BACK OF THE NAPKIN HACKING

Quick test script

- **Decrypt a known initial block using a known Nonce/Key**
- **Iterate over Nonce changes**
- **Return results that land in our required ranges**

```
Key                 - FAA30A7DCC58C862576C486BC858DBDCDE88B6DDE0612E8C3D292A30D6447B02
IV(Nonce+Counter)   - 01020304050607080000000000000000
Encrypted Value     - 5D10BBDA05498A9200878AE0A92E56DF
```

BACK OF THE NAPKIN HACKING

```
└─[$]> python nonce_hunt\ copy.py FAA30A7DCC58C862576C486BC858DBDCDE88B6DDE0
Searching by byte
potential iv 0192030405060708000000000000000000 - SP dd7ea2fd Reset 362cf679
potential iv 01020304050c0708000000000000000000 - SP dbdbbef4 Reset 36706836
searching by 4byte blocks
potential iv 0192030405060708000000000000000000 - SP dd7ea2fd Reset 362cf679
potential iv 0282030405060708000000000000000000 - SP 69b0b6c7 Reset 3634e178
potential iv 050a0304050607080000000000000000000 - SP c20a37db Reset 161b2fee
potential iv 0572030405060708000000000000000000 - SP fe4dc684 Reset 160d9b52
potential iv 0648030405060708000000000000000000 - SP 01eb79c4 Reset 367e69ee
potential iv 0682030405060708000000000000000000 - SP 8d43ae5b Reset 1602df1d
potential iv 06ea0304050607080000000000000000000 - SP 3fdf567f Reset 164b236f
potential iv 0815030405060708000000000000000000 - SP 9093b11d Reset 16545aaf
potential iv 0844030405060708000000000000000000 - SP 1f25dbbf Reset 160aaea2
potential iv 098a030405060708000000000000000000 - SP 8657becd Reset 3627840e
```

IV = Nonce + Block Counter