partir de Y.
- Cifrado de César: En este criptosistema, lo primero es codificar el texto de un mensaje X dado, que supondremos contiene sólo caracteres del alfabeto (excluyendo espacios y la letra ñ). Para eso asociamos a las 26 letras del alfabeto los números del 0 al 25, en el orden usual (alfabético). La clave K se fija como un entero en el intervalo [0, 25].

- Para encriptar, dado un mensaje X (que suponemos ya codificado, con lo cual está formado por enteros en [0, 25]), a cada uno de los números que lo forman le sumamos K, y reducimos el resultado módulo 26 para de nuevo volver a obtener enteros en el intervalo [0, 25].
- Si decodificamos el resultado obtenido, es decir, sustituimos ahora los enteros obtenidos por las correspondientes letras del alfabeto, obtenemos el mensaje Y que se envía (mensaje encriptado).
- Para desencriptar el mensaje Y recibido, Bernat debe deshacer el proceso haciendo uso de la clave secreta K: primero transforma las letras de Y en números del intervalo [0, 25] (codifica), luego resta K a cada uno de los números obtenidos y reduce el resultado módulo 26 (es decir, coge el representante en el intervalo [0, 25] de cada resultado), y finalmente transforma los números obtenidos en las correspondientes letras del alfabeto.

- Si, para simplificar la notación, identificamos un mensaje de texto con el correspondiente mensaje codificado (es decir, suponemos que los mensajes son cadenas de enteros en el intervalo [0, 25]), los procesos de encriptado y desencriptado vienen por lo tanto dados por una función y su inversa, ambas a valores en $\mathbb{Z}/26\,\mathbb{Z}$, y esta función es simplemente sumar la constante K en cada componente, con la suma en $\mathbb{Z}/26\,\mathbb{Z}$:
- $X = (x_1, x_2, \ldots, x_n) \in (\mathbb{Z}/26\,\mathbb{Z})^n \rightarrow X + \vec{K} = (x_1 + K, x_2 + K, \ldots, x_n + K) \in (\mathbb{Z}/26\,\mathbb{Z})^n$
- Si $X + \vec{K} := Y = (y_1, y_2, \ldots, y_n) \rightarrow Y - \vec{K} = (y_1 - K, y_2 - K, \ldots, y_n - K) = X \in (\mathbb{Z}/26\,\mathbb{Z})^n$
- Donde X es el mensaje a enviar e Y el mensaje encriptado que se envía.
- Tras desencriptar Y Bernat obtiene $Y - \vec{K}$ que vemos claramente que es el mensaje original X pues se han aplicado en las componentes las funciones inversas $F(x) = x + K$, $F^{-1}(y) = y - K$, ambas definidas en $\mathbb{Z}/26\,\mathbb{Z}$.

Ejemplo: Si Alicia y Bernat han acordado en usar la clave K = 10, averigua cuál es el mensaje que ha enviado Alicia si Bernat recibe:

Y = WKVNSDYFSBEC

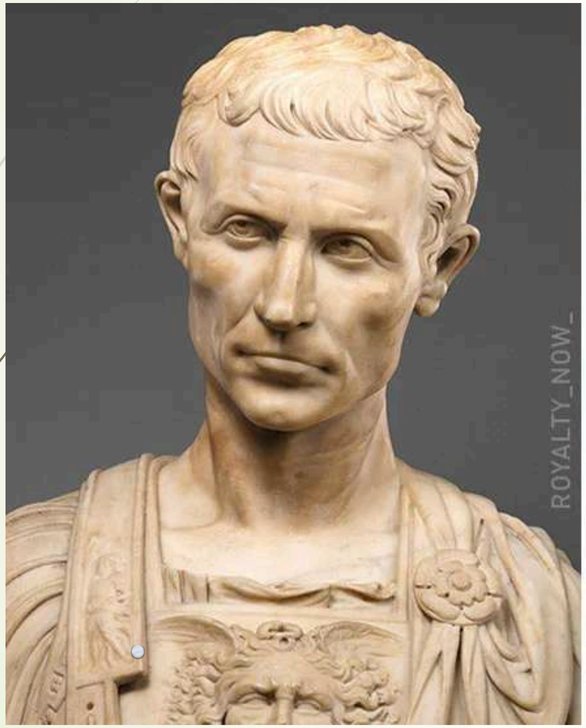
Codificando Y obtenemos: C(Y) = (22, 10, 21, 13, 18, 3, 24, 5, 18, 1, 4, 2)

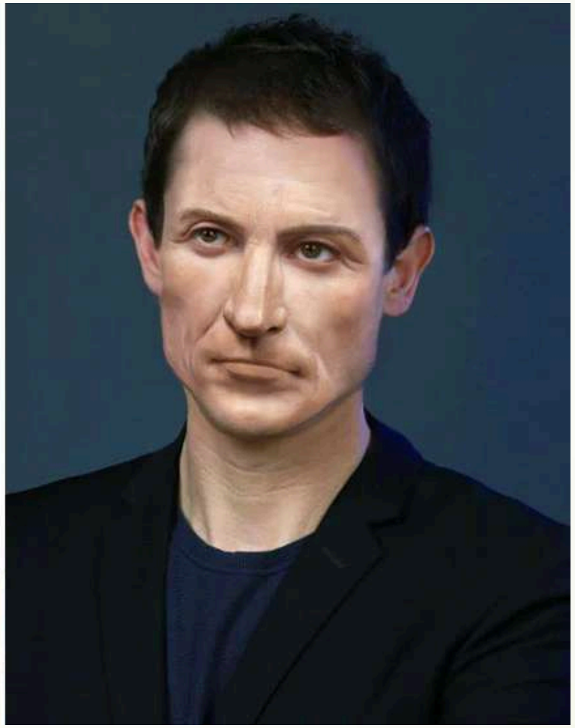
Desencripamos restando K = 10 a cada componente (y reduciendo módulo 26): C(Y) – K = (12, 0, 11, 3, 8, 19, 14, 21, 8, 17, 20, 18).

Las letras correspondientes a esta lista de números forman el mensaje:

X= MALDITOVIRUS

Ejercicio: En la película "2001, Una odisea del espacio" el ordenador de a bordo de la nave se llama HAL 9000. Si sabes que el nombre HAL fue obtenido por el escritor (A.C.Clarke) aplicando el cifrado de César a una marca conocida, ¿puedes decir cuál es esta marca, y cuál es la clave secreta K utilizada?





Julio César

Veamos ahora la definición formal de Criptosistema:

Definición: Un criptosistema es una quíntupla (T, C, K, E, D) tal que:

1) T es el conjunto finito de textos posibles

2) C es el conjunto finito de textos encriptados posibles

3) K es el conjunto finito de claves posibles

4) Para cada $k \in K$, hay una función de encriptado $e_k \in E$ y una función de desencriptado $d_k \in D$ tal que:

$$d_k(e_k(x)) = x, \text{ para todo texto } x \in T.$$

- Propiedades de un buen criptosistema:
- ✭ Para todo $k \in K$, las funciones de encriptado y desencriptado e_k y d_k se pueden calcular efectivamente, en "tiempo razonable" (es decir, el tiempo que se tarda tiene que ser polinomial en el tamaño del mensaje x).
- ✭ Dado un texto encriptado, debe ser difícil para un oponente (que no conoce la clave $k \in K$) identificar la clave y el texto original. "Difícil" en particular implica que cualquier ataque para romper el criptosistema sea un algoritmo que NO es polinomial en el tamaño de los mensajes.
- Esta dificultad debe persistir aún si el enemigo conoce como funciona el criptosistema: la seguridad se basa (sólamente) en mantener secreta la clave k (principio de Kerckhoffs).

A. Kerckhoffs

- El cifrado de César, descrito bajo este esquema (asumiendo que el mensaje ya se ha codificado), tiene los siguientes elementos: $(T = \mathbb{Z}/ 26\mathbb{Z})^m$,
- $C = (\mathbb{Z}/ 26\mathbb{Z})^m$, para un m apropiado, $K = \mathbb{Z}/26\mathbb{Z}$. Dado $k \in K$, la función e_k , de T en C, es la función que en cada componente viene dada por $e_k(x) = x + k$. Por último, la función d_k , de C en T, es la que en cada componente tiene la ley $d_k(y) = y - k$.
- Recordar que como estas funciones están definidas en las clases residuales que forman $\mathbb{Z}/26\mathbb{Z}$ (donde para cada clase cogemos siempre el representante en el intervalo [0, 25]), las fórmulas anteriores, por ejemplo $e_k(x) = x + k$, hay que interpretarlas como congruencias módulo 26.

Clase 18

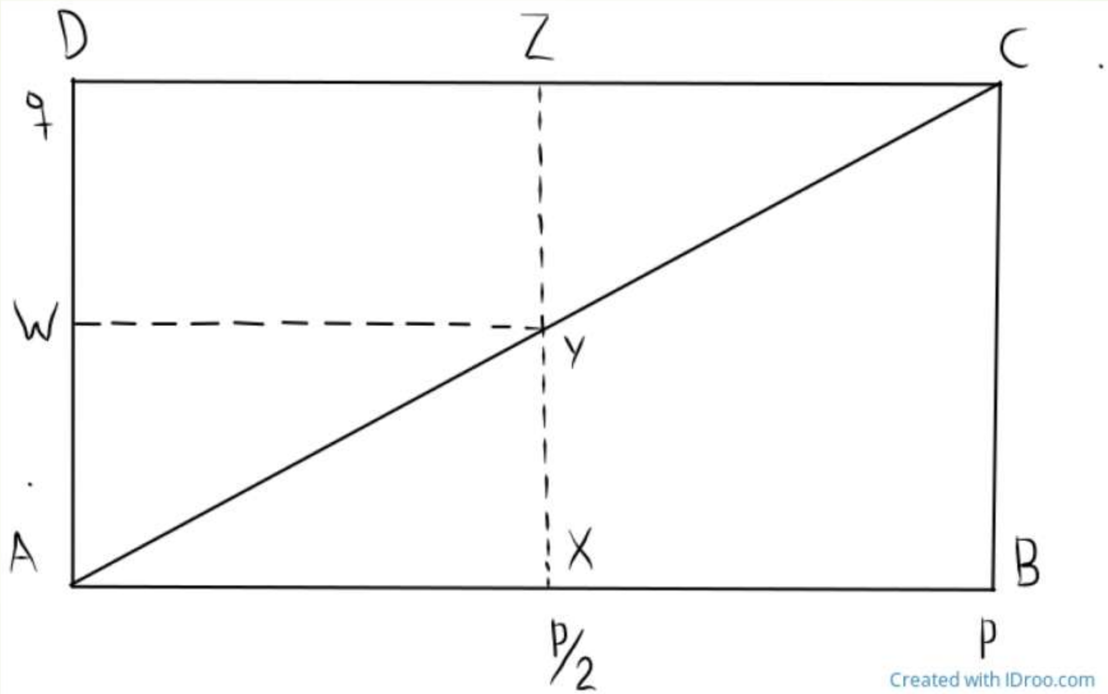
Teorema (Ley de Reciprocidad Cuadrática):

Sean p y q primos impares distintos. Entonces se tiene:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot \ (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Demostración: Partimos del lema de Eisenstein: $\left(\frac{q}{p}\right) = (-1)^{\sum_u \left[\frac{qu}{p}\right]}$ donde u recorre los números pares del intervalo [2, p-1].

La suma en el exponente cuenta la cantidad de puntos de coordenadas enteras tales que su coordenada x es par y están dentro del triángulo ABC en la siguiente figura:



- Pues como los catetos de ABC miden p y q, por proporcionalidad (Teorema de Tales) para cualquier v entre 0 y p la vertical por v corta al segmento AC en un punto con ordenada w = v · $\frac{q}{p}$.

Consideremos, de entre estos puntos, aquellos que quedan dentro del trapecio XYCB (es decir, aquellos que tienen la coordenada x mayor que p/2). Como el total de puntos con coordenada x par dentro del rectángulo ZCBX es par (pues hay q-1 en cada columna) ⇨

#{puntos con x par dentro de XYCB} + #{puntos con x par dentro de YZC} =

#{puntos con x par dentro de ZCBX} ≡ 0 (mod 2) ⇨

#{puntos con x par dentro de XYCB} ≡ #{puntos con x par dentro de YZC} (mod 2) (i).

Por otro lado, si consideramos la cantidad de puntos con x par dentro de YZC, vemos por simetría (respecto al punto Y) que ésta es igual a la cantidad de puntos con x impar dentro del triángulo YXA (ii).

- Aplicando (i) y (ii), vemos que el exponente de -1 en el lema de Eisenstein es igual a:
- #{puntos con x par dentro de ABC} = #{puntos con x par dentro de AYX} +
- #{puntos con x par dentro dentro de XYCB} ≡
- #{puntos con x par dentro de AYX} + #{puntos con x par dentro de ZYC} =
- #{puntos con x par dentro de AYX} + #{puntos con x impar dentro de AYX} = #{puntos de coordenadas enteras dentro del triángulo AYX} := μ , donde la congruencia (entre el segundo y tercer término) es módulo 2.
- Luego, se tiene: $\left(\frac{q}{p}\right)$ = $(-1)^{\mu}$.

- Un argumento similar, pero intercambiando los roles de p y q, permite probar que: $\left(\frac{p}{q}\right)$ = (-1)$^{\nu}$ donde ν es la cantidad de puntos de coordenadas enteras dentro del triángulo WYA. Como no hay puntos de coordenadas enteras sobre el segmento AY (por el teorema de Tales: como p y q so coprimos no puede darse $\frac{y}{x} = \frac{q}{p}$ con x, y enteros, 0 < x < p) se tiene:
- $\mu + \nu$ = #{puntos de coordenadas enteras dentro de AXYW} = $\frac{p-1}{2} \cdot \frac{q-1}{2}$, con lo cual (-1)$^{\mu+\nu}$ = $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$. Combinando con las dos fórmulas previas obtenemos: $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right)$ = (-1)$^{\mu+\nu}$ = $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$, y de aquí:
- $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

- Corolario: Sean p y q primos impares distintos. Entonces se tiene:
- $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ si al menos uno de estos primos es congruente con 1 módulo 4, y
- $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ si tanto p como q son congruentes con 3 módulo 4.
- Demostración: Es consecuencia directa de la Ley de Reciprocidad Cuadrática. Por esta ley, vemos que $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ se cumple sí y sólo sí el exponente de -1 en la fórmula, que es $\frac{p-1}{2} \cdot \frac{q-1}{2}$, es par. Esto a su vez equivale a que al menos uno de los factores $\frac{p-1}{2}$ y $\frac{q-1}{2}$ sea par, que equivale a pedir que se cumpla: $p - 1 \equiv 0 \pmod 4$ o $q - 1 \equiv 0 \pmod 4$, es decir: $p \equiv 1 \pmod 4$ o $q \equiv 1 \pmod 4$.