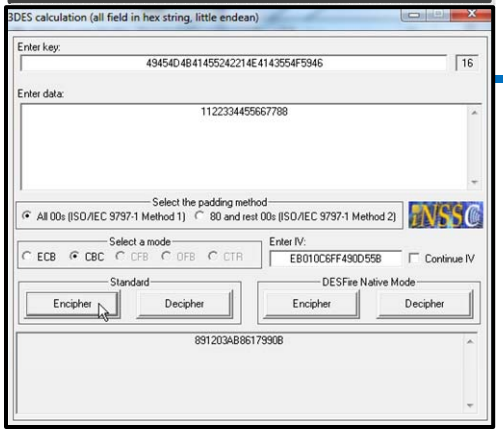
Generating Ek(RndA)

- MODE = CBC, IV = Ek(RndB)
- Padding Method is ISO/IEC 9797-1, Method 1

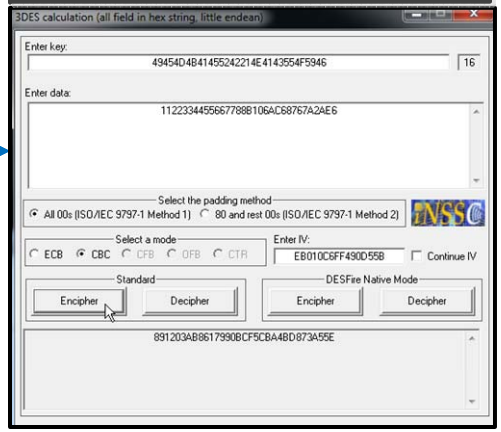
- 16 byte key
- Data = 8 bytes random # (generated by PCD)
- DES algorithm (**encipher**)
- Generates Ek(RndA)



Generating Ek(RndA + RndB')

- MODE = CBC, IV = Ek(RndB)
- Padding Method is ISO/IEC 9797-1, Method 1

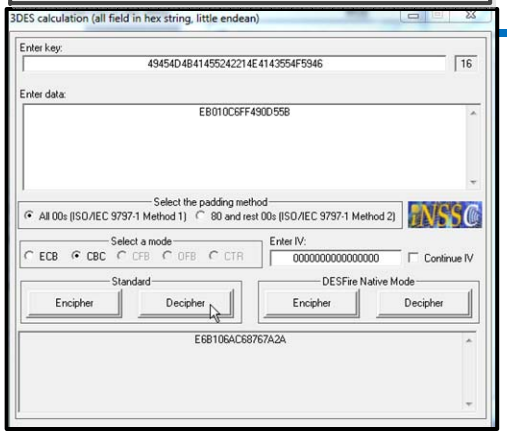
- 16 byte key
- Data = 8 bytes random # (RndA) + RndB'
- (RndB' = RndB with first byte rotated)
- DES algorithm (**encipher**)
- Generates Ek(RndA + RndB')

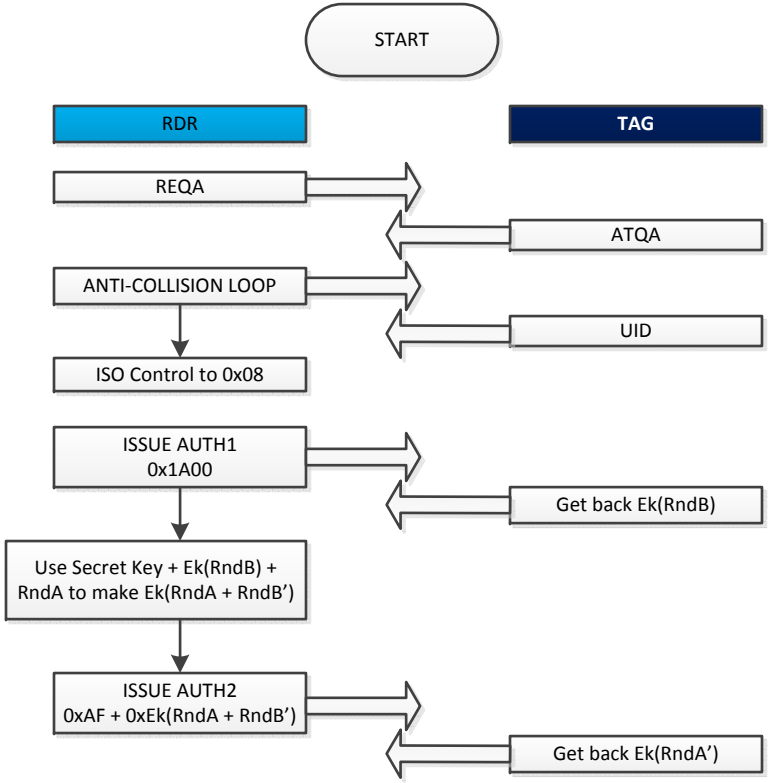


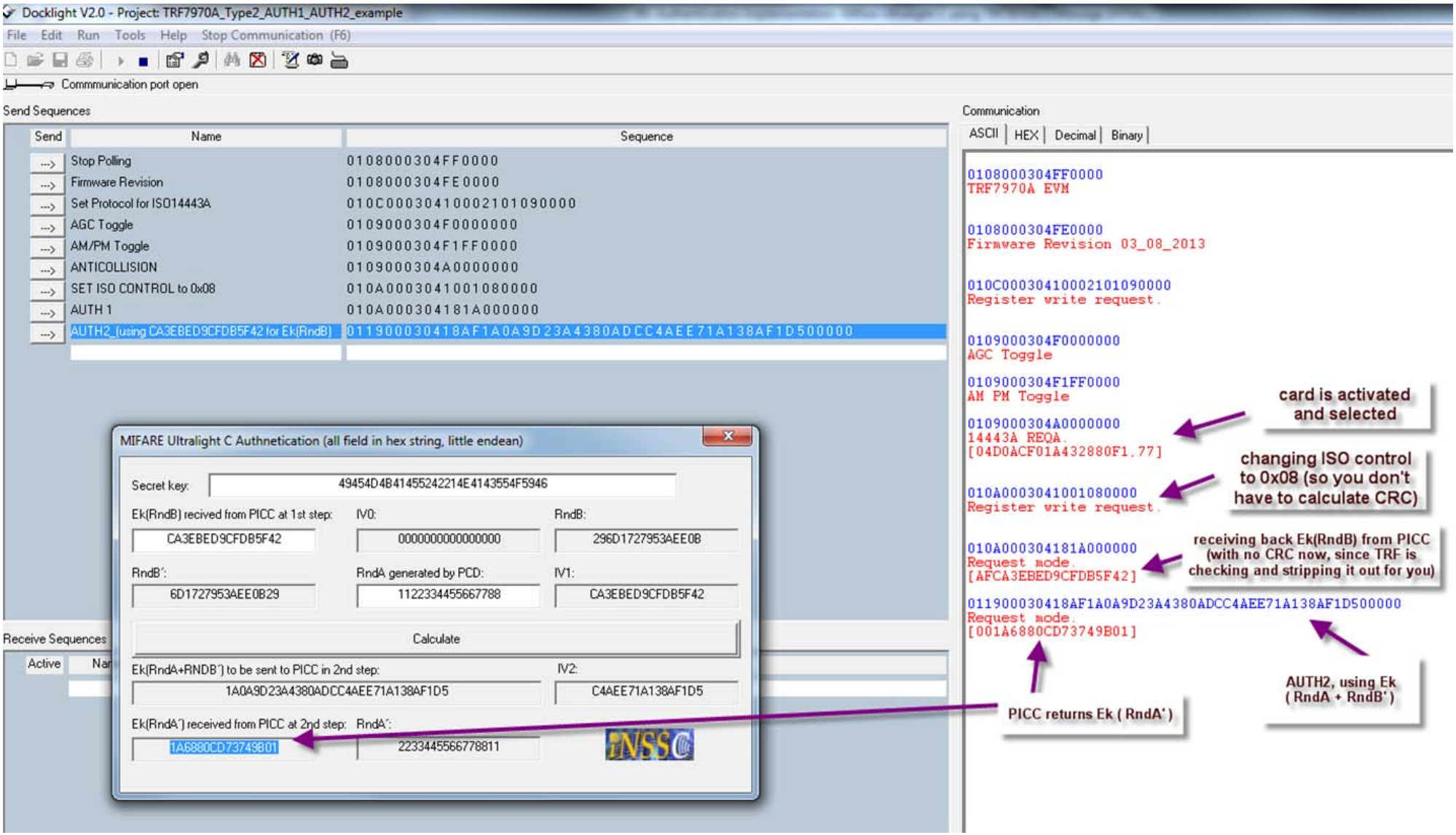
Generating RndB

- MODE = CBC, IV = 0000000000000000
- Padding Method is ISO/IEC 9797-1, Method 1

- 16 byte key
- Data = Ek(RndB), rx'ed from PICC
- DES algorithm (**decipher**)
- Generates: RndB






Docklight V2.0 - Project: TRF7970A_Type2_AUTH1_AUTH2_example
File Edit Run Tools Help Stop Communication (F6)
Commmunication port open
Send Sequences
Send
Name
Sequence
Stop Polling 0108000304FF0000
Firmware Revision 0108000304FE0000
Set Protocol for ISO14443A 010C0003041000210109000 0
AGC Toggle 0109000304F0000000
AM/PM Toggle 0109000304F1FF0000
ANTICOLLISION 0109000304A0000000
SET ISO CONTROL to 0x08 010A0003041001080000
AUTH 1 010A000304181A000000
AUTH2_(using CA3EBED9CFDB5F42 for Ek(RndB) 011900030418AF1A0A9D23A4380ADCC4AEE71A138AF1D500000
MIFARE Ultralight C Authnetication (all field in hex string, little endean)
Secret key: 49454D4B41455242214E4143554F5946
Ek(RndB) recived from PICC at 1st step: CA3EBED9CFDB5F42
IV0: 0000000000000000
RndB: 296D1727953AEE0B
RndB´: 6D1727953AEE0B29
RndA generated by PCD: 1122334455667788
IV1: CA3EBED9CFDB5F42
Calculate
Ek(RndA+RNDB´) to be sent to PICC in 2nd step: 1A0A9D23A4380ADCC4AEE71A138AF1D5
IV2: C4AEE71A138AF1D5
Ek(RndA´) received from PICC at 2nd step: 1A6880CD73749B01
RndA´: 2233445566778811
Receive Sequences
Active
Communication
ASCII HEX Decimal Binary
0108000304FF0000
TRF7970A EVM
0108000304FE0000
Firmware Revision 03_08_2013
010C0003041000210109000 0
Register write request.
0109000304F0000000
AGC Toggle
0109000304F1FF0000
AM PM Toggle
0109000304A0000000
14443A REQA.
[04D0ACF01A432880F1.77]
010A0003041001080000
Register write request.
010A000304181A000000
Request mode.
[AFCA3EBED9CFDB5F42]
011900030418AF1A0A9D23A4380ADCC4AEE71A138AF1D500000
Request mode.
[001A6880CD73749B01]
card is activated and selected
changing ISO control to 0x08 (so you don't have to calculate CRC)
receiving back Ek(RndB) from PICC (with no CRC now, since TRF is checking and stripping it out for you)
AUTH2, using Ek (RndA + RndB')
PICC returns Ek (RndA')