EL CIFRADO DE VIGENÈRE ⇝ S. XVI

QUE SE USAN PARA ROMPER LOS CIFRADOS DE SUST

PARA EVITAR EL USO DE ANÁLISIS DE FRECUENCIA, ESTE CIFRADO UTILIZA UNA TRASLACIÓN DISTINTA POR CADA LETRA DEL MENSAJE.

EJEMPLO: SI LA PALABRA CLAVE ES "ESO" Y QUEREMOS ENCRIPTAR EL MENSAJE "VAMOS LOS CELESTES",

+ VAMOS LOS CELESTES
  ESOESOESOESOESOE
= ZSASKZSKQIDSWLSW

+: TRASLADAMOS COLUMNA A COLUMNA COMO EN EL CIFRADO DEL CÉSA

⇝ ES COMO SUMAR EN $\mathbb{Z}/26$ (SACAMOS LA Ñ)

+ V ⟷ 21 | M ⟷ 12
  E ⟷ 4 | O ⟷ 14
  Z ⟷ 25 | A ⟷ 0

OBS: LA "E" SE TRANSFORMA TANTO EN "I" COMO EN "S"

⇝ SE ROMPE CON LAS FRECUENCIAS

PARA DESENCRIPTAR, BETO DEBE CONOCER LA CLAVE

  ZSASK...
- ESOESOESOESOESOE
  VAMOSLOSCELESTES

OBS:
  ZSASK...
- VAMOSLOSCELESTES
  ESOESO

⇝ ES VULNERABLE A UN ATAQUE DE TEXTO PLANO ELEGIDO

EJERCICIO: IMPLEMENTAR EN SAGE FUNCIONES DE CIFRADO / DESCIFRADO

¿CÓMO ROMPER ESTE CIFRADO?

1ER OBJETIVO: HALLAR EL LARGO DE LA CLAVE.

PARA ESTO, SE PUEDEN UTILIZAR LAS SIG. DOS HERRAMIENTAS

MÉTODO DE KASISKI: SI UN TRIGRAMA SE REPITE MUCHAS VECES, ES PROBABLE QUE EL LARGO DE LA CLAVE DIVIDA A LAS DIFERENCIAS ENTRE LOS TRIGRAMAS

↳ NO SIRVEN SI LA CLAVE ES MUY LARGA... PERO PUEDE UNA CLAVE LARGA NO ES CONVENIENTE

EJEMPLO (CON DIGRAMAS):

EN EL ANTERIOR, LOS DIGRAMAS REPETIDOS SON

ZS, SK, SW

↓ DIF. 5 ↓ DIF. 3 ↓ DIF. 3

↳ UNO "INTUYE" QUE EL LARGO DE LA CLAVE ES 3.

(SIRVE POR LO GENERAL PARA MENSAJES LARGOS)

ÍNDICE DE COINCIDENCIA

DADO UN STRING S,

indco(S) := PROB. DE QUE DOS CARACTERES DE S ELEGIDOS AL AZAR SEAN IGUALES ↳ "ÍNDICE DE COINCIDENCIA"

¿CÓMO LO CALCULAMOS?

SI F_i := # VECES QUE LA i-ÉSIMA LETRA DEL ABECEDARIO APARECE EN S,

$$\text{ind}_{CO}(S) = \frac{\#\text{CASOS FAVORABLES}}{\#\text{CASOS POSIBLES}} = \frac{\sum_{i=0}^{25} \#\text{SUBCONJ DE DOS LETRAS } i\text{-ÉSIMAS}}{\binom{m}{2}}$$

m = LARGO DE S

$$= \frac{\sum_{i=0}^{25} \binom{F_i}{2}}{\binom{m}{2}} = \frac{\sum_{i=0}^{25} F_i(F_i-1)}{m(m-1)}$$

OBS: SI SE TIENE QUE $F_i = m/26$ (ie, TODOS LOS CARACTERES APARECEN LA MISMA CANTIDAD DE VECES) 9.

$$\text{ind}_{CO}(S) = \frac{\frac{m}{26}\left(\frac{m}{26}-1\right)}{m(m-1)} = \frac{1/26 - 1/m}{1-1/m} \longrightarrow 1/26 = 0{,}0385\ldots$$

$m \to \infty$

IDEA: DADO UN STRING $S = C_1C_2C_3\cdots$ (QUE PENSAMOS COMO UN TEXTO CIFRADO CON VIGENERE), CONSIDERAMOS, PARA $k \in \mathbb{N}$, LOS STRINGS $S_1, \ldots, S_k$ DADOS POR

$$S_i = C_i\, C_{i+k}\, C_{i+2k}\, C_{i+3k} \cdots$$

ENTONCES, SI k ES EL LARGO DE LA CLAVE, TODOS LOS CARACTERES DE S_i FUERON TRASLADADOS USANDO LA MISMA LETRA DE LA CLAVE

$$\rightsquigarrow \text{ind}_{CO}(S_i) \approx \text{ind}_{CO}(\text{TEXTO EN INGLÉS/CASTELLANO})$$

$$\approx 0{,}068 \,/\, 0{,}074;$$

SI k NO ES EL LARGO, S_i SERÁ TEXTO MÁS BIEN ALEATORIO, POR LO QUE ESPERAMOS $\text{ind}_{CO}(S_i) \approx 0{,}038\ldots$

~> PARA AVERIGUAR EL LARGO DE LA CLAVE, BUSCO k PARA EL CUAL $\text{ind}_0(S_1), \ldots, \text{ind}_0(S_k)$ SEAN LO MÁS GRANDES POSIBLES.

HALLADO k: SI LA CLAVE ES $p = p_1 \ldots p_k$, ↘ Y EL MENSAJE $m = m_1 m_2 \ldots$

TENDREMOS QUE PARA $1 \le i \le k$,

$$\begin{array}{llll} & m_i & m_{i+k} & m_{i+2k} \ldots \\ + & p_i & p_i & p_i \ldots \\ \hline & c_i & c_{i+k} & c_{i+2k} \ldots \end{array}$$

~> HAGO UN ANÁLISIS DE FREC. SOBRE S_i, Y DE AHÍ BUSCO HALLAR p_i.

EJ: SI LA QUE MÁS APARECE EN S_i ES H, ES PROBABLE QUE $p_i = D$, YA QUE "E + D = H"

↓ LA QUE MÁS APARECE EN INGLÉS