


## Criterios de evaluación y condiciones de entrega

- Para cualquier duda y/o aclaración sobre el enunciado tenéis que dirigiros al consultor responsable de vuestra aula.
- Se tiene que entregar la solución en un archivo, preferiblemente, en formato PDF .
- El nombre del archivo tiene que ser **ApellidoNombre\_asignatura\_PEC2** con extensión **.pdf**
- Razonad la respuesta en todos los ejercicios e indicad todos los pasos que habéis realizado para obtener la solución.
- Las respuestas sin justificación, que sean una copia de una fuente de información y/o que no contengan las referencias utilizadas, no recibirán ninguna puntuación.
- La fecha límite de entrega será el día **26 de noviembre del 2019** antes de las **23:59h**. La entrega se realizará a través del REC (*Registro de Evaluación Continuada*).

## Enunciado

### Ejercicio 1 (3 puntos)

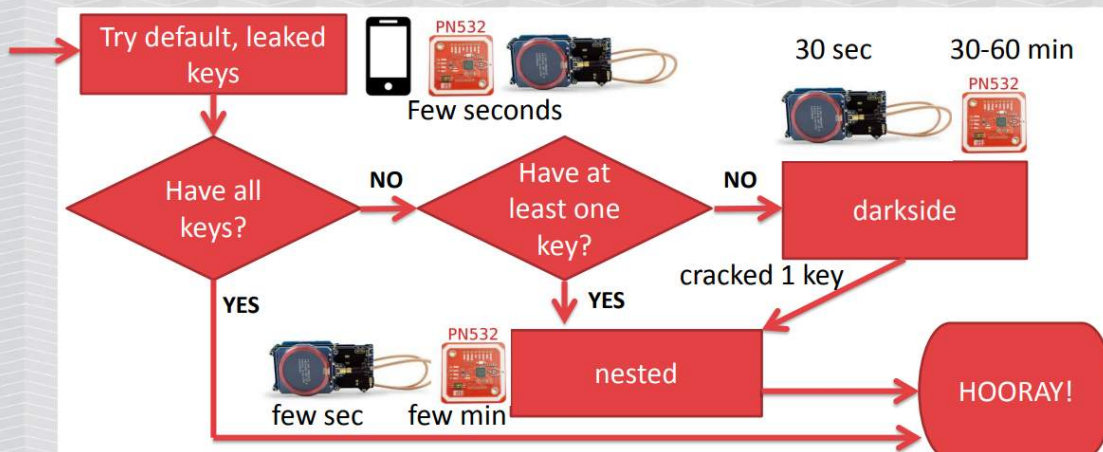
Las MIFARE Classic 1K son unas tarjetas NFC ampliamente utilizadas en la actualidad para usos como puede ser control de acceso físico o, incluso en sistemas de pago (e.g. máquinas de *vending*). A pesar de su popularidad, dichas tarjetas presentan ciertas vulnerabilidades. Busca información sobre dichas tarjetas y responde a las siguientes cuestiones:

- Describe su estructura interna a nivel de bloques y sectores
- Describe cómo estas tarjetas protegen la información a nivel de claves
- En qué consisten los *Access Bits* y cuál es su uso?
- Qué es el UID y cómo puede usarse como mecanismo de control de acceso físico?
- Se te ocurre un sistema más robusto que el basado en el UID pero empleando una clave de un sector? Describe una propuesta basada en esta idea.

### Ejercicio 2 (3 puntos)

La siguiente imagen describe un flujo para poder romper las claves de cifrado asociado a las tarjetas MIFARE Classic 1K, lo que permite su posterior clonado. En concreto en dicho *workflow* se identifican tres posibles ataques 1) *Claves por defecto*, 2) *Nested*, y 3) *Darkside*. Busca información relacionada con estos ataques y responde las siguientes cuestiones:

## Mifare Classic cracking process



- Describe brevemente en qué consiste el ataque de *Claves por defecto*.
- Describe brevemente en qué consiste el ataque *Nested*.
- Describe brevemente en qué consiste el ataque *Darkside*.
- Teniendo en cuenta cada uno de los ataques anteriores, describe la lógica del *workflow* de la imagen anterior.

### Ejercicio 3 (4 puntos)

Este último ejercicio consiste en un cuestionario *online* que tenéis que responder. Este cuestionario hace referencia a los módulos 3 y 4 de la asignatura. Para acceder al cuestionario tenéis que ir al enlace “Cuestionarios” del aula y entrar en el correspondiente a la PEC 2. Es importante que tengáis en cuenta:

- Es muy recomendable que hayáis repasado los módulos antes de iniciar el test.
- Tenéis dos intentos para hacer el test. La nota final será la nota más alta de los dos intentos.
- La duración del test es de un máximo de 30 minutos por cada intento.
- El test se puede realizar hasta la fecha de entrega de la PEC 2.