4.1)

a) tenemos que, al usar AES 128, como cada byte son 8 bits, podremos usar $\frac{128}{8} = 16$ bytes.

Como en cada byte tenemos 27 posibilidades, tendremos $27^{16} = 7,9766 \cdot 10^{22}$ posibilidades.

Como tenemos que probar la mitad tendremos $3,9883 \cdot 10^{22}$ posibilidades

Como la capacidad de cómputo es 10^{-6} s → $3,9883 \cdot 10^{22} \cdot 10^{-6} = 3,9883 \cdot 10^{16}$

b)

posibilidades $= 54^{16}$

tiempo $= \frac{54^{16}}{2} \cdot 10^{-6} = 2,6138 \cdot 10^{21}$ s $= 7,2605 \cdot 10^{17}$

c) posibilidades $(54 + 10) = 64^{16}$

tiempo: $\frac{64^{16}}{2} \cdot 10^{-6} = 3,9614 \cdot 10^{22}$ s $= 1,1003 \cdot 10^{19}$ h

4.2)

Su objetivo principal es el de convertir la clave de usuario en un conjunto de subclaves que pueden estar constituidas por varias cientas de bits en total.

4.3.)

AES adopta el algoritmo Rijndael, el cual es un sistema de Cifrado por bloques cuya clave y cuyos bloques pueden ser de longitud variable.

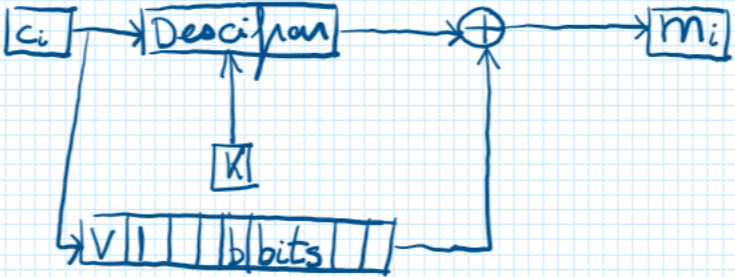
Para AES, se fijó un tamaño de bloque de 128 bits y tres tamaños de clave diferente:

- 128 bits → AES 128
- 192 bits → AES 192
- 256 bits → AES 256

También se definen varias modas. Uno de ellas es el CBC, que para descifrar, cada bloque C_i de b bits del criptograma se descifra con la misma clave K y alimenta el registro de b bits que se suma módulo 2 con la salida $D(C_i)$

Para descifrar se aplican las siguientes ecuaciones:

$m_1 = D_K(C_1) \oplus V1$; $m_i = D_K(C_i) \oplus C_{i-1}$ para $i = 2, 3, \ldots, n$



4.4)

C2	CB	C9	50
02	F4	69	89
64	26	6E	63
FB	27	23	9A

4.5) Cifradores en flujo

- Operan sobre los bits individuales.
- Son más rápidos y usan menos memoria que los cifradores en bloque
- Son útiles cuando la cantidad de datos es desconocida
- Ejemplos: ChaCha20 (TLS y SSL) RC4 → no se recomienda su uso debido a la gran cantidad de vulnerabilidades que se conocen

Cifradores en bloque

- Cifran los datos en bloques de un tamaño fijo.
- Son más seguros que los cifradores en flujo, pero también son más lentos y usan más memoria.
- Son ideales para el cifrado de datos almacenados, como archivos y bases de datos.
- Ejemplo: AES (para WPA2) y DES

4.6)

a) El alfabeto en castellano, tiene 27 caracteres. Como solo vamos a usar 7 caracteres, tendremos 27^7 combinaciones. Por ello el tiempo en horas será: $t = \frac{27^7}{2} \cdot \frac{10^{-6}}{3600} = 1,4528\,h$

b) Ahora tendremos 54 caracteres

↳ $t = \frac{54^7}{2} \cdot \frac{10^{-6}}{3600} = 185,96\,h$

c) Finalmente, tendremos 64 caracteres

↳ $t = \frac{64^7}{2} \cdot \frac{10^{-6}}{3600} = 610,84\,h$