AYUDA TWO-TIME PAD

Supongamos que estos son los mensajes originales (en la práctica 1 los desconocemos pero queremos adivinarlos):

$\boldsymbol{m_0} =$	k	A	i	x	o		l	i	b	e
$\boldsymbol{m_1} =$	a	B		c	d		e	f		g
$\boldsymbol{m_2} =$	h	I	j		k	l	m		n	o

Sabemos que se ha utilizado la misma clave para cifrar los mensajes:

$\boldsymbol{k} =$	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9

Los mensajes cifrados que conocemos son:

$$c_0 = m_0 \oplus k$$

$$c_1 = m_1 \oplus k$$

$$c_2 = m_2 \oplus k$$

Calculando $c_0 \oplus c_1$ podemos conseguir una relación entre m_0 y m_1:

$$c_0 \oplus c_1 = m_0 \oplus m_1$$

$$c_0 \oplus c_2 = m_0 \oplus m_2$$

$$c_1 \oplus c_2 = m_1 \oplus m_2$$

El resultado de realizar el XOR entre un espacio y una letra a-z/A-z es el siguiente:

$'a' \oplus ' ' = 'A' \rightarrow 97 \oplus 32 = 65$	$'A' \oplus ' ' = 'a' \rightarrow 65 \oplus 32 = 97$
$'b' \oplus ' ' = 'B' \rightarrow 98 \oplus 32 = 66$	$'B' \oplus ' ' = 'b' \rightarrow 66 \oplus 32 = 98$
…	…
$'z' \oplus ' ' = 'Z' \rightarrow 122 \oplus 32 = 90$	$'Z' \oplus ' ' = 'z' \rightarrow 90 \oplus 32 = 122$

Entonces, calculando $c_0 \oplus c_1$ conseguimos la siguiente información:

$\boldsymbol{m_0} =$	k	a	i	x	o		L	i	b	e
$\boldsymbol{m_1} =$	a	b		c	d		E	f		g
$\boldsymbol{c_0 \oplus c_1 = m_0 \oplus m_1} =$	?	?	I	?	?	?	?	?	B	?

Si detectamos una letra 97-122 (‘a’-‘z’) o 65-90 (‘A’-‘Z’) significa que m_0 o m_1 tiene un espacio en esa posición.

Podemos realizar el mismo análisis con $c_0 \oplus c_2$ y $c_1 \oplus c_2$:

$\boldsymbol{m_0} =$	k	a	i	x	o		l	i	b	e
$\boldsymbol{m_2} =$	h	i	j		k	l	m		n	o
$\boldsymbol{c_0 \oplus c_2 = m_0 \oplus m_2} =$	?	?	?	X	?	L	?	I	?	?

$\boldsymbol{m_1} =$	a	b		c	d		e	f		g
$\boldsymbol{m_2} =$	h	i	j		k	l	m		n	o
$\boldsymbol{c_0 \oplus c_2 = m_0 \oplus m_2} =$	?	?	J	C	?	L	?	F	N	?

Finalmente, si por ejemplo detectamos los espacios en m_0 podemos calcular la clave en esa posición, teniendo en cuenta que $k = m \oplus c$.

$\boldsymbol{c_0} =$	$c_0[0]$	$c_0[1]$	$c_0[2]$	$c_0[3]$	$c_0[4]$	$c_0[4]$	$c_0[6]$	$c_0[7]$	$c_0[8]$	$c_0[9]$
$\boldsymbol{m_0} =$						32				
$\boldsymbol{key} =$						$c_0[4] \oplus 32$				

Podemos repetir el mismo proceso con m_1 y m_2:

$\boldsymbol{c_1} =$	$c_1[0]$	$c_1[1]$	$c_1[2]$	$c_1[3]$	$c_1[4]$	$c_1[4]$	$c_1[6]$	$c_1[7]$	$c_1[8]$	$c_1[9]$
$\boldsymbol{m_1} =$			32			32			32	
$\boldsymbol{key} =$			$c_1[2] \oplus 32$			$c_0[4] \oplus 32$			$c_1[8] \oplus 32$	

$\boldsymbol{c_2} =$	$c_2[0]$	$c_2[1]$	$c_2[2]$	$c_2[3]$	$c_2[4]$	$c_2[4]$	$c_2[6]$	$c_2[7]$	$c_2[8]$	$c_2[9]$
$\boldsymbol{m_2} =$				32				32		
$\boldsymbol{key} =$			$c_1[2] \oplus 32$	$c_2[3] \oplus 32$		$c_0[4] \oplus 32$		$c_2[7] \oplus 32$	$c_1[8] \oplus 32$	

Hemos conseguido adivinar parte de la clave comparando 3 mensajes, si tenemos acceso a más mensajes podremos conseguir más información de la clave.

Una vez que adivinamos la clave, podemos calcular el *plaintext* $m = k \oplus c$.