Secure Processor MicroArchitecture
Assignment 2

Team Members:
Surya Prasad S - EE19B121
Sai Dheeraj Ettamsetty - CS18B055

1. Round keys used in the first round in the Encryption function:
   Each of these round keys are 32-bit written as a list of 4 one byte (8-bit) numbers.

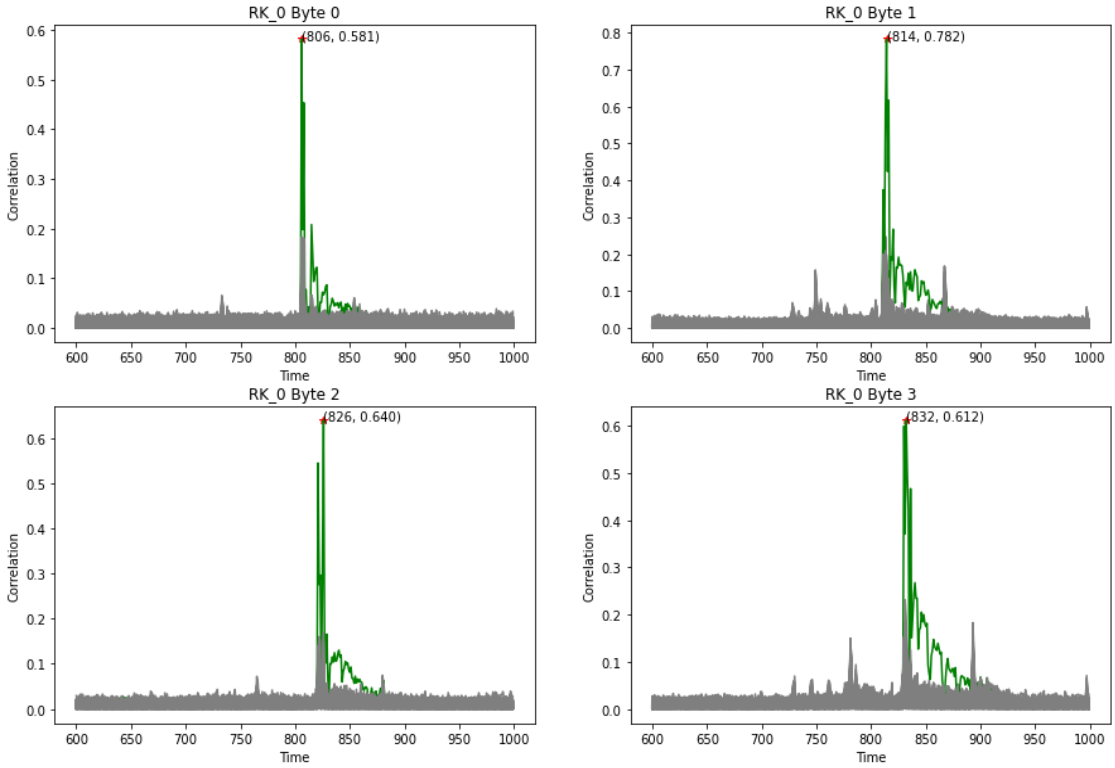
   Finding RK0 -
   In Hexa form - [60, B6, 89, 83]
   In Decimal form - [96, 182, 137, 131]

   Each block in the following figure has 3 numbers:
   1. Key byte in Hex form.
   2. Correlation/Mean difference value obtained for that particular key.
   3. Exact time point where that correlation is obtained. (Only for CPA)

	0	1	2	3
0	60 0.581 806	B6 0.782 814	89 0.640 826	83 0.612 832
1	63 0.183 806	71 0.259 811	95 0.169 826	9A 0.232 831
2	20 0.178 807	8F 0.248 813	8A 0.160 822	7A 0.183 831
3	7A 0.166 807	67 0.237 813	4E 0.156 821	89 0.183 893
4	7C 0.156 806	AF 0.220 813	B5 0.151 826	BA 0.183 831

	0	1	2	3
0	60 0.015	B6 0.030	89 0.014	83 0.015
1	E2 0.006	67 0.010	34 0.006	9A 0.010
2	63 0.005	D0 0.009	F2 0.006	52 0.009
3	08 0.005	F7 0.009	8A 0.006	15 0.009
4	7A 0.005	C9 0.009	52 0.005	7A 0.008

(Left) Using CPA and (RIght) using DOM with Hamming Weight model



Correct key hypothesis (marked in green) vs other key guesses (plotted in gray) are show above. Each plot corresponds to one byte of the round key.

As you can see the X-axis (Time) is showing between 600 and 1000 as RK0 is only being used during this time frame.

Finding RK1 -

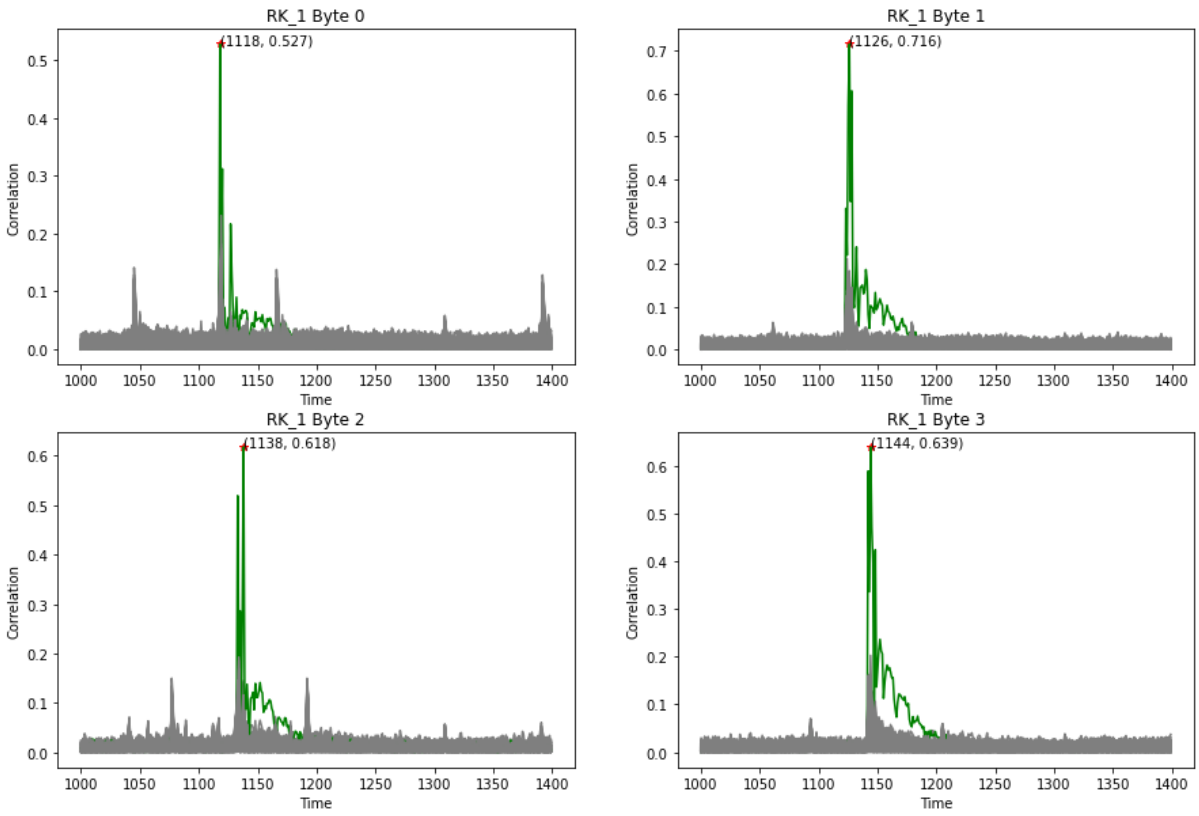
In Hexa form - [6E, 6B, DB, 7A]

In Decimal form - [110, 107, 219, 122]

	0	1	2	3
0	6E 0.527 1118	6B 0.716 1126	DB 0.618 1138	7A 0.639 1144
1	B0 0.231 1119	07 0.213 1124	17 0.225 1134	79 0.203 1144
2	40 0.205 1119	CD 0.184 1126	CE 0.196 1134	7F 0.161 1142
3	3F 0.200 1119	49 0.173 1126	F7 0.192 1134	46 0.160 1144
4	70 0.182 1119	39 0.168 1124	2E 0.186 1134	33 0.156 1142

	0	1	2	3
0	6E 0.013	6B 0.029	DB 0.013	7A 0.018
1	B0 0.009	D2 0.009	87 0.010	C3 0.008
2	9F 0.007	CD 0.009	17 0.009	E5 0.008
3	E5 0.007	EC 0.008	2E 0.009	E2 0.007
4	40 0.007	BC 0.008	CE 0.009	9F 0.006

(Left) Using CPA and (RIght) using DOM with Hamming Weight model



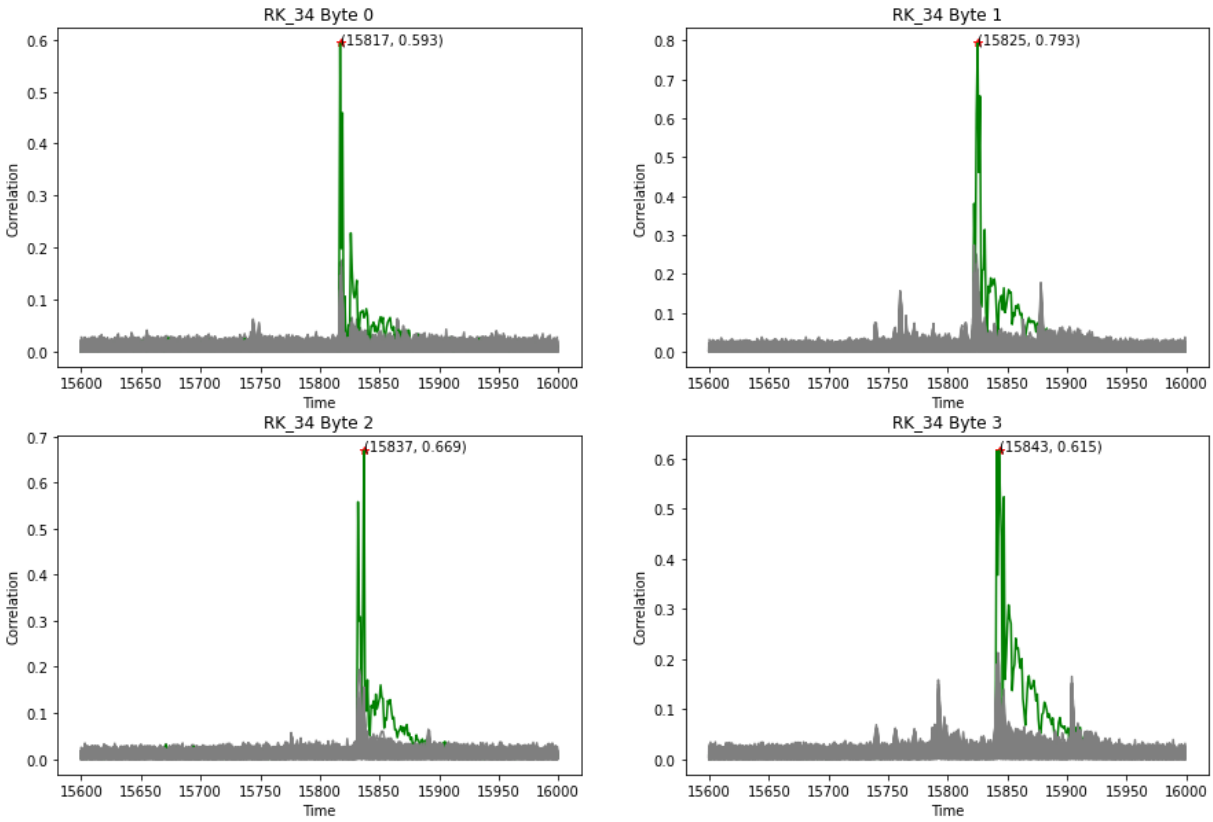
Correct key hypothesis (marked in green) vs other key guesses (plotted in gray) are show above. Each plot corresponds to one byte of the round key

2. Round keys used in the last round (round 18) in the Encryption function:
   Finding RK34 -
   In Hexa form - [BB, 79, 70, 2A]
   In Decimal form - [187, 121, 112, 42]

	0	1	2	3
0	BB 0.593 15817	79 0.793 15825	70 0.669 15837	2A 0.615 15843
1	B8 0.177 15819	BE 0.274 15822	73 0.194 15833	33 0.212 15842
2	A1 0.173 15818	40 0.251 15824	6C 0.149 15837	13 0.189 15842
3	7C 0.167 15817	70 0.227 15824	4C 0.146 15837	FF 0.189 15841
4	FB 0.164 15818	A8 0.226 15824	B7 0.146 15832	D3 0.186 15842

	0	1	2	3
0	BB 0.016	79 0.030	70 0.014	2A 0.015
1	39 0.006	A8 0.010	73 0.007	FB 0.009
2	B8 0.005	06 0.009	AB 0.006	33 0.009
3	D3 0.005	75 0.009	23 0.006	BC 0.008
4	AF 0.005	70 0.009	A7 0.006	03 0.008

(Left) Using CPA and (RIght) using DOM with Hamming Weight model



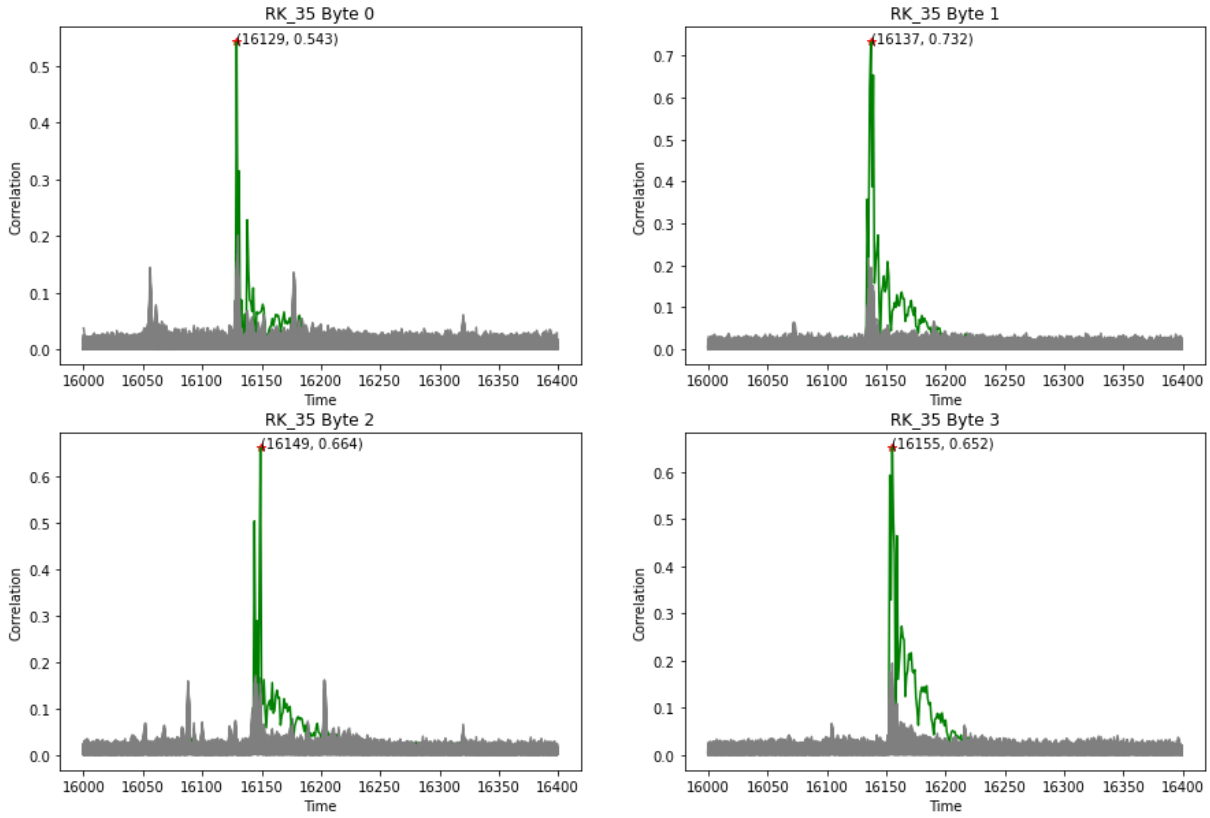
Correct key hypothesis (marked in green) vs other key guesses (plotted in gray) are show above. Each plot corresponds to one byte of the round key

Finding RK35 -
In Hexa form - [B3, 68, BD, 41]
In Decimal form - [179, 104, 189, 65]

	0	1	2	3
0	B3 0.543 16129	68 0.732 16137	BD 0.664 16149	41 0.652 16155
1	6D 0.213 16130	04 0.215 16135	71 0.210 16145	42 0.194 16155
2	E2 0.201 16130	CE 0.195 16137	48 0.193 16145	44 0.176 16153
3	9D 0.196 16130	4A 0.190 16137	91 0.186 16145	7D 0.162 16155
4	2D 0.184 16130	98 0.167 16137	A8 0.186 16145	F5 0.160 16155

	0	1	2	3
0	B3 0.013	68 0.029	BD 0.012	41 0.018
1	6D 0.008	D1 0.009	71 0.009	F8 0.009
2	42 0.007	CE 0.009	91 0.009	DE 0.008
3	38 0.007	4A 0.008	21 0.009	D9 0.006
4	52 0.007	BF 0.008	A8 0.008	9D 0.006

(Left) Using CPA and (RIght) using DOM with Hamming Weight model



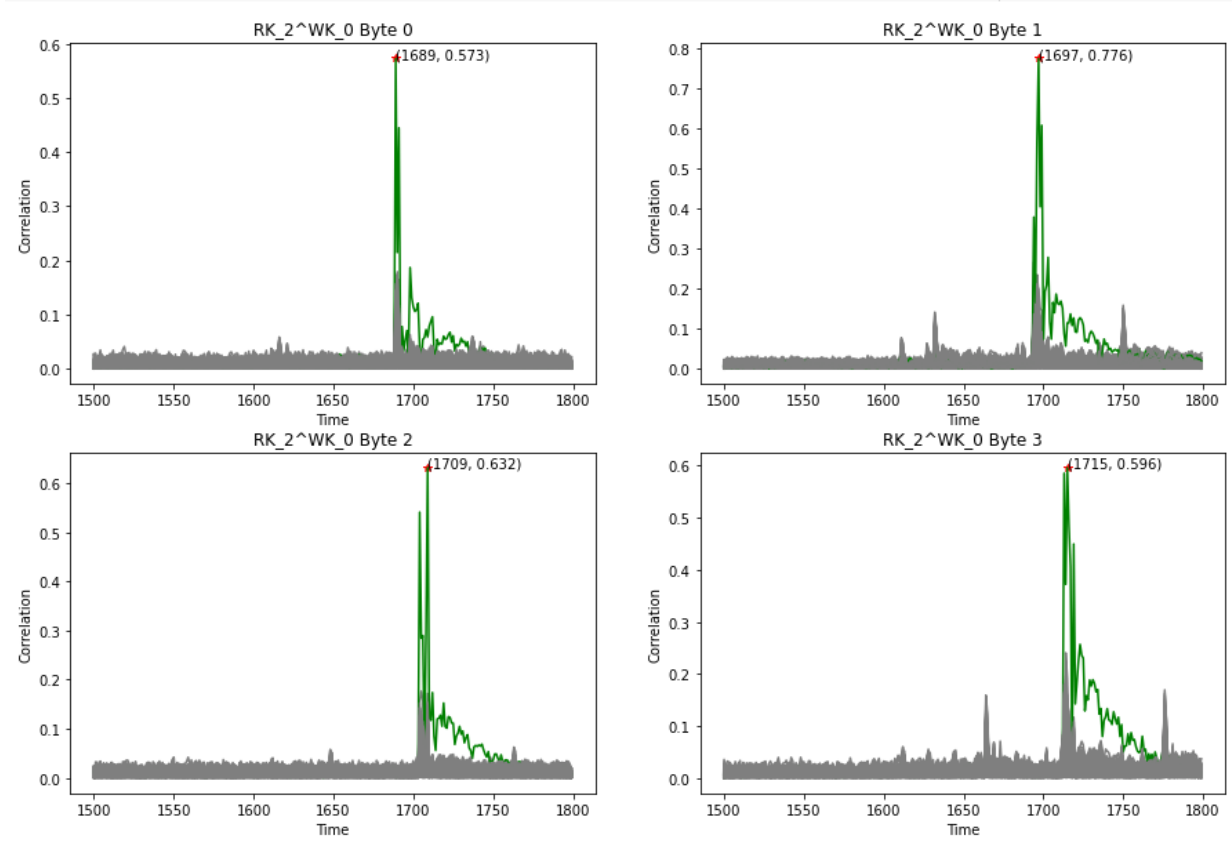
Correct key hypothesis (marked in green) vs other key guesses (plotted in gray) are show above. Each plot corresponds to one byte of the round key

3. Round keys for the second round masked by the whitening keys:
   Finding RK2 ⊕ WK0 -
   In Hexa form - [87, F3, 6A, 67]
   In Decimal form - [135, 243, 106, 103]

	0	1	2	3
0	87 0.573 1689	F3 0.776 1697	6A 0.632 1709	67 0.596 1715
1	9D 0.179 1690	34 0.266 1694	69 0.176 1705	7E 0.240 1714
2	C7 0.174 1690	CA 0.235 1696	76 0.153 1709	5E 0.196 1714
3	84 0.173 1689	22 0.216 1696	AD 0.152 1704	4B 0.188 1714
4	40 0.173 1689	FA 0.212 1696	56 0.148 1709	8A 0.180 1713

	0	1	2	3
0	87 0.573	F3 0.776	6A 0.632	67 0.596
1	9D 0.179	34 0.266	69 0.176	7E 0.240
2	C7 0.174	CA 0.235	76 0.153	5E 0.196
3	84 0.173	22 0.216	AD 0.152	4B 0.188
4	40 0.173	FA 0.212	56 0.148	8A 0.180

(Left) Using CPA and (RIght) using DOM with Hamming Weight model



Correct byte hypothesis (marked in green) vs other byte guesses (plotted in gray) are show above. Each plot corresponds to one byte of the whitened round key

Finding RK3 ⊕ WK1 -

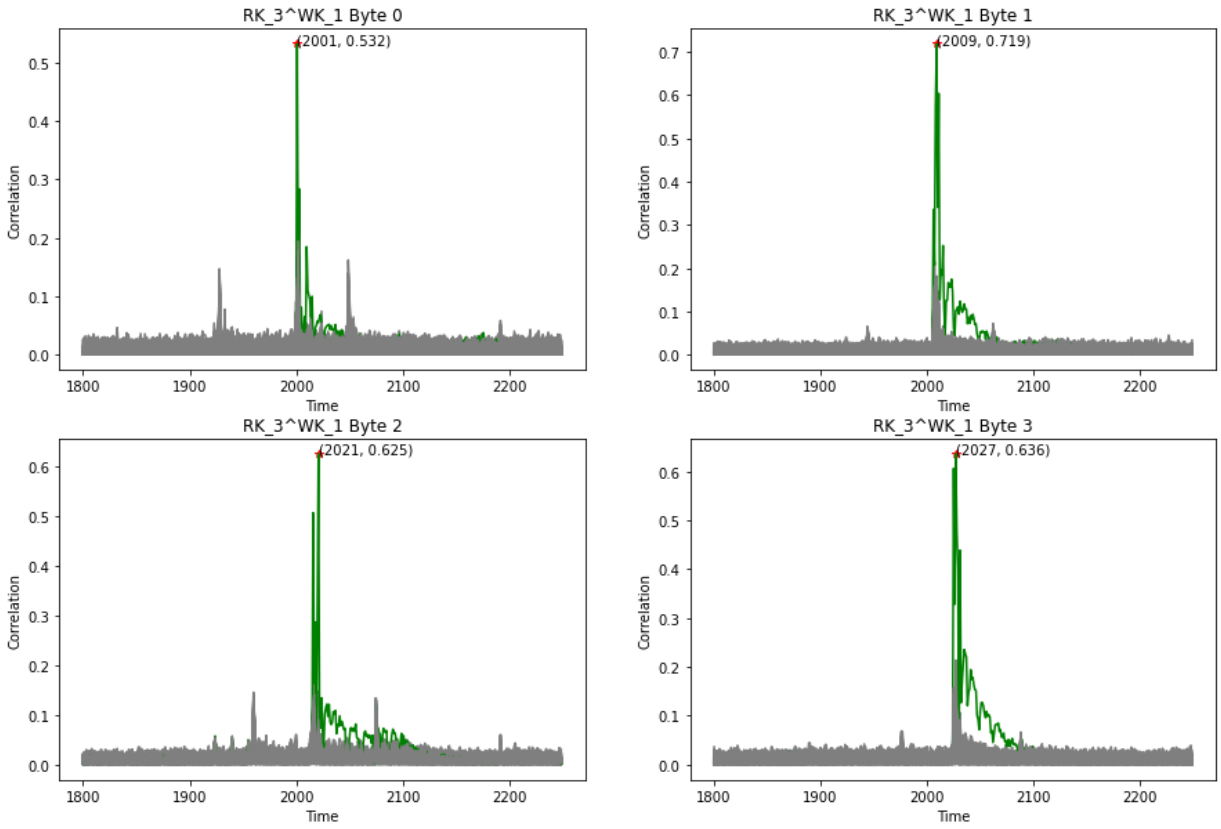
In Hexa form - [C7, C3, F1, A8]

In Decimal form - [199, 195, 241, 168]

	0	1	2	3
0	C7 0.532 2001	C3 0.719 2009	F1 0.625 2021	A8 0.636 2027
1	19 0.202 2002	AF 0.214 2007	3D 0.220 2017	AB 0.214 2027
2	E9 0.194 2002	65 0.182 2009	04 0.187 2017	94 0.177 2027
3	96 0.188 2002	E1 0.172 2009	E4 0.184 2017	1C 0.165 2027
4	99 0.182 2002	C8 0.161 2007	DD 0.181 2017	58 0.159 2027

	0	1	2	3
0	C7 0.014	C3 0.028	F1 0.013	A8 0.018
1	19 0.008	7A 0.009	E4 0.009	11 0.008
2	26 0.007	65 0.009	3D 0.009	37 0.007
3	36 0.007	14 0.008	04 0.009	74 0.006
4	E9 0.007	E1 0.008	AD 0.009	30 0.006

(Left) Using CPA and (RIght) using DOM with Hamming Weight model



Correct byte hypothesis (marked in green) vs other byte guesses (plotted in gray) are show above. Each plot corresponds to one byte of the whitened round key

4. For our power analysis, we used both CPA and DOM to get the round keys. We focussed mostly on CPA as it is a stronger attack and gave a more distinguishable result for all bytes of keys than DOM. DOM is faster as can be seen below but the difference between first row and second is not well separated for some bytes reducing our confidence in its answer. CPA and DOM with Hamming weight power model was used for the attacks. We couldn't use DOM by taking the difference with respect to only one bit as it didn't give the right results even with all the traces.

```
## With CPA
roundkey0_guess, roundkey0_Rmatrix, roundkey0_printable = getroundkey_CPA(startTime = 600, e
```

	0	1	2	3
0	60 0.581	B6 0.782	89 0.640	83 0.612
1	63 0.183	71 0.259	95 0.169	9A 0.232
2	20 0.178	8F 0.248	8A 0.160	7A 0.183
3	7A 0.166	67 0.237	4E 0.156	89 0.183
4	7C 0.156	AF 0.220	B5 0.151	BA 0.183

```
time: 14min 3s (started: 2022-09-03 09:05:28 +05:30)
```

```
## With DOM
roundkey0_guess2, roundkey0_MeanDiffs, roundkey0_printable2 = getroundkey_DOM_HW(startTime =
```

	0	1	2	3
0	60 0.015	B6 0.030	89 0.014	83 0.015
1	E2 0.006	67 0.010	34 0.006	9A 0.010
2	63 0.005	D0 0.009	F2 0.006	52 0.009
3	08 0.005	F7 0.009	8A 0.006	15 0.009
4	7A 0.005	C9 0.009	52 0.005	7A 0.008

```
time: 2min 25s (started: 2022-09-03 09:19:32 +05:30)
```

Changes from the Template code:
We have used the `pearsonr` function in `scipy.stats` to calculate the correlation in the CPA attack between the columns of the Hamming weight matrix and the Traces.

We chose our intermediate function based on our T-table implementation of Clefia-128 and we have a 32-bit output for each input byte. The inputs to the T-table are the table number and Plaintext xored with Key. The trace points with zero variance are given a default value of zero to avoid getting NaN values while calculating correlation.
We have retrieved all the keys by performing the CPA attack byte by byte i.e., iterating over the possible 256 values for each byte of a round key and then taking the maximum correlated value. We also verified these values by performing the DOM attack.

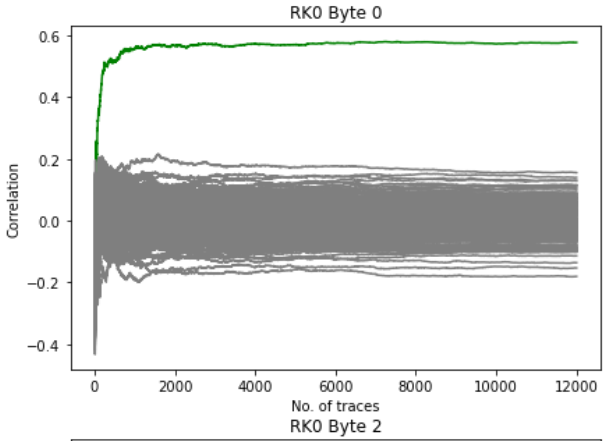
The following are the time frames where we searched for the respected round keys or Xor-keys:
1. Round key 0 - [600, 1000]
2. Round key 1 - [1000, 1400]
3. Round key 34 - [15600, 16000]
4. Round key 35 - [16000, 16400]
5. RK2 ^ WK0 - [1500, 1800]
6. RK3 ^ WK1 - [1800, 2250]

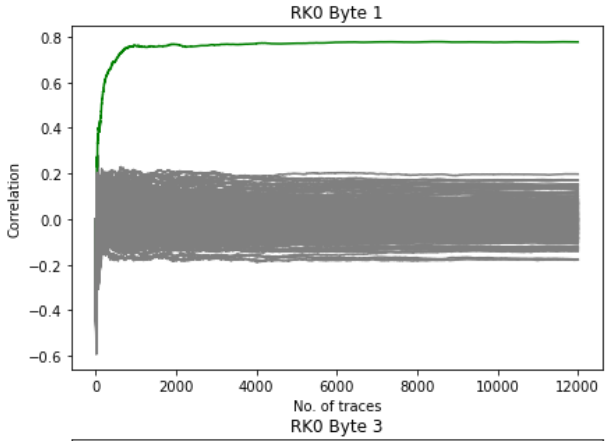
We have finalized on searching these time frames for the respective keys after close examination of the traces provided.

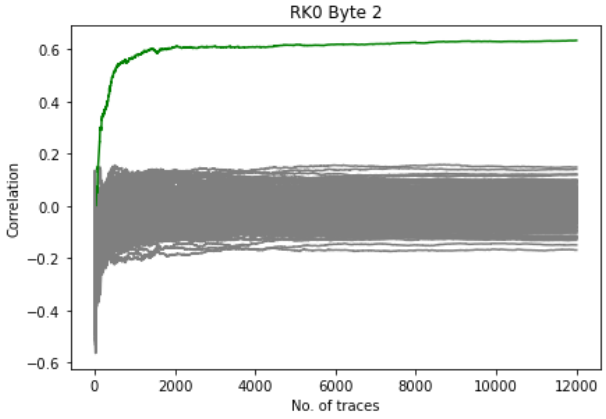
Confidence in our key guesses:

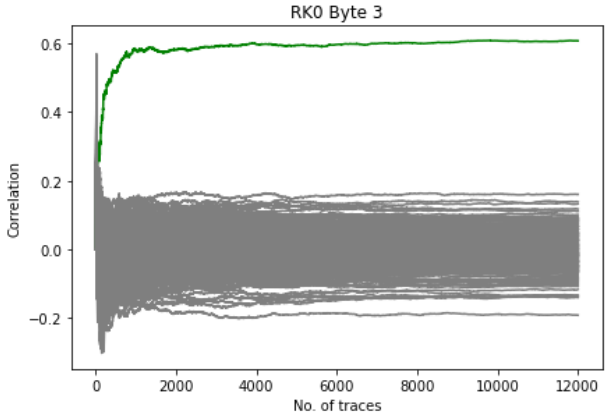
Correlation vs Number of traces for RK0:

Each plot consists of 256 possible values for each byte of key; the correct key is marked in green color which stands apart from the rest of the values. We also note that the correlation reaches

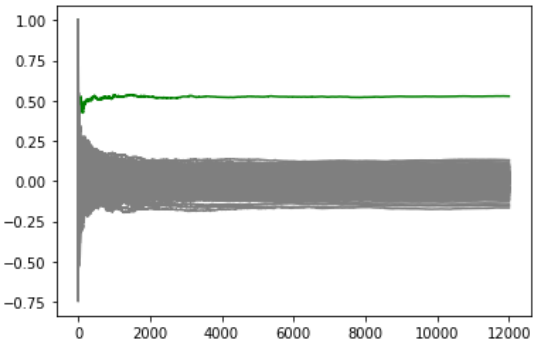




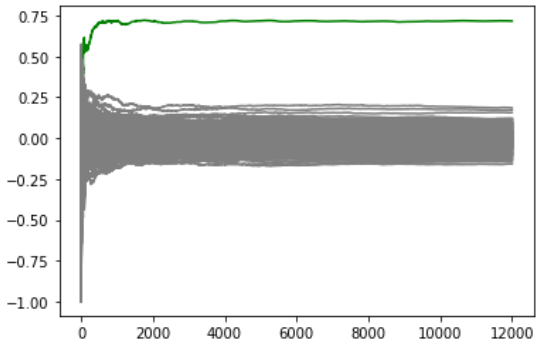




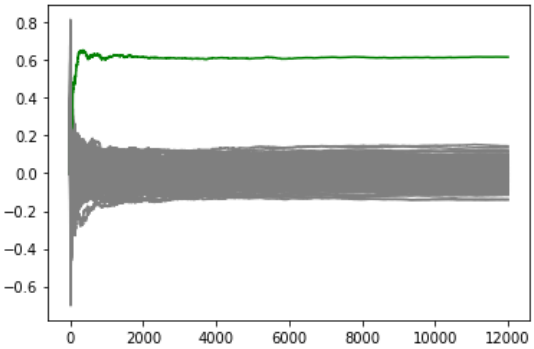
Correlation vs Number of traces for RK1:



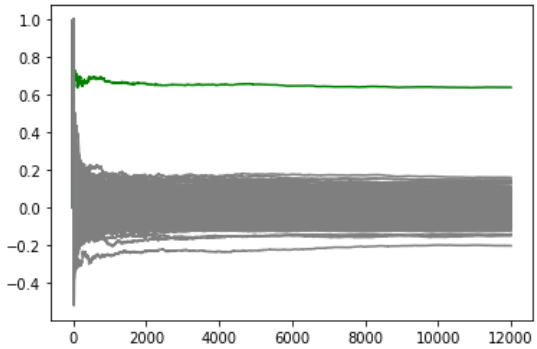
Byte 0



Byte 1

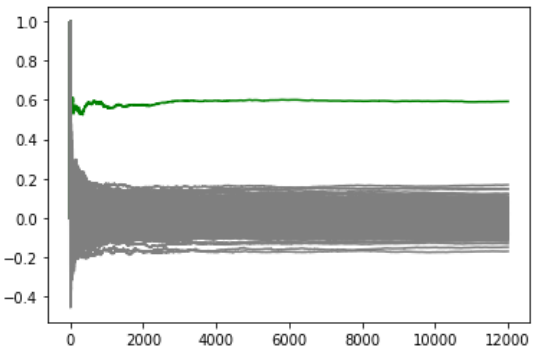


Byte 2

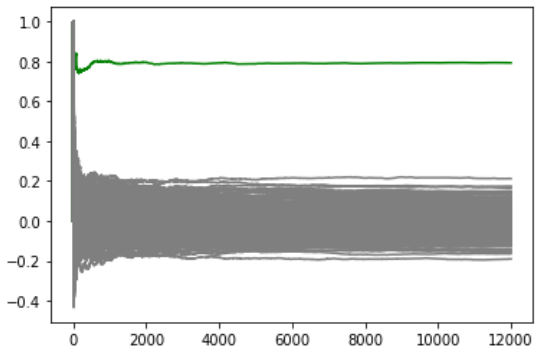


Byte 3

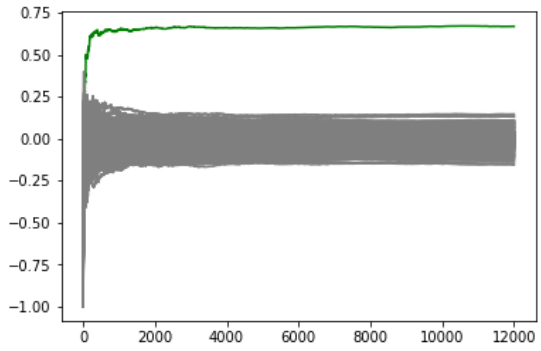
Correlation vs Number of traces for RK34:



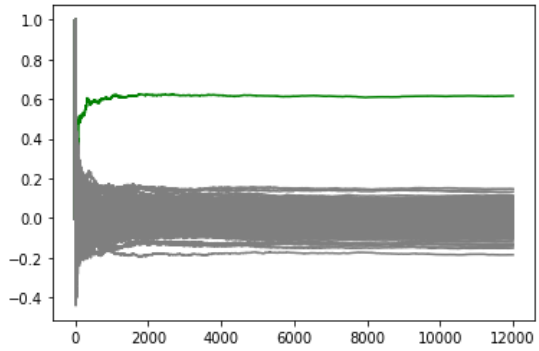
Byte 0



Byte 1

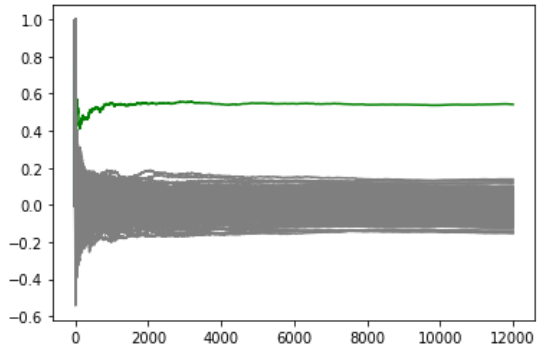


Byte 2

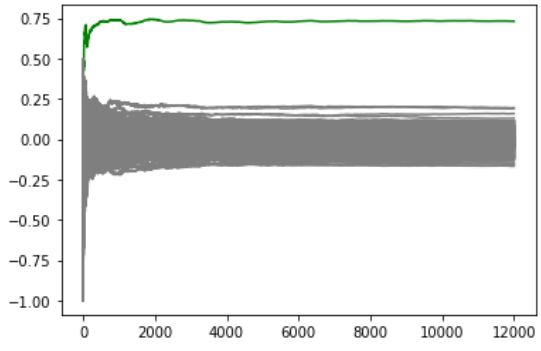


Byte 3

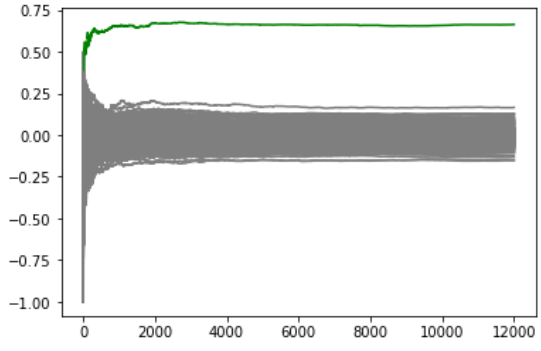
Correlation vs Number of traces fo RK35:



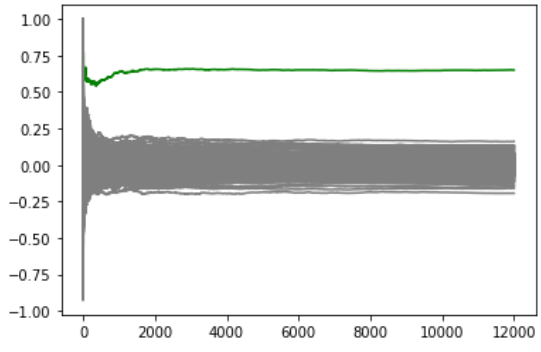
Byte 0



Byte 1

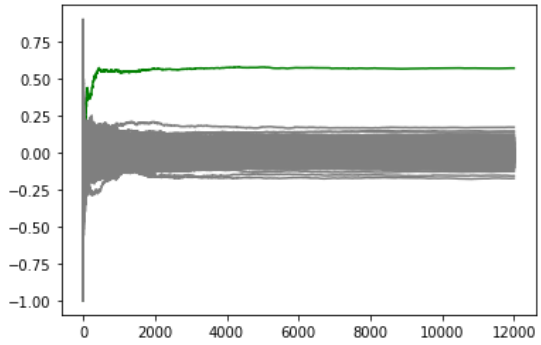


Byte 2

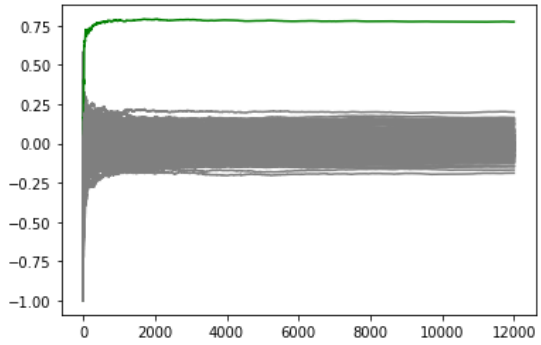


Byte 3

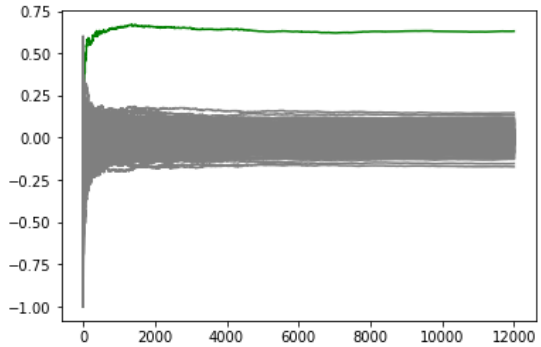
Correlation vs Number of trace for RK2^WK0:



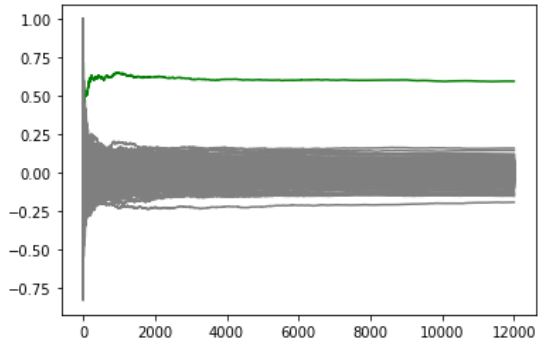
Byte 0



Byte 1

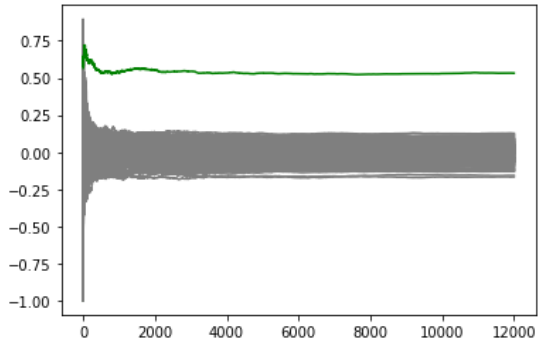


Byte 2

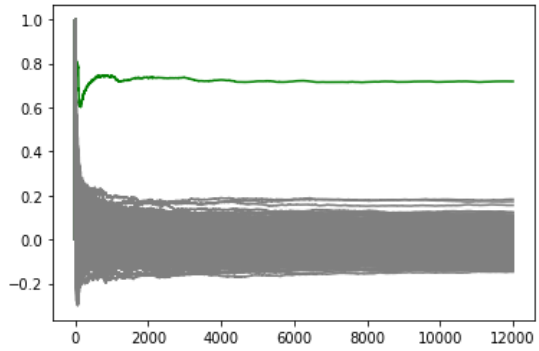


Byte 3

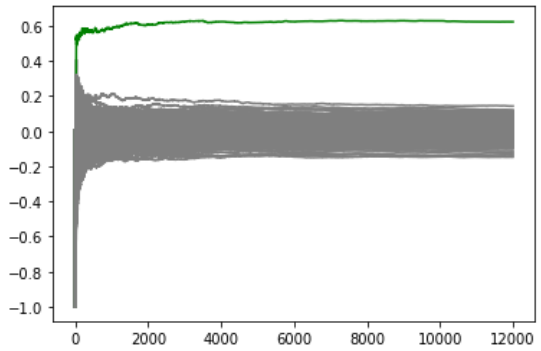
Correlation vs Number of traces for RK3^WK1:



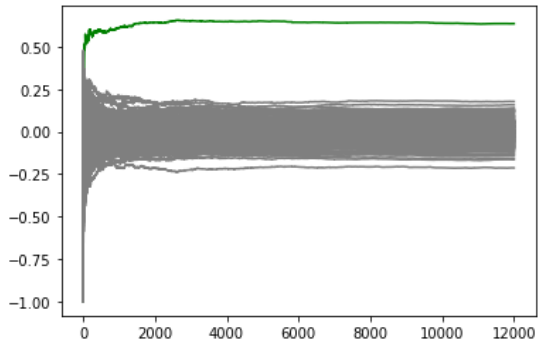
Byte 0



Byte 1



Byte 2



Byte 3