

**EE4215 Security Technology
Assignment 4 (Total 65 marks)**

Name: _____
Student ID: _____

Date: _____
Mark: _____

Due date: April 29, 2019 (Monday) – mid-night
Electronic submission only on Canvas

Use the contactless smart card system Mifare provided by the Digital Systems Laboratory (P1800) and the software interface manual and the Mifare program EE4215-assignment4-ACR_Reader.exe and Mifare card supplied. Run the program and fill in the answer below:

- a) Write down the reader Model no. _____
- b) Reference No. of Reader : _____ Card No: _____
- c) Press the Initialize button, a screen is display as below:

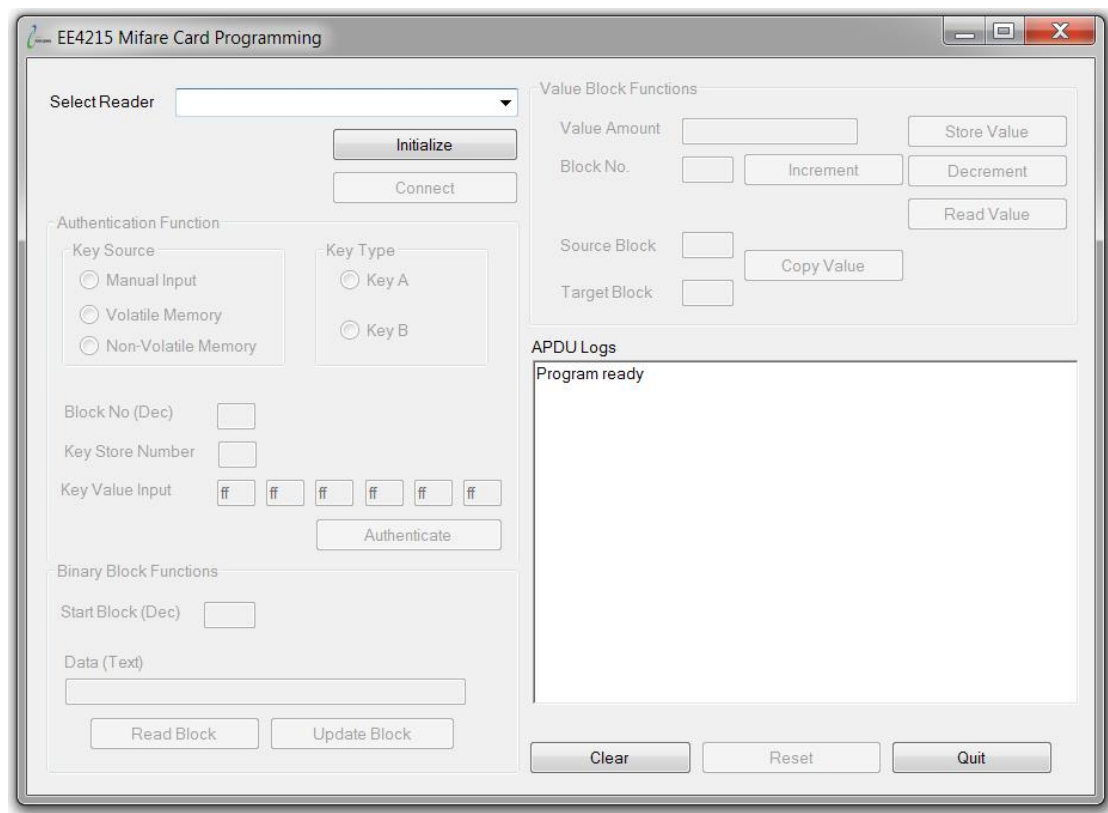


Figure 1: EE4215 Mifare Card Programming

d) Place the card on the reader and select the “Connect” button to connect the card reader.

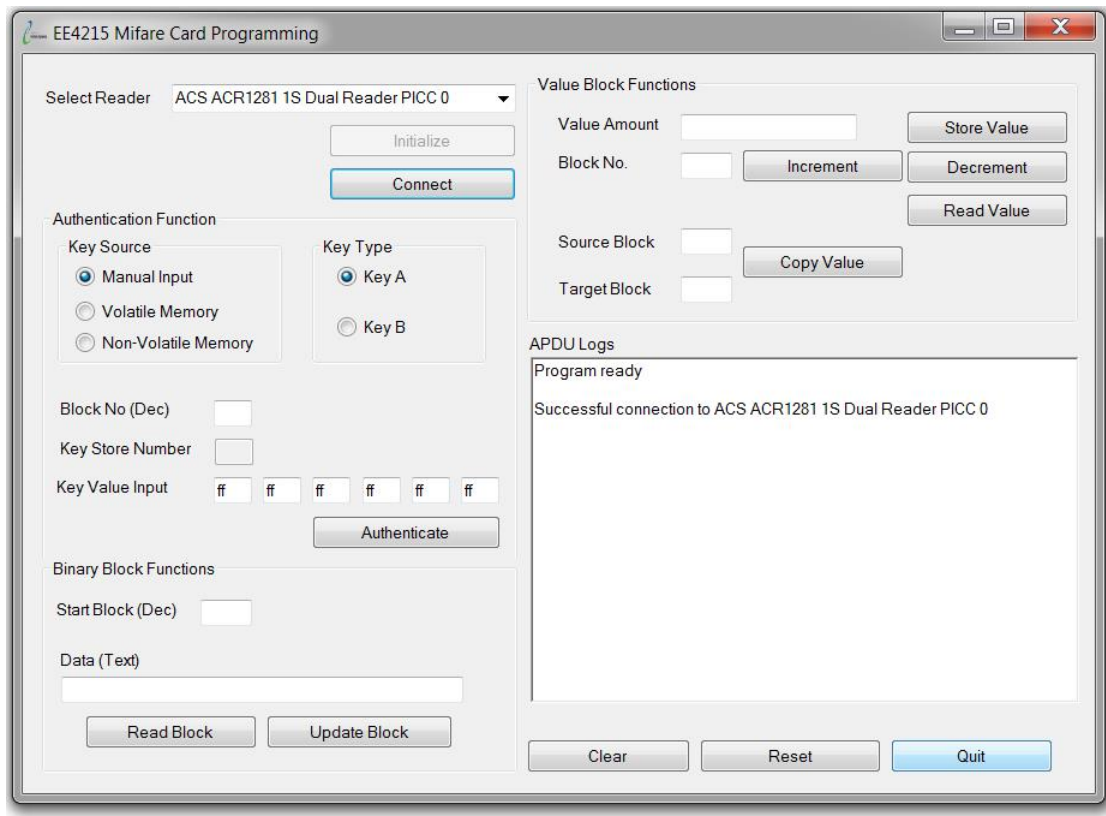


Figure 2: Connect Card Reader

e) Ensure response of the APDU logs show the message:
Successful connection to ACS ACR 1281 1S Dual Reader PICC 0
That means the Card Valid.

Part A - Card ID: (10 marks)

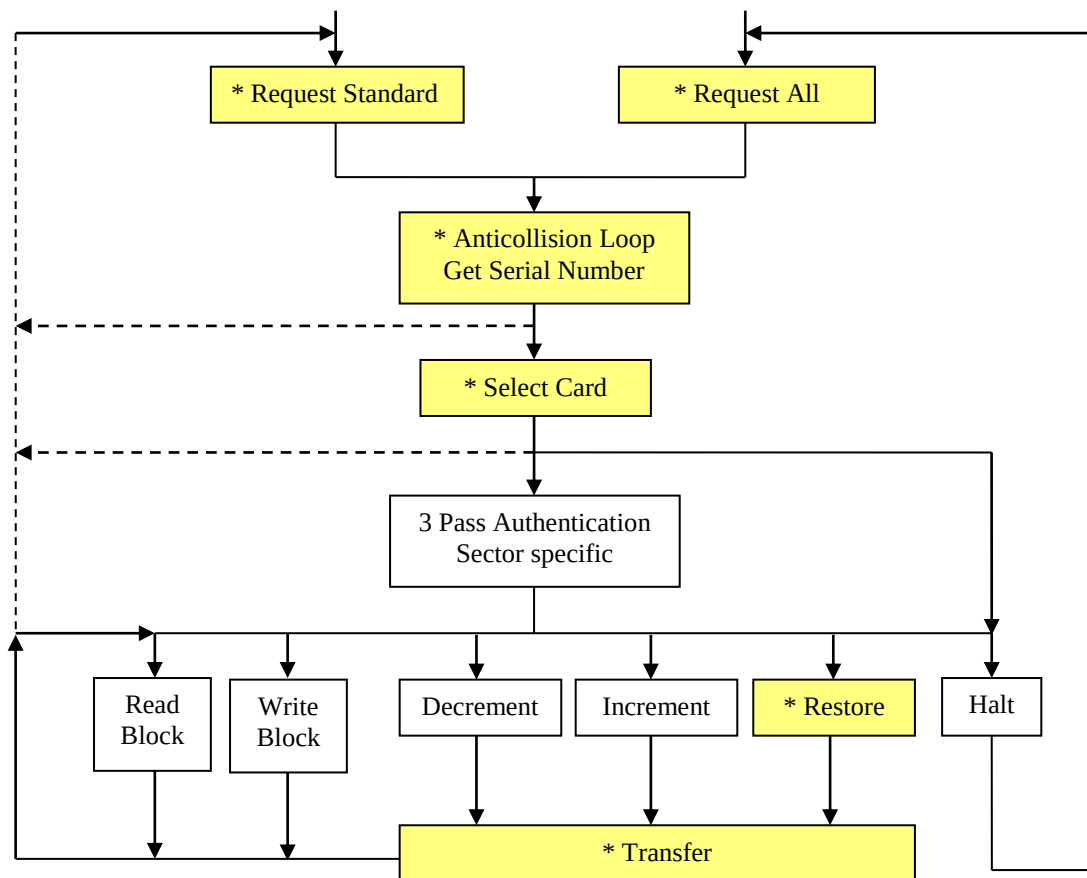


Figure 3: Transaction Flow

***** *The command not implemented by the ACR reader.*

- f) Use the default Authentication Function setting:
 Key Source: Manual Input
 Key Type: Key A
 Key Value Input: ff ff ff ff ff ff

The image shows a software interface for the 'Authentication Function'. It contains two main sections: 'Key Source' and 'Key Type'. In the 'Key Source' section, 'Manual Input' is selected with a radio button, while 'Volatile Memory' and 'Non-Volatile Memory' are unselected. In the 'Key Type' section, 'Key A' is selected with a radio button, while 'Key B' is unselected. Below these sections are three input fields: 'Block No (Dec)' (empty), 'Key Store Number' (empty), and 'Key Value Input' (containing 'ff ff ff ff ff ff'). At the bottom right is an 'Authenticate' button.

Figure 4: Authentication Function

- g) Type the Block number(Dec) “0” and Select “Authenticate” and write down the APDU Command _____ and Response Message_____.

Binary Block Function:

- h) Type the Start Block number “0” and select “Read Block”, write down the APDU Command _____ and Response Message_____.

Read Binary Blocks

This command is used to retrieve multiple “data blocks” from the PICC. The data block/trailer must be authenticated first before executing the “Read Binary Blocks” command.

Command

Command	Class	INS	P1	P2	Le
Read Binary Blocks	FF _H	B0 _H	00 _H	Block Number	Number of Bytes to Read

Where:

Block Number: 1 Byte. Starting Block.

Number of Bytes to Read: 1 Byte. The length of the bytes to be read can be a multiple of 16 bytes for Mifare 1K/4K or a multiple of 4 bytes for Mifare Ultralight

Maximum of 16 bytes for Mifare Ultralight.

Maximum of 48 bytes for Mifare 1K. (Multiple Blocks Mode; 3 consecutive blocks)

Maximum of 240 bytes for Mifare 4K. (Multiple Blocks Mode; 15 consecutive blocks)

Example 1: 10_H (16 bytes). The starting block only. (Single Block Mode)

Example 2: 40_H (64 bytes). From the starting block to starting block+3. (Multiple Blocks Mode)

Note: For security considerations, the Multiple Block Mode is used for accessing Data Blocks only. The Trailer Block is not supposed to be accessed in Multiple Blocks Mode. Please use Single Block Mode to access the Trailer Block.

Response

Response	Data Out		
Result	Data (Multiple of 4 or 16 bytes)	SW1	SW2

Where:

SW1, SW2 = 90 00_H means the operation is completed successfully
= 63 00_H means the operation failed

Example 1: Read 16 bytes from the binary block 04_H (Mifare 1K or 4K)

APDU = { FF B0 00 04 10_H }

Figure 5: ADPU Format

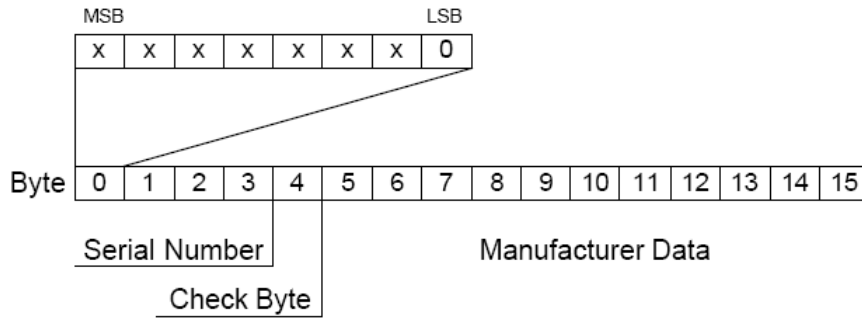


Figure 6: Block 0 Sector 0 Data Format

- i) Select the part of the data out corresponding to the CardID (byte 0-4)
 _____ . How many byte is the CardID (Card Serial Number) ?
 Answer: _____ .
- j) Read the card ID as _____ .
- k) Write the Check byte (byte 4) _____ and
 the Manufacturer Data (byte 5-15) _____ .
- l) Select “Write” and try to write all “0” to Block by clicking “write” button,
 explain why the write operation failed _____ .
- m) Will the card be blocked to operate when error occurred? ☐ Yes ☐ No.

Part B - Normal Read and Write Operations: (5 marks)

Sector	Block	Byte Number within a Block																Description
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
15	3	Key A				Access Bits				Key B								Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A				Access Bits				Key B								Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A				Access Bits				Key B								Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A				Access Bits				Key B								Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

Figure 6: Memory Organization

- n) Type block no. "1" and select "Read Block", write down the Response Data out without SW1 and SW2 : _____.
- o) Type Data(Text) all "1" and select "Update Block", Write down the Response for the block 1 without SW1 and SW2 : _____.
- p) Select "Read Block" and write down the Response Data without SW1 and Sw2 as _____.
- q) Type block no. "2" and select "Update Block", with data "1234567890123456". Write down the Response without SW1 and SW2 : _____.
- r) Select "Read Block", write down the Response Data without SW1 and SW2 _____.

Part C- Access Conditions: (10 marks)

Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	Key A					Access Bits				Key B (optional)						

Figure 7: Sector Trailer (Block 3)

- s) Type Block no. “3” and select “Read Block”, write down the Response Data _____.
- t) Select the part of data in block 3 which is corresponding to the key A (Byte0-5) _____ and key B (Byte10-15) _____.
- u) What are the Access Bytes (Byte 6-9)? _____.
- v) Given the access conditions in Figures below:

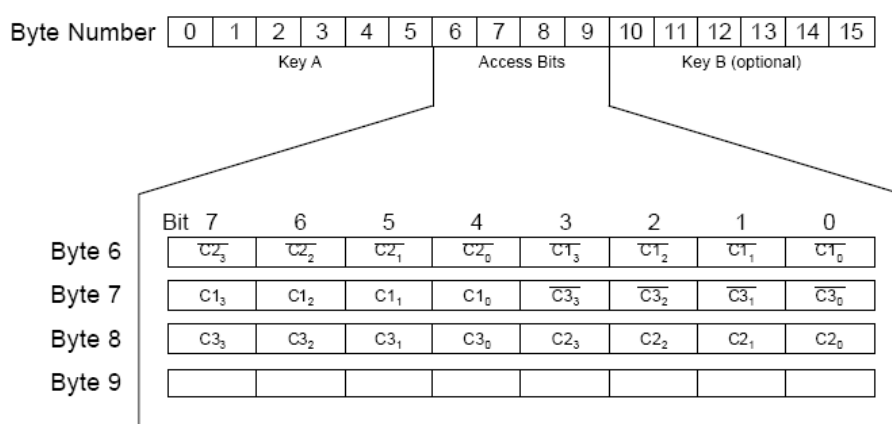


Figure 8: Access Bits

Where CN_m is the access bit N in block m and $\overline{x}$ is the complement of x.

Access bits			Access condition for						Remark
			KEYA		Access bits		KEYB		
C1	C2	C3	read	write	read	write	read	write	
0	0	0	never	key A	key A	never	key A	key A	Key B may be read
0	1	0	never	never	key A	never	key A	never	Key B may be read
1	0	0	never	key B	key A B	never	never	key B	
1	1	0	never	never	key A B	never	never	never	
0	0	1	never	key A	key A	key A	key A	key A	Key B may be read, transport configuration
0	1	1	never	key B	key A B	key B	never	key B	
1	0	1	never	never	key A B	key B	never	never	
1	1	1	never	never	key A B	never	never	never	

Figure 9: Key Block Access Condition

Access bits			Access condition for				Application
C1	C2	C3	read	write	increment	decrement, transfer, restore	
0	0	0	key A B ¹	key A B ¹	key A B ¹	key A B ¹	transport configuration
0	1	0	key A B ¹	never	never	never	read/write block
1	0	0	key A B ¹	key B ¹	never	never	read/write block
1	1	0	key A B ¹	key B ¹	key B ¹	key A B ¹	value block
0	0	1	key A B ¹	never	never	key A B ¹	value block
0	1	1	key B ¹	key B ¹	never	never	read/write block
1	0	1	key B ¹	never	never	never	read/write block
1	1	1	never	never	never	never	read/write block

Figure 10: Data Block Access Condition

- w) Write down the access condition of this sector Block 3 (Key Block): _____,
means Access Read/Write by ☐ Key A ☐ Key B ☐ Key A|B.
- x) Write down the access condition of this sector, Block 0-2 (Data Block):
_____ (Block 0/1/2), means read/write access by ☐ Key A ☐ Key B
☐ Key A|B.
- y) Select “Update Block” again and explain why “block 3” is barred from modification in this exercise,
_____.
- z) If “block 3” is allowed to be modified and the original key is used, will the
“sector” operation be blocked? ☐ Yes ☐ No.

Part D- Value Block: (20 marks)

- aa) Type the block no. “1” in Authentication Function and select “Authenticate” to get the data access right. **Please do not use the trailer block to store/increment/decrement/copy value.**
- bb) Type Data(Text) “0000000000000000” and Select “Update Block”.
- cc) Select “Read Block”, write down the APDU Logs Response Data
_____.
- dd) Type the block no. “1” and Value Amount “0” in Value Block Functions and select “Store Value”, write down the APDU Logs Response Data as
_____.
- ee) Select “Read Block”, write down the APDU Logs Response Data
_____.
- Note that there is a major format difference between reading in steps aa) and cc).
- ff) Refer to the value block format below:

Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	Value				Value				Value				Adr	Adr	Adr	Adr

Figure 11: Value Block Format

- Write down the data of Value (byte 0-3) in step ff) _____ and data of *Value* (byte 4-7) _____ and the repeated data of Value (byte 8-11) _____ and data of *Adr* in byte 12 _____ and *Adr* in byte 13 _____; and data of *Adr* in byte 14 _____ and *Adr* in byte 15 _____. Ensure they are complement.
- gg) Change the Value Amount to “1000”, and Select “Store Value”, write down the APDU Logs Response Data _____.
- hh) Select “Read Value” and write down the value amount.
_____.
- ii) Type Block no. “1” and select “Read Value” in Value Block Functions, write down the value _____ and APDU Logs Response Data
_____.
- jj) Type Block no. “1” and select “Read Block” in Binary Block Function, write down the APDU Logs Response Data
_____.
- kk) Given 1000 (decimal) is represented by 03E8 in Hexi-decimal form, state where the data E8 (lower byte) can be found in byte _____ of block 1 and the data 03 (higher byte) can be found in byte _____ of block 1.
- ll) Write down the Value (byte 0-3) _____ and *Value* (byte 4-7) _____ in jj). Check if they are complementary ☐ Yes ☐ No.

Part E- Value Block Increment/Decrement Operations: (10 marks)

Value block can be manipulated using increment and decrement operations with values. Increment or decrement values are pre-stored in REGISTERS and the update is completed by a “Transfer” command. The incremental/decrement REGISTER can be clear using a “Restore” command if the incremental/decrement operation is cancelled by a “revocation” action. Unfortunately, the command not implemented by the ACR reader. The amount of value will be updated directly by using the “Increment” /”Decrement”.

- mm) Type Value Amount “100” , Block no. “1” and select “Increment”, write down the APDU Logs Response Data
_____.
- nn) Select “Read Value”, write down the Value Amount _____ and APDU Logs Response Data _____.
- oo) Check if the amount is increased correctly ☐ Yes ☐ No.
- pp) Type Value Amount “10” , Block no. “1” and select “Decrement”, write down the APDU Logs Response Data _____.
- qq) Select “Read Value”, write down the Value Amount _____ and APDU Logs Response Data _____.
- rr) Check if the amount is increased correctly ☐ Yes ☐ No.

END