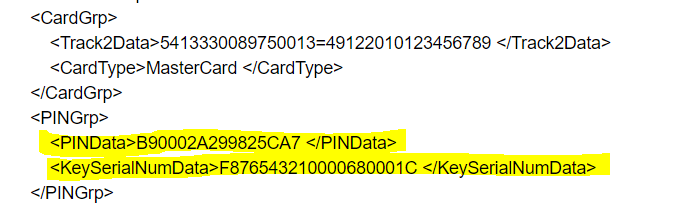
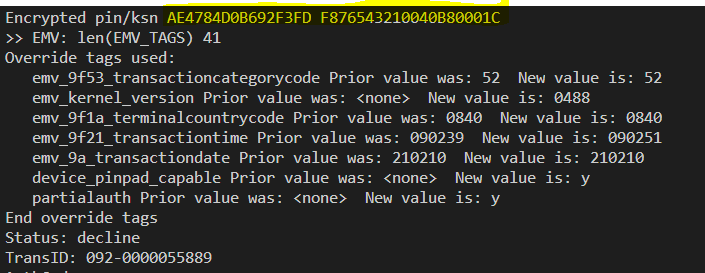
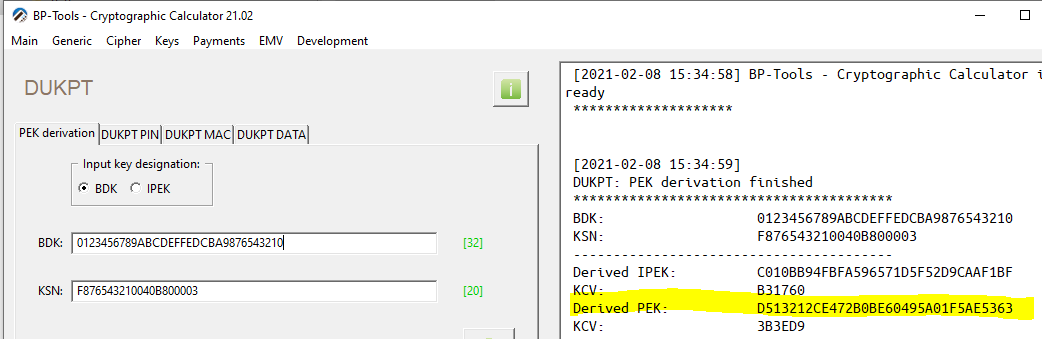
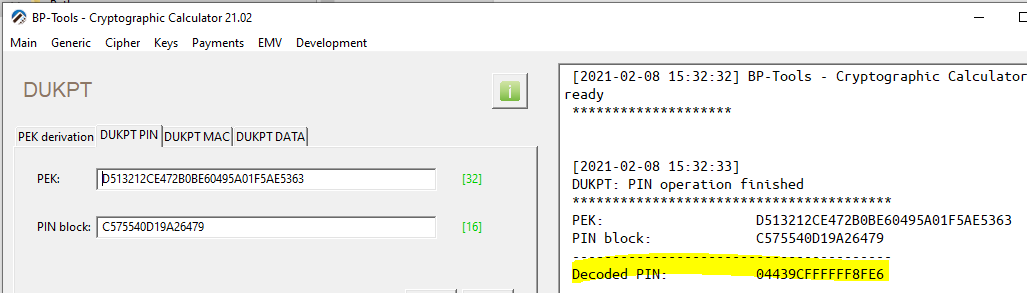
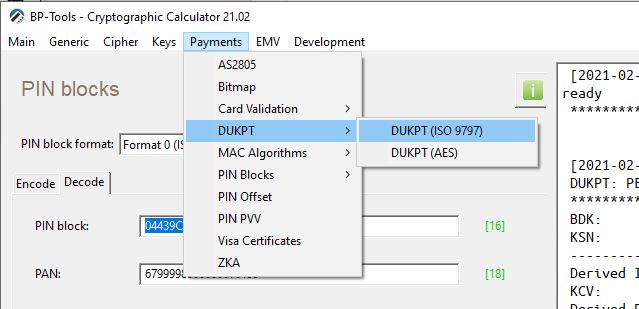
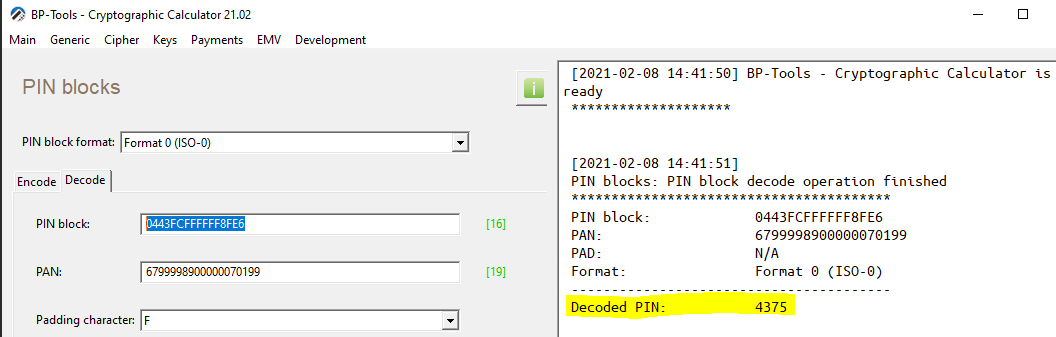
When a card reader pauses to obtain the user's PIN, the reader must send the card number (PAN) to the PIN pad along with a KSN. The PIN pad uses the KSN to derive a one-time PIN key. The PAN is then combined with the PIN (using XOR), and the combination (called a "PIN block") is encrypted with the one-time key before being sent to the reader. The procedure outlined below shows how to decrypt the PIN block.

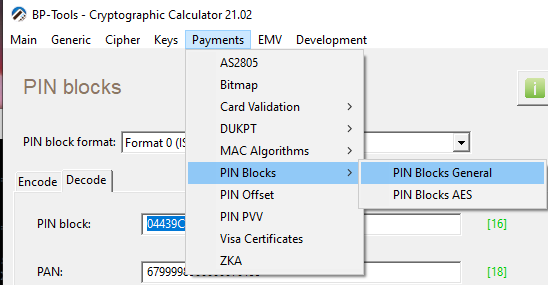
1. **OBTAIN KSN / EncryptedPIN:**  
   1.1 PYTHON TESTHARNESS  
     
     
   1.2 FDRC TRANSACTION LOG  
     
     
   THE FOLLOWING VALUES ARE USED FOR THIS EXAMPLE:  
     
   \* KSN: F876543210040B800003  
   \* EncryptedPIN: C575540D19A26479



**USING DUPKT IN BP-TOOLS**  
  
Obtain Derived PEK: D513212CE472B0BE60495A01F5AE5363  
  
  
  
Decode output using DUKPT PIN method:  
  
  
Notice the Decoded PIN format:  
  
- the first two bytes indicate the PIN length: 04  
- the next two bytes indicate the unencrypted first two digits PIN entry: **43**- decryption is performed on the remaining bytes to obtain the last 2 PIN digits: FCFFFFFF8FE6



1. **USING PIN BLOCKS**  
     
     
     
   Decode the PIN using:  
   \* DecryptedPIN: 0443FCFFFFFF8FE6  
   \* PAN: 6799998900000070199  
     
   



This gives us the remaining 2 digits in the PIN: **75**  
The decrypted PIN is: **4375**

**REFERENCES**:

BP-TOOLS Installer: [S:\Department Private Folders\Business Development\Business Administration\Payment App\5\_TC IPA\IPA5\EMV Certification\Tools\bp-tools](https://sphereclientsolutions.visualstudio.com/Integrated%20Applications/_wiki/wikis/IPA.wiki?wikiVersion=GBwikiMaster&pagePath=%2FDevelopment%20Tools%2FONLINE%20PIN%20DECRYPTION&pageId=211&_a=edit)