1. Práctica: Many Time Pad

1 Objetivo

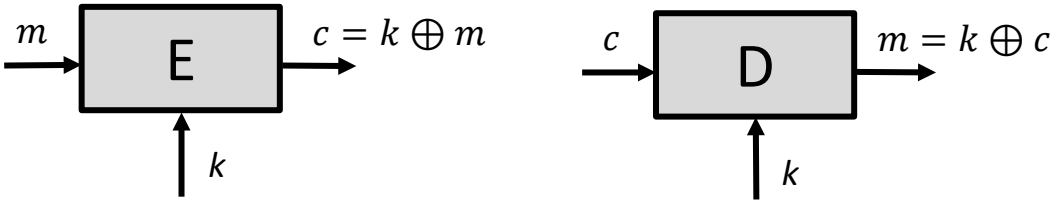
Has interceptado 14 mensajes encriptados utilizando el *stream cipher one-time-pad*. Sospechas que se ha utilizado la misma clave para cifrar todos los mensajes, y sabéis que la estrategia *two-time pad* es incorrecta. **Por ello, vas a intentar adivinar la clave y descifrar los 14 mensajes originales.**

Ten en cuenta que los siguientes 14 mensajes están representados con **notación hexadecimal**.

c0	1a1617451a411517490b061b0f08535404044e17450c1c45326222420a00340006544816170b54030b55020d530046
c1	184f184f0a081a000016071a00010017090b00100416010054530e060c52301b0c000a131304430e0a0640
c2	09001a5248041b04490a4f060b07550601115953150c010007000604134f2b4f01481a0417115348
c3	7926114506151f1159461b1d0b025454010850120617014542104b08104c35061a4e48201b00520f0c1400170e
c4	0c3c5547071713174e0b0a1b1a445018090b5353110c52160445050159046 85a5542010d1a0c4f084f1a0044430d0a005200000007171d54124b
c5	1a001c4e480c1f0b490808551e1645070d0b5400450252071d474b020b4f2e1b1d00010f560659040a070d1649190d4b
c6	0d0710003d32560c5346211a4e55000009174716114314 0a06001f040b473c1b1044480002114105040640
c7	1c02054c0718130000080a12020d47110606455306021c45174f06150b4f34060645480f131157091d1e4e1745171d1749071c4d
c8	103b55530d02031749121655070a5411040949140 00d1100544918450c4e3d0a07551c081a0c5a030b5b
c9	120a1050010f1145410a03551d0b46001f0452164516020115540e0159492a4f14441e0805004448
c10	793b024f48151f0845461f140a444907480b4f074510170601520e4959552a0a5541480f1312000d0a0c4e0141170045541a08065c
c11	163b55530d020317491216551e1645070d0b54004502520b11574b161c54790013000b0917094c0301120b170e
c12	100021000c04000c43031c550d054e54010b4301000201005 4530e060c52301b0c001e141a0b45140e17070849000100535d
c13	793b1d451a04560c53460e550d1d42111a4553160616000c00594b161249350306001b0919175407081040

2 One time pad

One time pad consiste en cifrar y descifrar mensajes utilizando la operación lógica XOR.



¿Por qué es peligroso utilizar la misma clave para cifrar múltiples mensajes?

Supongamos que ciframos dos mensajes utilizando la misma clave.

$$c0 = k \oplus m0$$

$$c1 = k \oplus m1$$

Si combinamos los dos mensajes cifrados podemos obtener información sobre los mensajes originales $m0$ y $m1$.

$$c0 \oplus c1 = m0 \oplus k \oplus m1 \oplus k$$
$$c0 \oplus c1 = m0 \oplus m1 \oplus k \oplus k$$
$$c0 \oplus c1 = m0 \oplus m1$$

Si tenemos más de dos mensajes, podemos obtener más información combinándolos.

¿Y cómo podemos utilizar esta información para descifrar los mensajes interceptados?

Pista: piensa que ocurre al realizar la operación XOR entre [a-z] o [A-Z] y el espacio (“ “ = 0x20).