Criptografía y Seguridad
Tarea 1

Alumnos:
Barredo Escalona Paola Betsabe
Altamirano Niño Luis Enrique

17 de junio de 2022

Preguntas

1. a) Sea $M = a$ y $C = x$, entonces como $|\mathcal{M}| = 26$ se tiene que:

$$P(M = a) = \frac{1}{26} \text{ y } P(C = x) = \frac{1}{26}$$

Ahora calculemos $P(C = x|M = a)$, entonces si tomamos los índices de las posiciones de ambas letras en $\mathcal{M}$, tenemos que $a \mapsto 1$ y $x \mapsto 24$, y como $E(k, m) = k + m$ mód 26, entonces:

$$24 = k + 1 \text{ mód } 26$$

entonces si resolvemos la ecuación, se tiene que:

$$k = 26y + 23 \text{ con } y \in \mathbb{Z}$$

pero como $|\mathcal{K}| = 27$, entonces $1 \leq k \leq 27$, por lo que el único valor posible para y es 0, en ese caso:

$$k = 26 \cdot 0 + 23 = 23$$

entonces:

$$P(C = x|M = a) = \frac{1}{27}$$

y por lo tanto:

$$\begin{aligned} P(M = a|C = x) &= \frac{P(C = x|M = a) \cdot P(M = a)}{P(C = x)} \qquad \text{(Teorema de Bayes)} \\ &= \frac{\frac{1}{27} \cdot \frac{1}{26}}{\frac{1}{26}} \\ &= \frac{1}{27} \neq \frac{1}{26} = P(M = a) \end{aligned}$$

por lo que:

$$P(M = a) \neq P(M = a|C = x)$$

y el mecanismo no es perfectamente seguro.

b) Sean $m \in \mathcal{M}, c \in C = \mathcal{M}$, como $|\mathcal{M}| = 26$, entonces

$$P(M = m) = \frac{1}{26} \text{ y } P(C = c) = \frac{1}{26}$$

ahora:

$$P(C = c|M = m) = \frac{1}{26}$$

ya que ahora $|\mathcal{K}| = 26$, y para cada mensaje m solo existe una llave k que lo cifra en c.

Por lo tanto:

$$\begin{aligned} P(M = m|C = c) &= \frac{P(C = c|M = m) \cdot P(M = m)}{P(C = c)} \qquad \text{(Teorema de Bayes)} \\ &= \frac{\frac{1}{26} \cdot \frac{1}{26}}{\frac{1}{26}} \\ &= \frac{1}{26} \\ &= P(M = m) \end{aligned}$$

por lo que:

$$P(M = m) = P(M = m|C = c)$$

y el mecanismo ahora es perfectamente seguro.

2.

3. *a*) Tenemos que $c =$`0xfb0762a891`, entonces como `ff` $\mapsto$ `fb`, `75` $\mapsto$ `62` y `04` $\mapsto$ `91`, y se trata de una simple sustitución monoalfabética, entonces solo sustituiremos el byte `fb` por `ff`, `62` por `75`, `91` por `04` y el resto de los bytes quedarán igual , entonces se tiene que $m =$ `0xff0775a804`.

   b) Para Vigenere con desplazamientos, si k_i es la parte de la llave que se usó para cifrar m_j y obtener c_j se tiene que:

$$D(k_i, c_j) = c_j + k_i \text{ mód } 256 = m_j$$

   Si empatamos a c con k y repetimos k tantas veces como sea necesario, tendremos que:

$$\begin{aligned} c &= \texttt{0x 00ab23cd45} \\ k &= \texttt{0x fa03fa03fa} \end{aligned}$$

   Ahora si separamos cada byte de c y k, y obtenemos su representación en decimal se tendrá que:

$$\begin{aligned} 00 &\equiv 0 \\ ab &\equiv 171 \\ 23 &\equiv 35 \\ cd &\equiv 205 \\ 45 &\equiv 69 \\ fa &\equiv 250 \\ 03 &\equiv 3 \end{aligned}$$

   Entonces:

$$\begin{aligned} m_1 &= \texttt{00} + \texttt{fa} \text{ mód } 256 = 0 + 250 \text{ mód } 256 = 250 \text{ mód } 256 = 250 \equiv \texttt{fa} \\ m_2 &= \texttt{ab} + \texttt{03} \text{ mód } 256 = 171 + 3 \text{ mód } 256 = 174 \text{ mód } 256 = 174 \equiv \texttt{ae} \\ m_3 &= \texttt{23} + \texttt{fa} \text{ mód } 256 = 35 + 250 \text{ mód } 256 = 285 \text{ mód } 256 = 29 \equiv \texttt{1d} \\ m_4 &= \texttt{cd} + \texttt{03} \text{ mód } 256 = 205 + 3 \text{ mód } 256 = 208 \text{ mód } 256 = 208 \equiv \texttt{d0} \\ m_5 &= \texttt{45} + \texttt{fa} \text{ mód } 256 = 69 + 250 \text{ mód } 256 = 319 \text{ mód } 256 = 63 \equiv \texttt{3f} \end{aligned}$$

   Y por lo tanto $m =$`0xfaae1dd03f`.

   c) Si $k = (a, b)$ y $c = c_1 c_2 \dots c_n$ se tiene que:

$$m_i = (c_i - b)a^{-1} \text{ mód } 256$$

donde a^{-1} representa el inverso multiplicativo de a mód 256, en este caso $a = 255$ y $a^{-1} = 255$ puesto que:

$$255 \cdot 255 \equiv 1 \text{ mód } 256$$
$$65025 \equiv 1 \text{ mód } 256$$

ya que 256 divide a $65025 - 1 = 65024$, además:

$$\texttt{23} \equiv 35$$
$$\texttt{aa} \equiv 170$$
$$\texttt{7f} \equiv 127$$

entonces:

$$m_1 = (35 - 7)255 \text{ mód } 256 = 28 \cdot 255 \text{ mód } 256 = 7140 \text{ mód } 256 = 228 \equiv \texttt{e4}$$
$$m_2 = (170 - 7)255 \text{ mód } 256 = 163 \cdot 255 \text{ mód } 256 = 41565 \text{ mód } 256 = 93 \equiv \texttt{5d}$$
$$m_3 = (127 - 7)255 \text{ mód } 256 = 120 \cdot 255 \text{ mód } 256 = 30600 \text{ mód } 256 = 136 \equiv \texttt{88}$$

Por lo tanto $m =$`0xe45d88`.

4. El texto claro en español es:

```
HAAHIGZ BCVM MS RSHVMYH BMS BMZGMAYL RHCS ZM MURMJL H ZMVYGA VMAOGLZL
ARRAKIS DUNE EL PLANETA DEL DESIERTO PAUL SE EMPEZO A SENTIR NERVIOSO

T BMPGBGL RAHPYGPHA CVL BM SLZ MEMAPGPGLZ PLARLAHSMZ UMVYHSMZ
Y DECIDIO PRACTICAR UNO DE LOS EJERCICIOS CORPORALES MENTALES

DCM SM WHÑGH MVZMNHBL ZC UHBAM YAMZ AHRGBHZ GVZRGAHPGLVMZ BMZMVPHBMVHALV
QUE LE HABIA ENSEÑADO SU MADRE TRES RAPIDAS INSPIRACIONES DESENCADENARON

SHZ AMZRCMZYHZ MZYHBL BM RMAPMRPGLV QSLYHVYM HECZYM BM
LAS RESPUESTAS ESTADO DE PERCEPCION FLOTANTE AJUSTE DE

ZC PLVZPGMVPGH BGSHYHPGLV HLAYGPH HSMEHUGMVYL BM YLBL UMPHVGZUL
SU CONSCIENCIA DILATACION AORTICA ALEJAMIENTO DE TODO MECANISMO

VL QLPHSGJHBL PLVPGMVPGHPGLV BMSGÑMAHBH MVAGDCMPGUGMVYL BM
NO FOCALIZADO CONCIENCIACION DELIBERADA ENRIQUECIMIENTO DE

SH ZHVXAM M GAAGXHPGLV BM SHZ AMXGLVMZ ZLÑAMPHAXHBHZ
LA SANGRE E IRRIGACION DE LAS REGIONES SOBRECARGADAS
```

Figura 1: texto descifrado

Lo primero que se hizo fue usar la tabla de frecuencias de las letras en el idioma español para tratar de mapear cada letra con su correspondiente (en función de la frecuencia), y como después de hacer eso aún no se obtuvo el texto claro, decidimos primero a aplicar fuerza bruta e ir intercambiando letras hasta que vimos que al principio del criptotexto el texto 'arrakis', de ahi buscamos esa palabra en google y encontramos el texto claro, hicimos los cambios y logramos descifrar el texto.

5.

6. - Para descifrar uno.vigenere usamos un ataque de texto claro conocido, pues como sabemos que el archivo original tiene la extensión .png entonces significa que el primer byte del archivo original era `89`, pues si analizamos cualquier archivo .png como una cadena de bytes, notaremos que los primeros 8 bytes son `89504E47 0D0A1A0A`, entonces como el primer byte en el archivo cifrado es `05`, se tiene que la llave de un byte k debe ser aquella tal que:

$$89 \oplus k = 05$$

si representamos a `89` y `05` en binario tendremos que:

$$10001001 \oplus k = 00000101$$

de ahi es facil ver que $k = 10001100 \equiv$`8c`$\equiv 140$ simplemente viendo bit por bit cual byte vuelve la igualdad cierta. Como la imagen es una larga cadena de bytes nos ayudamos de un pequeño código en python para descifrar el archivo (este se incluye en los documentos adjuntos a la entrega).

Figura 2: Imagen obtenida luego de descifrar uno.vigenere

- Para descifrar ocho.vigenere se usó exactamente lo mismo que en el texto anterior, solo que en este caso nos fijamos en los primero 8 bytes del archivo cifrado, y conociendo los primeros 8 bytes del archivo descifrado se tiene que:

$$\texttt{89} \oplus k_1 = \texttt{f4} \implies 10001001 \oplus k_1 = 11110100 \implies k_1 = 01111101 \equiv \texttt{7d} \equiv 125$$
$$\texttt{50} \oplus k_2 = \texttt{35} \implies k_2 = \texttt{65} \equiv 101$$
$$\texttt{4e} \oplus k_3 = \texttt{72} \implies k_3 = \texttt{3c} \equiv 60$$
$$\texttt{47} \oplus k_4 = \texttt{09} \implies k_4 = \texttt{4e} \equiv 78$$
$$\texttt{0d} \oplus k_5 = \texttt{6e} \implies k_5 = \texttt{63} \equiv 99$$
$$\texttt{0a} \oplus k_6 = \texttt{f0} \implies k_6 = \texttt{fa} \equiv 250$$
$$\texttt{1a} \oplus k_7 = \texttt{1f} \implies k_7 = \texttt{05} \equiv 5$$
$$\texttt{0a} \oplus k_8 = \texttt{0b} \implies k_8 = \texttt{01} \equiv 1$$

Por lo que $k =$`0x7d653c4e63fa0501`. Para descifrar la imagen se usó un programa en python que también se adjunta.

Figura 3: Imagen obtenida luego de descifrar ocho.vigenere