Security Access

Purpose : Provide Security to

- Data / Information
- Diagnostic Services

Why Security needed : Services like **Routines or some data** into the server to be **read / write specific memory** locations from / to the server security is needed because if improper handling of any of these may cause severe damage the electronics **(Mother Board)** hardware or corrupt the complete software and other vehicle components. To avoid such kind of risk in the vehicle security access service is the only hope while using this protocol.

Algorithm

Access to the data or services with security is for many reasons like **Emissions related data, Lawful security & Safety.**

The security concept uses a seed and key relationship, i.e seed and key algorithm

Algorithm Sequence

The security Access Flow sequence

- Client requests for the **“seed”**
- Server responds with **“seed”**
- Client requests with the **“key”** (respective for the Seed received)
- Server responds positively if **“key”** is valid and that it will unlock itself otherwise Server responds with negative NRC and

Key Structures

The security Access Key has some formats

- Internally Stored Value
- Encrypted Value
- Calculated Value

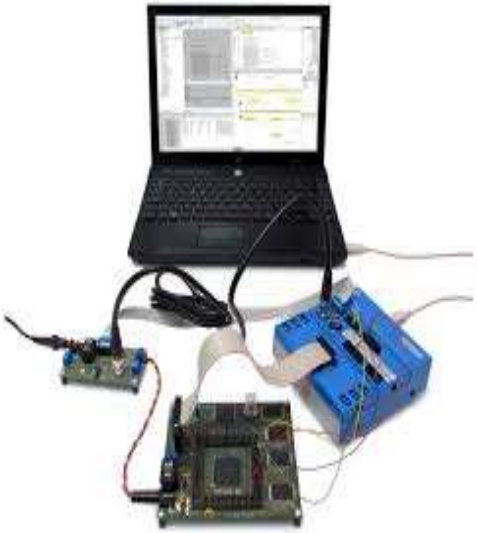
Sub-Function - Security Access

There are levels of sub-function in security Access

- **Request for Seed**
- **Send Key**

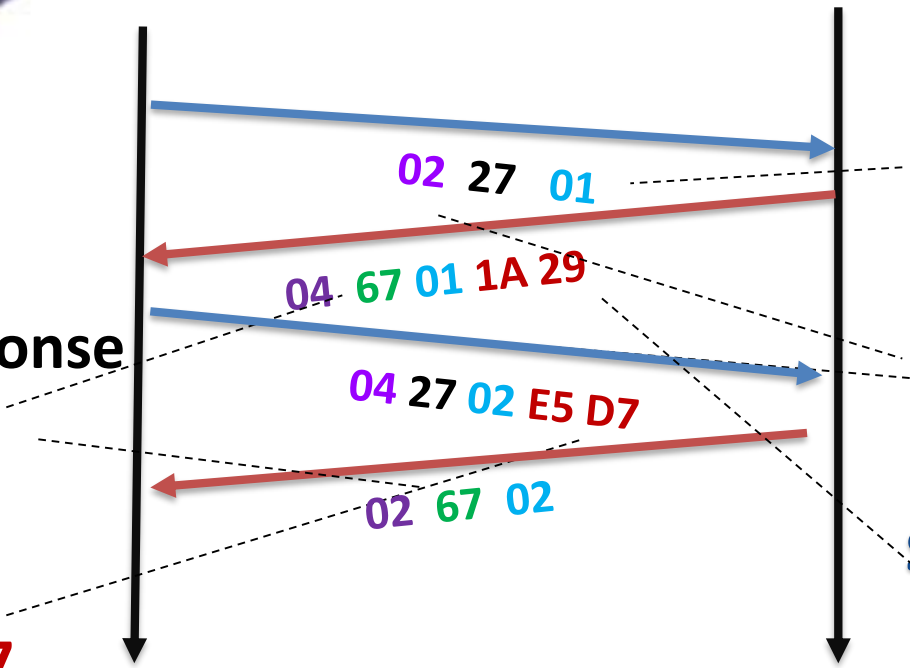
There are levels of sub-function in security Access

- **Request for Seed (0x01, 0x03, 0x05..0x41)**
- **Send Key (0x02, 0x04, 0x06..0x42)**



Request & Response

First Level Security



Sub-function
01

PCI Length : 02
04

Positive Response : 67

Key :
E5 D7

Seed :
1A 29

Calculation on security Access

Seed – 1A 29 (hex)

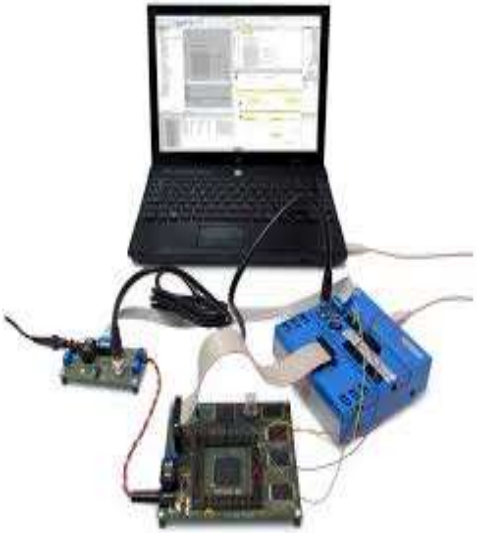
0001 1010 0010 1001 - Seed Value (1A 29)

1110 0101 1101 0110 - 1’s Comp

1 - 2’s Comp

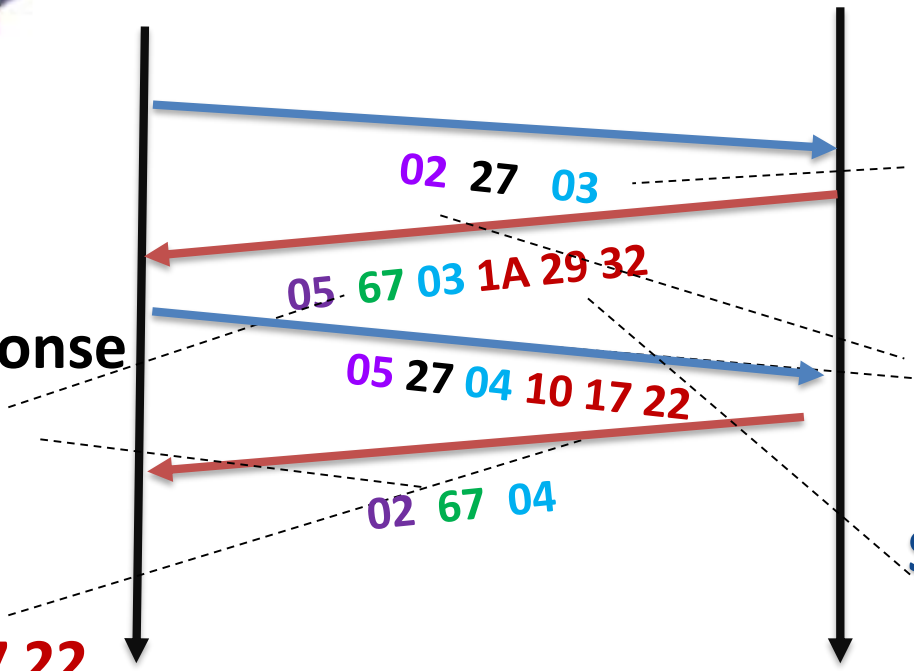
1110 0101 1101 0111- E5 97 (hex)

Key – E5 97



Request & Response

Second Level Security



Sub-function

03 & 04

Positive Response : 67

PCI Length : 02

05

Key :

11 27 22

Seed :

1A 29 32

Points to be discussed in security Access Service

1. **How levels of sub-function in security Access**

   21
2. **Why so many security levels are required ?**

   Each level has different purpose
3. **How all the levels are related ?**

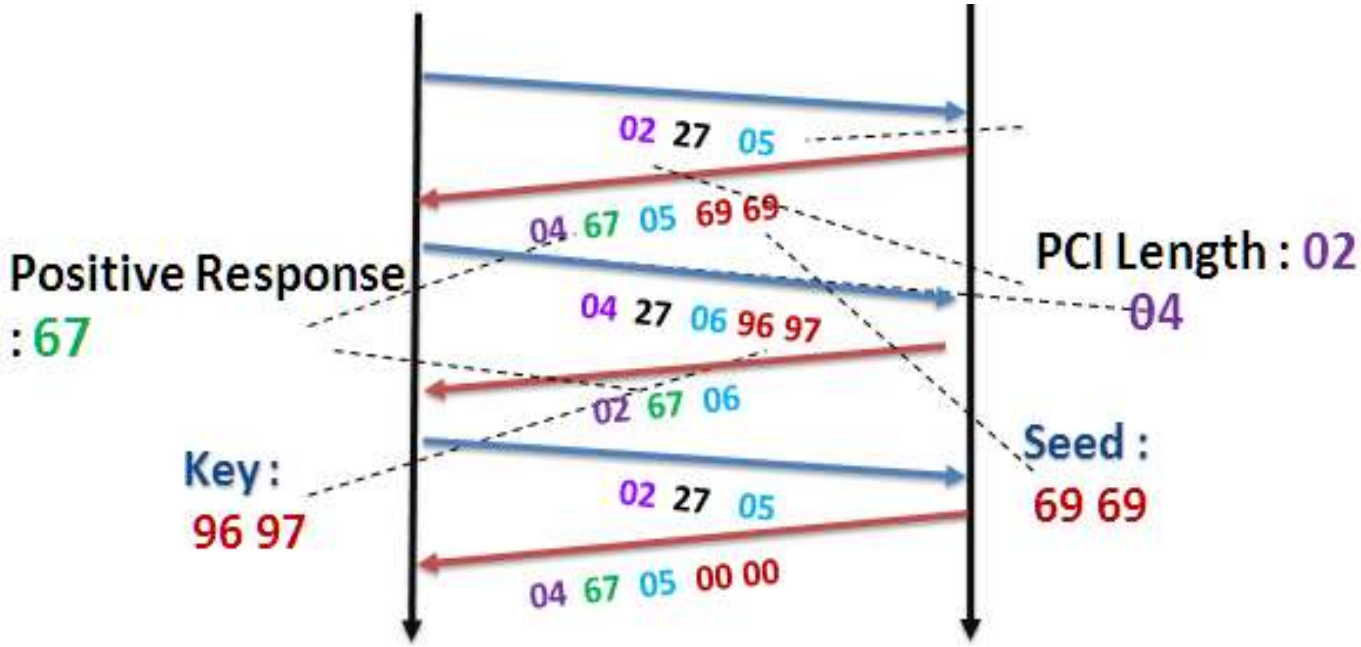
   No levels are related
4. **What happens if two levels of security unlocked consequently ?**

   Only one security level shall be active at any instant of time
5. **Give Example for unlocking**

   It will compare the key value with of returned and stored

Points to be discussed in security Access Service

6. If already security unlocked but tester tries to request seed the **ECU responds with positive** response message service with a seed value equal to **zero** and sends **non-zero** value for locked state
7. Invalid key requires the Tester to **start over** from the beginning of the Security Access



Timer and Time Delay in Security

Due to single failed attempt and Reset happened to the ECU then ECU has to obey the time delay defined as per requirement

If tester attempts multiple failed attempts then time delay has to be enabled for next attempt (Just like our android or IOS)

The delay timer is only required if server is locked due to unsuccessful attempt

Timer and Time Delay in Security

✓ If security gets unlocked then the unlocked state will be active for particular time only (say - 30sec's)depends on OEM

✓ Certain sequence to be followed while using security access

Supported NRC for 0x27

12 - Sub Function Not Supported : If tester send any non-implemented or wrong sub-function then it will give this NRC.

13 - Incorrect Message Length Or Invalid Format in PCI length Declaration : If we requested a wrong/invalid then the it will give this negative response.

22 - Conditions Not Correct : If the criteria for the request Security Access are not met.

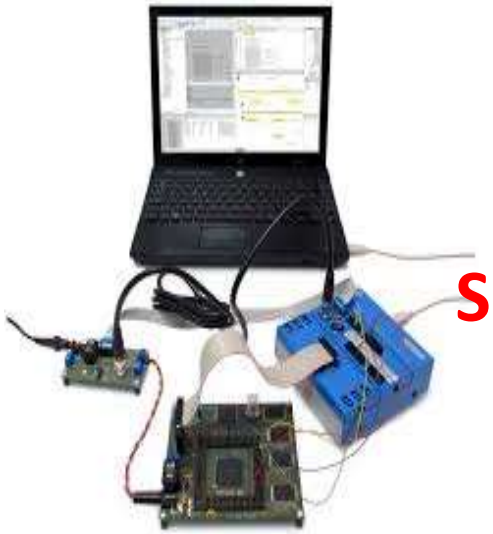
24 - Request Sequence Error : Send key directly without receiving seed.

31 - Request out of range : If user sends Invalid Data

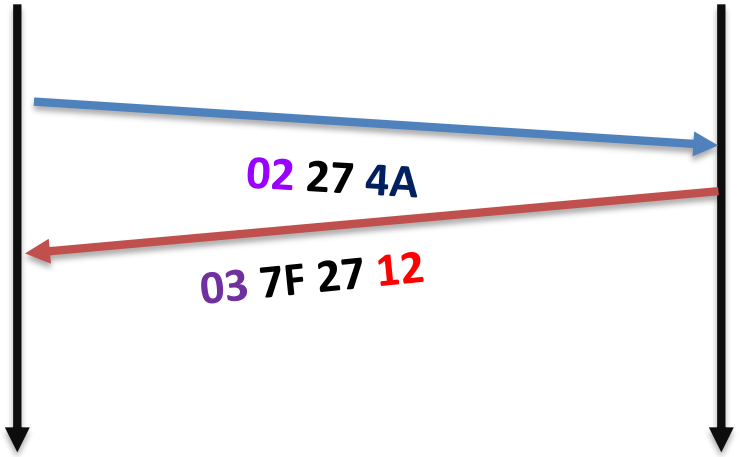
35 - Invalid Key : If the key value not match with stored value in server then tester will get NRC.

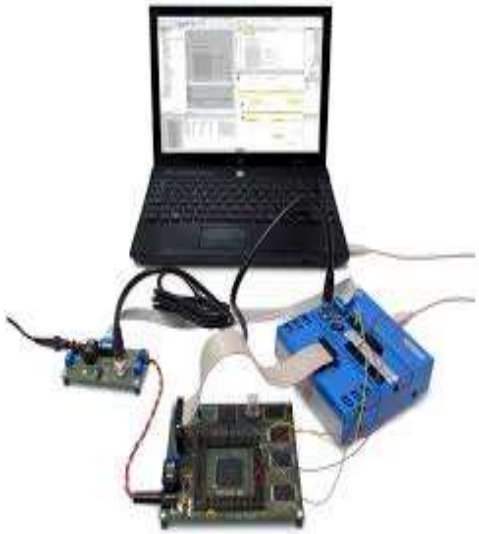
36 - Exceed number of Attempts : If the number of attempts exceeds maximum invalid attempts

37 – Required Time Delay not Expired : If the delay timer is active and request is sent

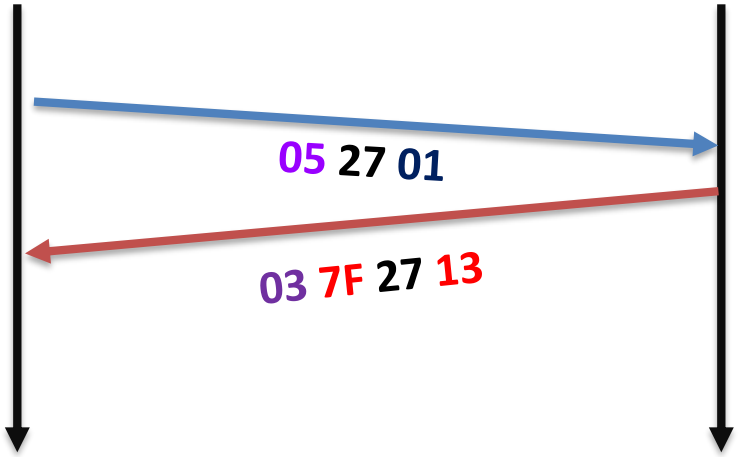


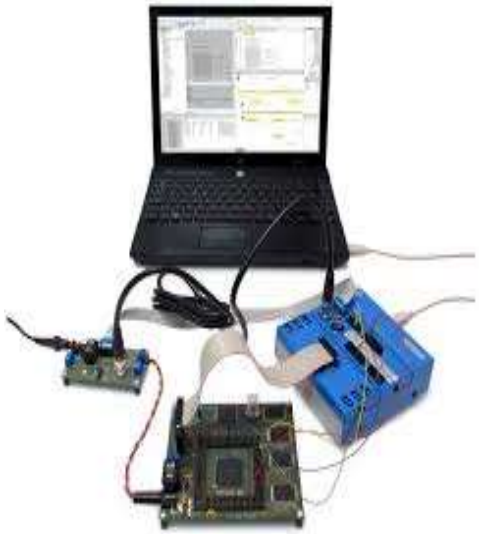
Sub-Function not Supported



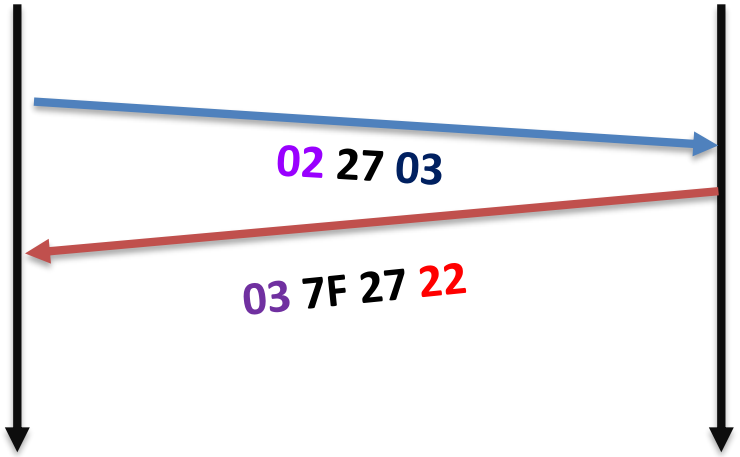


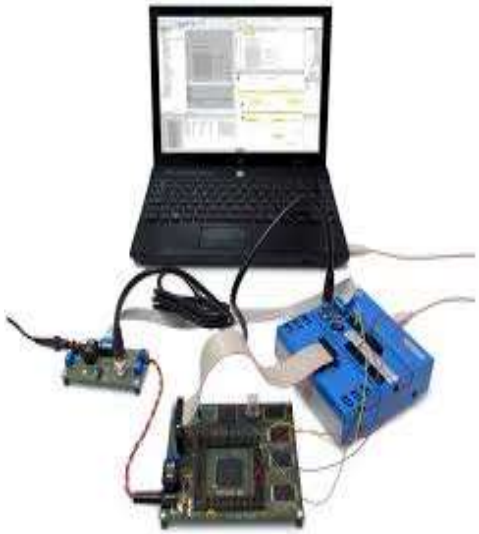
Incorrect Length



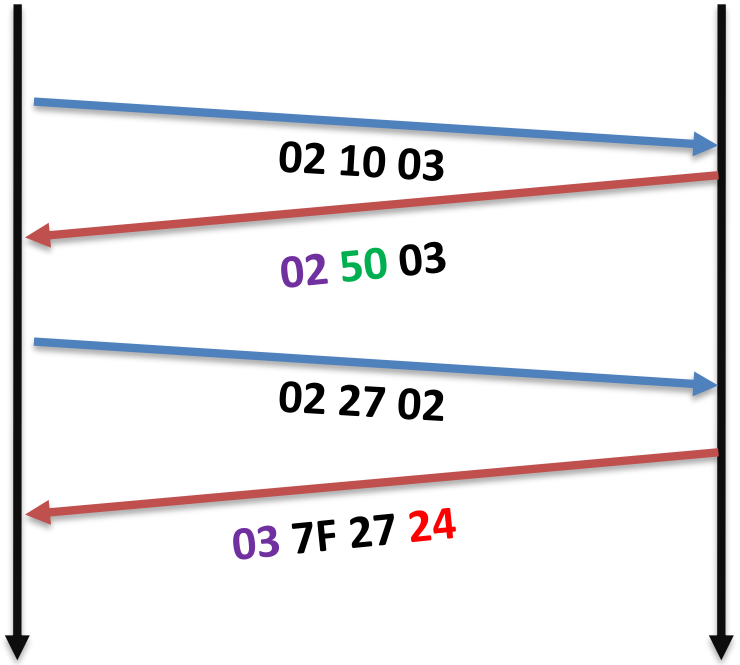


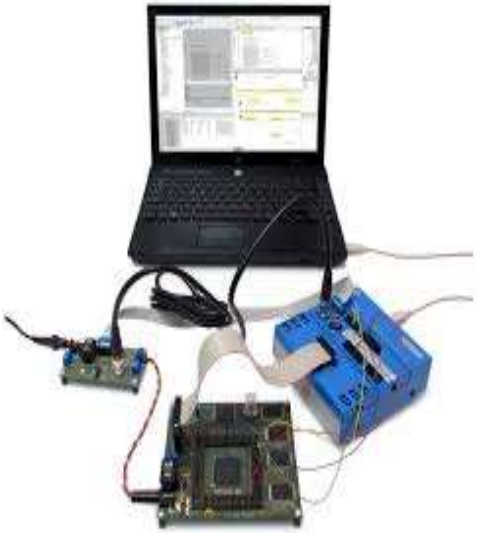
Condition not correct



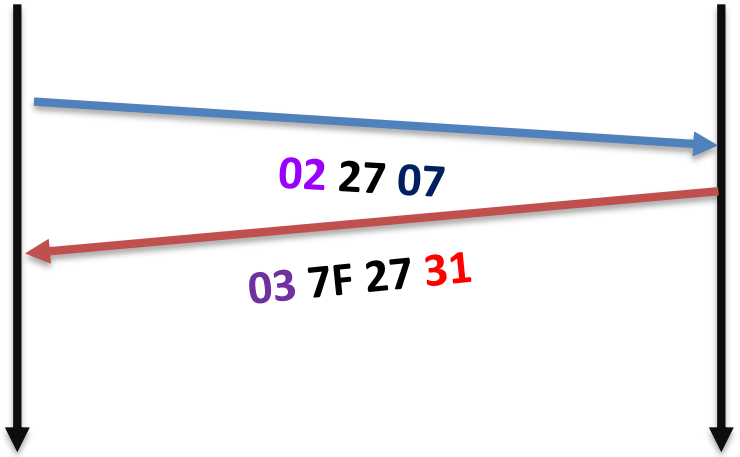


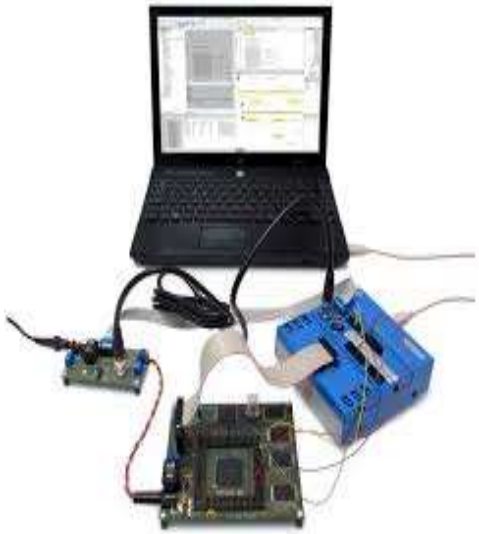
Request Sequence Error



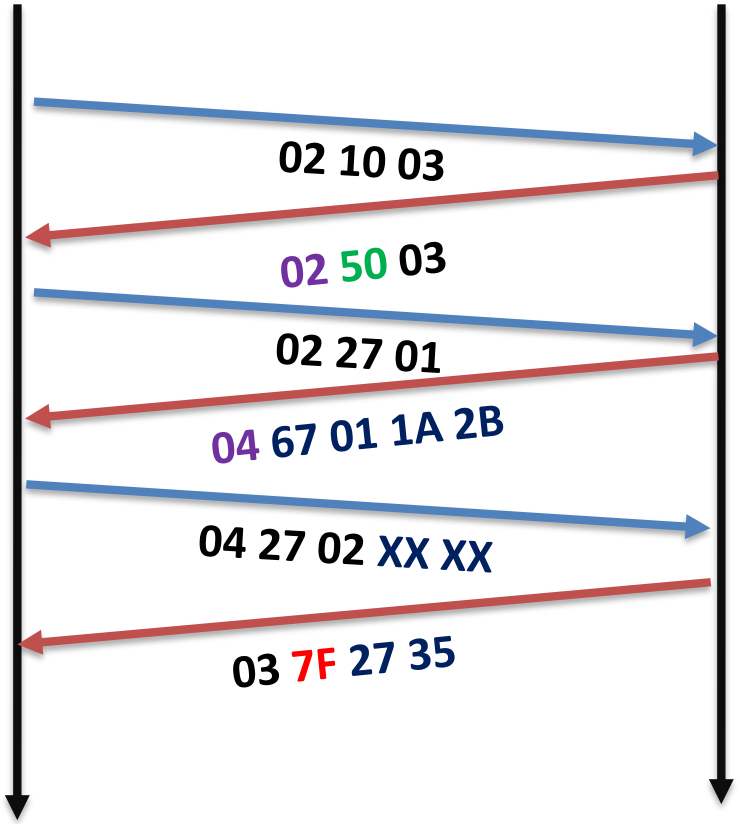


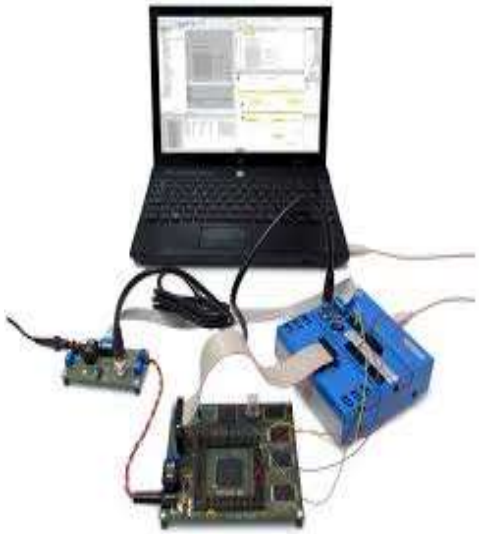
Request Out of Range



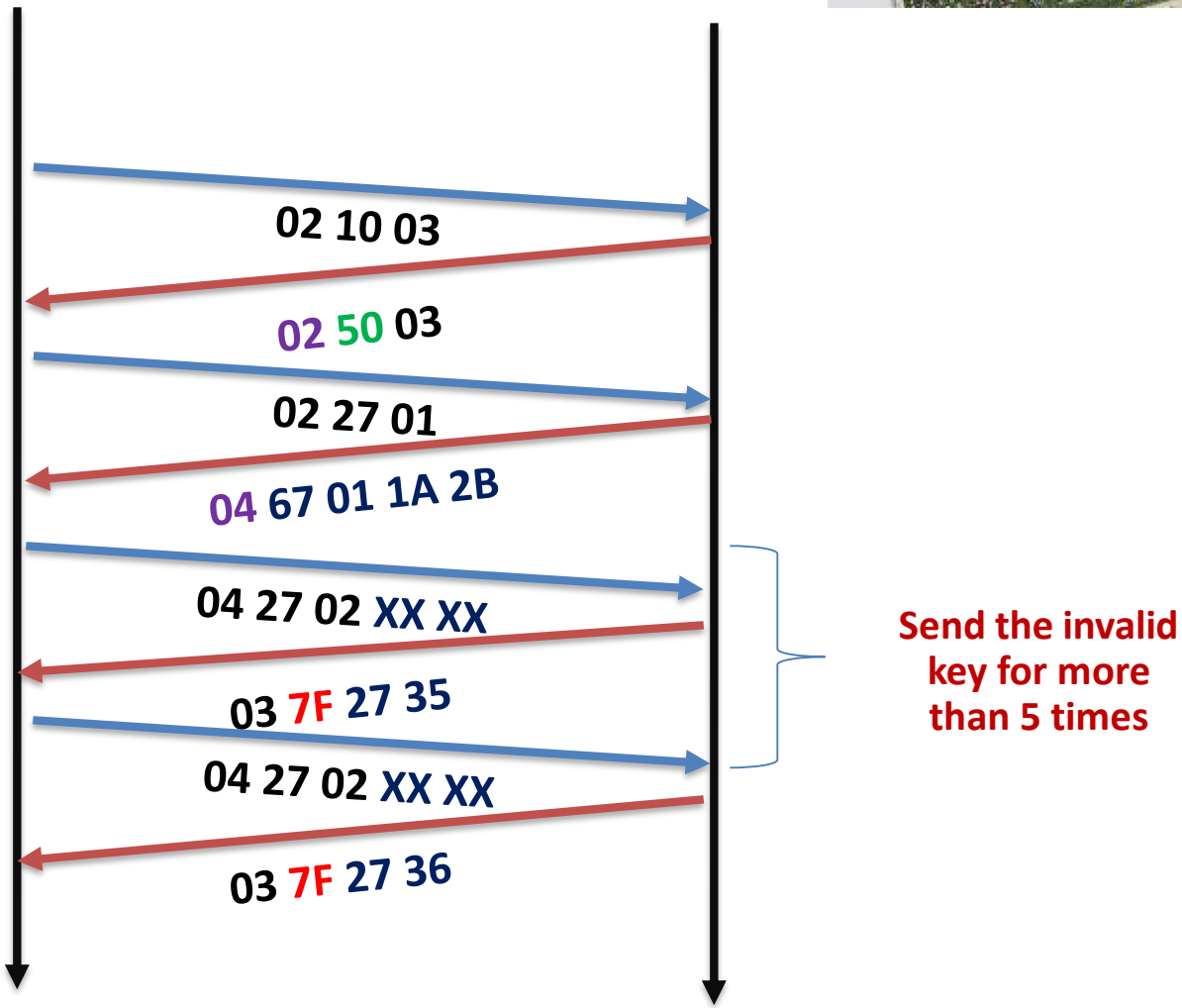


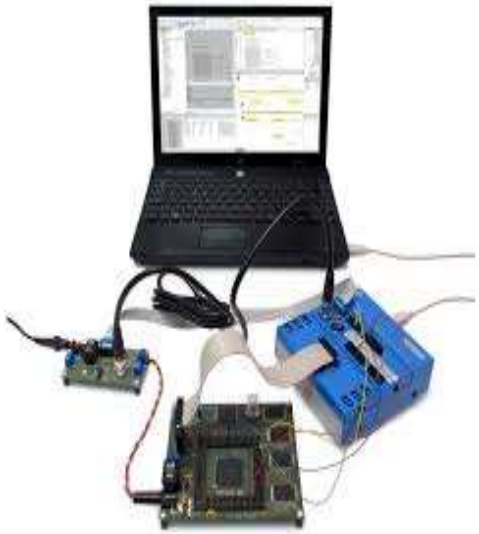
Invalid Key



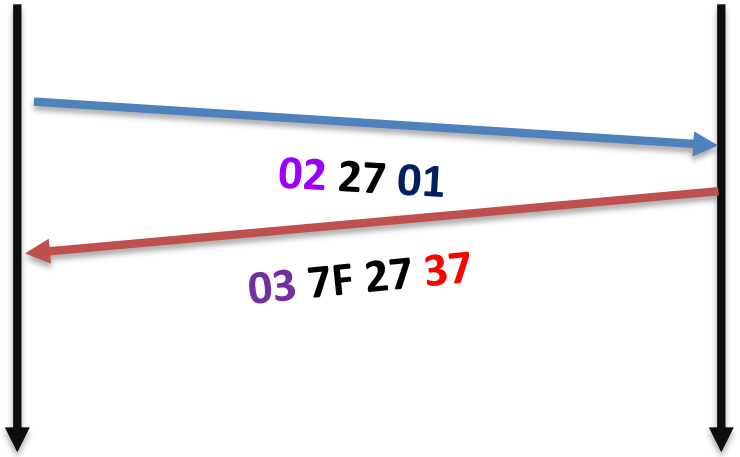


Exceed Number of Attempts





Required time delay not expired



End of the Tutorial !!