



Desarrollo aplicaciones con tarjetas inteligentes

Curso 2023-2024



CEU

| *Universidad
San Pablo*

INDICE DEL CURSO (Sesión #1/5)

PRESENTACION Y OBJETIVOS

TEMAS

- Tipos de tarjetas inteligentes
- Propósito de las tarjetas inteligentes (poca información//muchas seguridad)
- Fundamentos & ISO 7816
- Tipos de algoritmos (simétricos//asimétricos)
- Especificaciones del chip
- Historia de la criptografía

PRÁCTICAS

- Listado de tarjetas conocidas, uso y características técnicas.
- Comparativa de Chips (con PC y Arduino)
- Análisis de necesidades técnicas de una tarjeta que usemos en el día a día
- Diseñar un sistema basado en tarjeta
- Instalar el compilador.

TIPOS DE TARJETAS INTELIGENTES

Por funcionalidad:

- SIM gsm
- eDNI
- Bancarias
- Abono transporte
- Pasaporte
- Tarjeta estudiante
- Monedero vending
- Fidelidad
- Acceso

Por interface de comunicación:

- Contacto
- Contactless

Por capacidad criptográfica

- Código secreto // 'criptografía'
- TripleDES

- RSA

Por tamaño de memoria y Organización

- Memoria flash // almacenamiento de información
- Basada en ficheros
- Organizada con TLV

Por precio

- El precio lo define las características y el volumen.

Otras formas

- Pulseras, injertos...

INDICE DEL CURSO (Sesión #2/5)

TEMAS

- Fundamentos & ISO 7816
- Especificaciones del chip
- Tipos de algoritmos (simétricos//asimétricos)
- Historia de la criptografía

PRÁCTICAS

- Comparativa de Chips (con PC y Arduino)
- Diseñar un sistema basado en tarjeta
- Instalar el compilador.

Pregunta segunda sesión...

¿Cuál es la respuesta correcta?

- A. La memoria EEPROM//FLASH guarda la información de manera persistente y por ello compromete la seguridad.**
- B. Los pines se deben guardar en memoria RAM, para que no nos roben su valor lo hackers.**
- C. Las tarjetas chip con criptoprocador no tienen CPU.**
- D. Todas las anteriores son falsas.**

Evolución: una carrera hacia la seguridad



Smartcard basic

INDICE DEL CURSO (Sesión #3/5)

TEMAS

- Historia de la criptografía
- Propiedades fundamentales de la criptografía

PRÁCTICAS

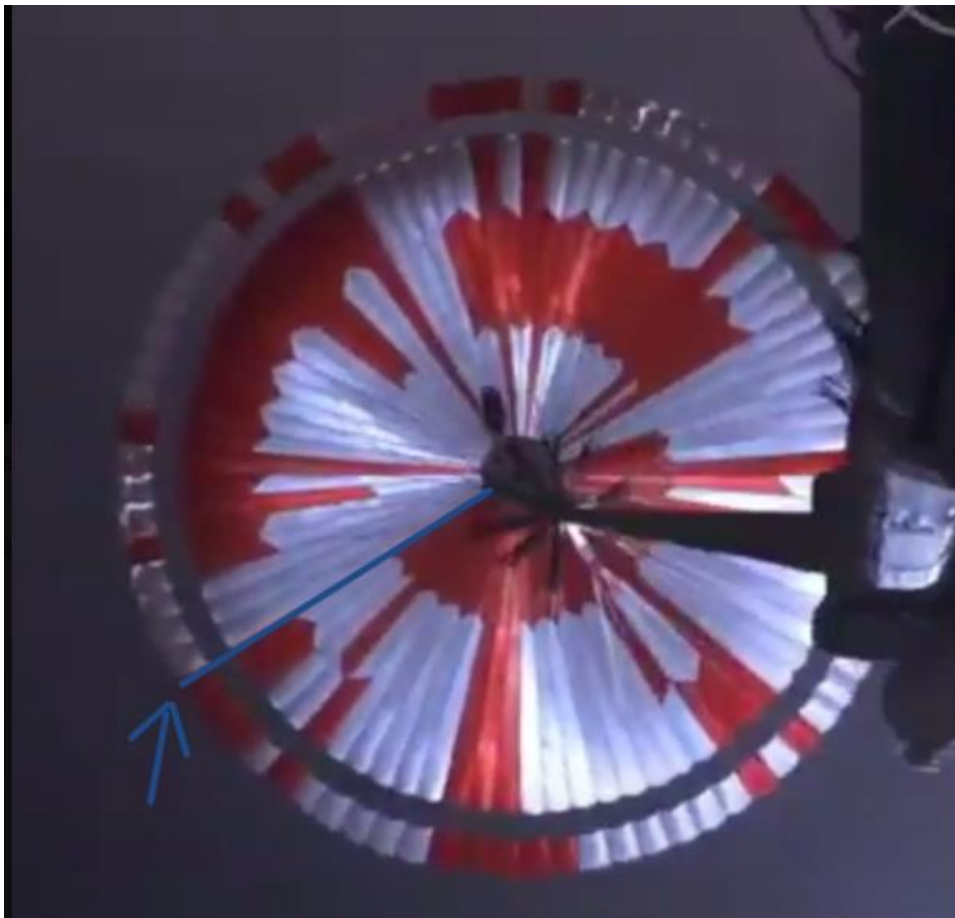
- Ejecutar 'holaMundo' en javaCard.
- Adu que descifre una criptografía sencilla o una codificación Morse

Historia de la criptografía

- **Diferencia entre codificación y criptografía (sist. decimal, hexadecimal, binario, ascii, morse, BCD...)**
- **Criptografía y la necesidad de comunicaciones secretas. La industria de la guerra**
- **Cifrado CESAR**
- **Problemas de la clave secreta, su intercambio y su vulnerabilidad**
- **Cifrado Vigenere**
- **Cifrados matemáticos, máquina Enigma en la II guerra mundial.**
- **Criptografía en la era digital: DES, RSA**
- **Criptomonedas**

- **ATAQUES A LOS SISTEMAS CRIPTOGRÁFICOS!!!**

Sistemas de Codificación basados en posición en el alfabeto y sistema binario





```

vim pattern
1 We identified a 10 bit pattern in the circles.
2 There are 4 groups, each one is built from a circle, starting from the center circle.
3
4 We ignore the big groups of 1's since they do not mean anything here.
5 Each binary number encodes a position in the alphabet, starting at 1.
6 For the word "mighty", we just have to start counting 40 bits later and it would be correct.
7 To help with understanding, we count everything from the same row as indicated in the picture,
8 and we work clockwise.
9
10 0000000100 4      D
11 0000000001 1      A
12 0000010010 18     R
13 0000000101 5      E
14 0001111111
15 1111111111
16 1111111111
17 1111111111
18
19
20 0000010100 20     T
21 0000011001 25     Y
22 0001111111
23 1111111111
24 0000001101 13     M
25 0000001001 9      I
26 0000000111 7      G
27 0000001000 8      H
28
29 0001111111
30 1111111111
31 0000010100 20     T
32 0000001000 8      H
33 0000001001 9      I
34 0000001110 14     N
35 0000000111 7      G
36 0000010011 19     S
37
38 0000100010 34
39 0000001011 11
40 0000111010 58
41 0000001110 14
42 0001110110 118
43 0000001010 10
44 0000011111 31

```

PROPIEDADES DE LOS SISTEMAS CRIPTOGRAFICOS

- **AUTENTICACION**
- **IDENTIFICACION**
- **INTEGRIDAD**
- **NO REPUDIO**
- **PRIVACIDAD**

Smartcard basic

Pregunta primera sesión...

Para un proyecto de tarjeta de abono en transporte urbano, cuál de las afirmaciones es cierta:


- A. Elijo la tarjeta más potente en cuanto a criptografía para asegurar que no se sube nadie gratis, tengo en cuenta que el valor de los autobuses es elevado.**
- B. Elijo una tarjeta de poca memoria porque guardo poca información sensible**
- C. Elijo la tarjeta más baratita porque tengo que comprar millones de unidades y la seguridad no es importante en un servicio público**
- D. Todas las anteriores son falsas**


Prueba del tercer día:






Clave: Quijote_12_a


Ej: RCDNQ => PABLO

¿FKWUHTOK?

BIBLIOTECA VIRTUAL
MIGUEL DE CERVANTES
www.cervantesvirtual.com

Búsqueda por título, autor o contenido 

 Portales  Ver más  Subir  Índice  Ficha

Analizar versos 

Capítulo I

Que trata de la condición y ejercicio del famoso hidalgo don Quijote de la Mancha

En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocín flaco y galgo corredor. Una olla de algo más vaca que carnero, salpicón las más noches, duelos y quebrantos los sábados, lantejas los viernes, algún palomino de añadidura los domingos, consumían las tres partes de su hacienda. El resto della concluían sayo de velarte, calzas de velludo para las fiestas, con sus pantuflos de lo mismo, y los días de entresemana se honraba con su vellori de lo más fino. Tenía en su casa una ama que pasaba de los cuarenta, y una sobrina que no llegaba a los veinte, y un mozo de campo y plaza, que así ensillaba el rocín como tomaba la podadera. Frisaba la edad de nuestro hidalgo con los cincuenta años; era de complexión recia, seco de carnes, enjuto de rostro, gran madrugador y amigo de la caza. Quieren decir que tenía el sobrenombre de Quijada, o Quesada, que en esto hay alguna diferencia en los autores que deste caso escriben; aunque por conjeturas verosímiles se deja entender que se llamaba Quijana. Pero esto importa poco a nuestro cuento: basta que en la narración dél no se salga un punto de la verdad.



DOCUMENTACIÓN ÚTIL

Documentación útil

ISO:

<https://cardwerk.com/iso-7816-smart-card-standard/>

Global Platform: <https://globalplatform.org/specs-library/>

Packages documentación: <https://docs.oracle.com/javacard/3.0.5/api/overview-tree.html>

Memoria: https://is.muni.cz/th/fzcjr/Ashwin_Report.pdf

Intro: <https://www.oracle.com/technetwork/java/javacard/javacard1-139251.html>

Tools: <https://www.javacardos.com/tools>

Ataques: <https://firefart.at/post/how-to-crack-mifare-classic-cards/>

C:\JavaCardKit\SDK\Sample\wallet

PROYECTOS CEU GTI

Memoria del proyecto

- **Propósito de la aplicación**
- **Definición de personas**
- **Historias de usuario**
- **Requisitos de seguridad, definir las 5 propiedades**

INDICE DEL CURSO (Sesión #4/5)

TEMAS

- Programación en Javacard

PRÁCTICAS

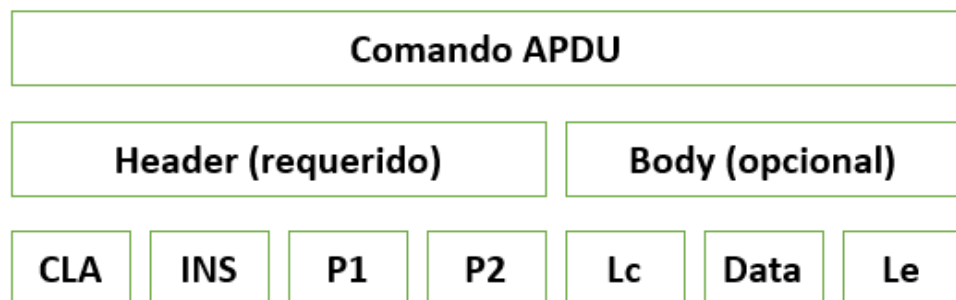
- Ejecutar 'holaMundo' en javaCard.
- Mi primer applet: Apdu que descifre una criptografía sencilla o una codificación Morse

- Cambiar las claves a la tarjeta de test por las genéricas ***XHST_Update KMC to No Diversification Mode Introduction_V1.0.pdf***
- Cargar el CAP file ***APDU SHELL(debugtool)_Load CAP User Manual V1.0.pdf***
- Instalar el applet ***walletDemoApplet***
- Select
 - Send: 00 A4 04 00 06 11 22 33 44 55 66
 - Recv: 90 00
- Read balance
 - Send: 80 50 00 00
 - Recv: 00 00 90 00

APDU

La estructura de un APDU está definida en los estándares ISO/IEC 7816.

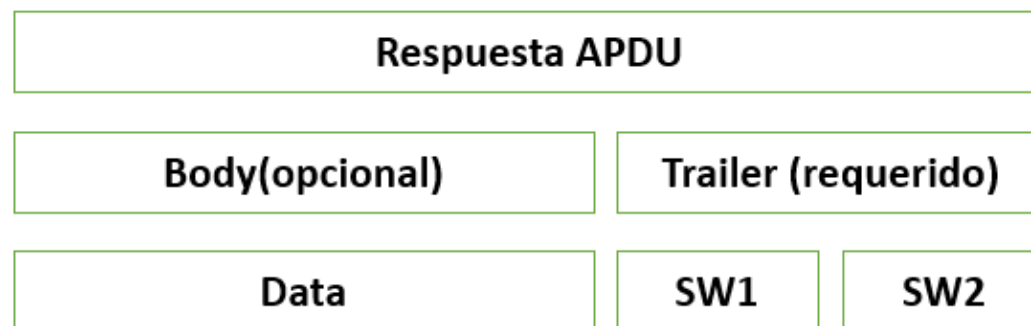
Estructura de un comando APDU



La trama APDU de tipo comando consta de los siguientes campos:

- **CLA** : Byte de clase
- **INS** : Byte de instrucción
- **P1,P2**: Parámetros
- **Lc** : tamaño del bloque de datos
- **Data**
- **Le** : Tamaño de la respuesta esperada

Estructura de una respuesta APDU



La trama APDU respuesta consta de los campos:

- **Data**
- **SW1, SW2**: Palabra de estado, dónde se codifica el estado de la operación (correcta, error criptográfico obligatorio).

Status SW1 SW2

#	SW1 SW2	Message
	'6X XX'	Transmission protocol related codes
	'61 XX'	SW2 indicates the number of response bytes still available
	'62 00'	No information given
	'62 81'	Returned data may be corrupted
	'62 82'	The end of the file has been reached before the end of reading
	'62 83'	Invalid DF
	'62 84'	Selected file is not valid. File descriptor error
	'63 00'	Authentication failed. Invalid secret code or forbidden value
	'63 81'	File filled up by the last write
	'63 CX'	Counter provided by 'X' (valued from 0 to 15) (exact meaning depending on the command)
	'65 01'	Memory failure. There have been problems in writing or reading the EEPROM.
	'65 81'	Write problem / Memory failure / Unknown mode
	'67 XX'	Error, incorrect parameter P3 (ISO code)
	'67 00'	Incorrect length or address range error
	'68 00'	The request function is not supported by the card.
	'68 81'	Logical channel not supported
	'68 82'	Secure messaging not supported
	'69 00'	No successful transaction executed during session
	'69 81'	Cannot select indicated file, command not compatible with file organization
	'69 82'	Access conditions not fulfilled
	'69 83'	Secret code locked
	'69 84'	Referenced data invalidated
	'69 85'	No currently selected EF, no command to monitor / no Transaction Manager File
	'69 86'	Command not allowed (no current EF)
	'69 87'	Expected SM data objects missing
	'69 88'	SM data objects incorrect
	'6A 00'	Bytes P1 and/or P2 are incorrect.
	'6A 80'	The parameters in the data field are incorrect
	'6A 81'	Card is blocked or command not supported
	'6A 82'	File not found
	'6A 83'	Record not found
	'6A 84'	There is insufficient memory space in record or file
	'6A 85'	Lc inconsistent with TLV structure
	'6A 86'	Incorrect parameters P1-P2
	'6A 87'	The P3 value is not consistent with the P1 and P2 values.
	'6A 88'	Referenced data not found.

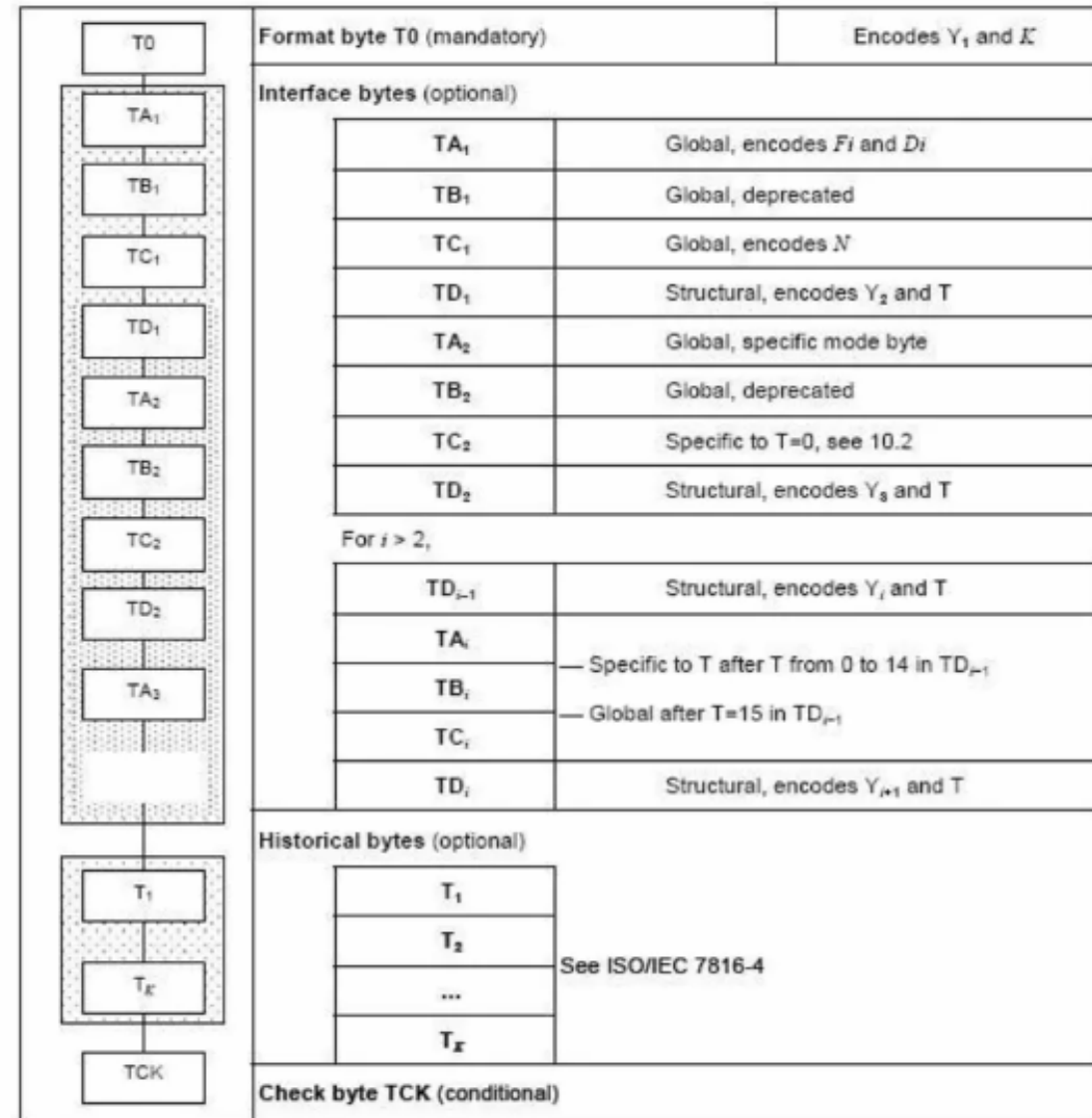
[link](#)

ATR

Es un mensaje emitido por una tarjeta inteligente de contacto que cumple con los estándares ISO / IEC 7816, luego del reinicio eléctrico del chip de la tarjeta por un lector de tarjetas. El ATR transmite información sobre los parámetros de comunicación propuestos por la tarjeta, y la naturaleza y el estado de la misma.

Para ver mas

<https://smartcard-atr.appspot.com/>



EMV PARA PRACTICAR EN CASA

Lista de principales AID basadas en el estándar EMV

<https://es.wikipedia.org/wiki/EMV>

A00000077018383081000F1000000100

3F00

1001

0101

0102

Card scheme	RID	Product	PIX	AID
Visa	A000000003	Visa credit or debit	1010	A0000000031010
		Visa Electron	2010	A0000000032010
		V PAY	2020	A0000000032020
		Plus	8010	A0000000038010
MasterCard	A000000004	MasterCard credit or debit	1010	A0000000041010
		MasterCard ²	9999	A0000000049999
		Maestro (debit card)	3060	A0000000043060
		Cirrus (interbank network) ATM card only	6000	A0000000046000
MasterCard	A000000005	Maestro UK (formerly branded as Switch)	0001	A0000000050001
American Express	A000000025	American Express	01	A00000002501
LINK (UK) ATM network	A000000029	ATM card	1010	A0000000291010
CB (France)	A000000042	CB (Credit or Debit card)	1010	A0000000421010
		CB (Debit card only)	2010	A0000000422010
JCB	A000000065	Japan Credit Bureau	1010	A0000000651010
Dankort (Denmark)	A000000121	Debit card	1010	A0000001211010
CoGeBan (Italy)	A000000141	PagoBANCOMAT	0001	A0000001410001
Diners Club/Discover	A000000152	Diners Club/Discover	3010	A0000001523010
Banrisul (Brazil)	A000000154	Banricompras Debito	4442	A0000001544442
SPAN2 (Saudi Arabia)	A000000228	SPAN	1010	A00000022820101010
Interac (Canada)	A000000277	Debit card	1010	A0000002771010
Discover	A000000324	ZIP	1010	A0000003241010
UnionPay	A000000333	Debit	010101	A000000333010101
		Credit	010102	A000000333010102
		Quasi Credit	010103	A000000333010103
		Electronic Cash	010106	A000000333010106
ZKA (Germany)	A000000359	Girocard	1010028001	A0000003591010028001
EAPS BANCOMAT (Italy)	A000000359	PagoBANCOMAT	10100380	A00000035910100380
Verve (Nigeria)	A000000371	Verve	0001	A0000003710001
The Exchange Network ATM Network	A000000439	ATM card	1010	A0000004391010
RuPay (India)	A000000524	RuPay	1010	A0000005241010

Estudiando el código javacard

```
8      */
9
10     package com.sun.javacard.samples.wallet;
11     import javacard.framework.*;
12
13     ▽public class Wallet extends Applet {
14
15         /* constants declaration */
16
17         // code of CLA byte in the command APDU header
18         final static byte Wallet_CLA = (byte) 0x80;
19
20         // codes of INS byte in the command APDU header
21         final static byte VERIFY = (byte) 0x20;
22         final static byte CREDIT = (byte) 0x30;
23         final static byte DEBIT = (byte) 0x40;
24         final static byte GET_BALANCE = (byte) 0x50;
25
26         // maximum balance
27         final static short MAX_BALANCE = 0x7FFF;
28         // maximum transaction amount
29         final static byte MAX_TRANSACTION_AMOUNT = 127;
30     }
```

```

public void process(APDU apdu) {

    // APDU object carries a byte array (buffer) to
    // transfer incoming and outgoing APDU header
    // and data bytes between card and CAD

    // At this point, only the first header bytes
    // [CLA, INS, P1, P2, P3] are available in
    // the APDU buffer.
    // The interface javacard.framework.ISO7816
    // declares constants to denote the offset of
    // these bytes in the APDU buffer

    byte[] buffer = apdu.getBuffer();
    // check SELECT APDU command

    /*if (apdu.isISOInterindustryCLA()) {
        if (buffer[ISO7816.OFFSET_INS] == (byte) (0xA4)) {
            return;
        } else {
            ISOException.throwIt (ISO7816.SW_CLA_NOT_SUPPORTED);
        }
    }
    */

    // verify the reset of commands have the
    // correct CLA byte, which specifies the
    // command structure
    if (buffer[ISO7816.OFFSET_CLA] != Wallet_CLA)
        ISOException.throwIt (ISO7816.SW_CLA_NOT_SUPPORTED);

    switch (buffer[ISO7816.OFFSET_INS]) {
    case GET_BALANCE:
        getBalance(apdu);
        return;
    case DEBIT:
        debit(apdu);
        return;
    case CREDIT:
        credit(apdu);
        return;
    case VERIFY:
        verify(apdu);
        return;
    default:
        ISOException.throwIt (ISO7816.SW_INS_NOT_SUPPORTED);
    }

    // end of process method
}

```

```

private void debit(APDU apdu) {

    // access authentication
    if ( ! pin.isValidated() )
        ISOException.throwIt(SW_PIN_VERIFICATION_REQUIRED);

    byte[] buffer = apdu.getBuffer();

    byte numBytes =
        (byte) (buffer[ISO7816.OFFSET_LC]);

    byte byteRead =
        (byte) (apdu.setIncomingAndReceive());

    if ( ( numBytes != 1 ) || (byteRead != 1) )
        ISOException.throwIt(ISO7816.SW_WRONG_LENGTH);

    // get debit amount
    byte debitAmount = buffer[ISO7816.OFFSET_CDATA];

    // check debit amount
    if ( ( debitAmount > MAX_TRANSACTION_AMOUNT)
        || ( debitAmount < 0 ) )
        ISOException.throwIt(SW_INVALID_TRANSACTION_AMOUNT);

    // check the new balance
    if ( (short) ( balance - debitAmount ) < (short) 0 )
        ISOException.throwIt(SW_NEGATIVE_BALANCE);

    balance = (short) (balance - debitAmount);

} // end of debit method

```

```
>> /select 112233332211
>> 00 A4 04 00 06 11 22 33 33 22 11 00
<< 90 00

>> /send 80BA000002
>> 80 BA 00 00 02
<< 0E 64 90 00
```

Factory Key

496E74615F546573745F4B4D435F3031

New

404142434445464748494A4B4C4D4E4F

Table 38 — SELECT command-response pair

CLA	As defined in 5.1.1
INS	'A4'
P1	See Table 39
P2	See Table 40
L _e field	Absent for encoding N _e = 0, present for encoding N _e > 0
Data field	Absent or file identifier or path or DF name (according to P1)
L _e field	Absent for encoding N _e = 0, present for encoding N _e > 0
Data field	Absent or file control information (according to P2)
SW1-SW2	See Tables 5 and 6 when relevant, e.g., '6283', '6284', '6A80', '6A81', '6A82', '6A86', '6A87'

Table 39 — P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning	Command data field
0	0	0	0	0	0	x	x	Selection by file identifier	
0	0	0	0	0	0	0	0	Select MF, DF or EF	File identifier or absent
0	0	0	0	0	0	0	1	Select child DF	DF identifier
0	0	0	0	0	0	1	0	Select EF under the current DF	EF identifier
0	0	0	0	0	0	1	1	Select parent DF of the current DF	Absent
0	0	0	0	0	1	x	x	Selection by DF name	
0	0	0	0	0	1	0	0	Select by DF name	e.g., [truncated] application identifier
0	0	0	0	1	0	x	x	Selection by path	
0	0	0	0	1	0	0	0	Select from the MF	Path without the MF identifier
0	0	0	0	1	0	0	1	Select from the current DF	Path without the current DF identifier
— Any other value is reserved for future use by ISO/IEC JTC 1/SC 17.									
— When present in the historical bytes (see 8.1.1) or in EF.ATR (see 8.2.1.1), the first software function table (see Table 86) indicates selection methods supported by the card.									

Table 40 — P2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	-	-	x	x	File occurrence
0	0	0	0	-	-	0	0	— First or only occurrence
0	0	0	0	-	-	0	1	— Last occurrence
0	0	0	0	-	-	1	0	— Next occurrence
0	0	0	0	-	-	1	1	— Previous occurrence
0	0	0	0	x	x	-	-	File control information (see 5.3.3 and Table 11)
0	0	0	0	0	0	-	-	— Return FCI template, optional use of FCI tag and length
0	0	0	0	0	1	-	-	— Return FCP template, mandatory use of FCP tag and length
0	0	0	0	1	0	-	-	— Return FMD template, mandatory use of FMD tag and length
0	0	0	0	1	1	-	-	— No response data if L _e field absent, or proprietary if L _e field present
— Any other value is reserved for future use by ISO/IEC JTC 1/SC 17.								

<https://centroderecursos.agesic.gub.uy/web/seguridad/wiki/-/wiki/Main/Gu%C3%ADa+de+uso+de+CI+electr%C3%B3nica+a+trav%C3%A9s+de+APDU>

Pregunta cuarta sesión...

¿Cuál es la respuesta correcta?

- A. El método 'process' en un programa de tarjetas javacard, es la función primera y principal.**
- B. Es mejor programar las funciones de seguridad para estar seguros que todo está bien hecho.**
- C. Puedo identificar al dueño de la tarjeta con el ATR.**
- D. El 'Response' a un comando APDU me dice si una tarjeta es auténtica o no.**

Pregunta quinta sesión...

¿Cuál es la respuesta correcta?

- A. La norma ISO7816 estandariza el mundo de la tarjeta inteligente**
- B. Los APDUS son comandos que siguen el protocolo pregunta respuesta para comunicarnos con la tarjeta.**
- C. El ATR es la primera respuesta de la tarjeta al alimentar el chip o resetearlo.**
- D. Todas son correctas.**

Prácticas intermedias

Sesión#1

- Listado tarjetas que usáis a diario
- Analizar una tarjeta de las conocidas conforme a su tipología

Sesión#2

- Comparar chip features arquitectura entre SmartCard y un PC y un Arduino
- Diseñar un sistema basado en tarjeta

Sesión#3

- Instalar el compilador

Sesión#4

- Programa hola mundo en emulador y tarjeta
- miprimerPrograma, APDU descodifique



Jose Javier Jiménez Vitón

Director de Innovación

T. 669409368

E. jjjimenez@diusframi.es



C/ Rufino González, 32 28037 Madrid

www.diusframi.es

