Unit 8 - Week 6

assignment 6

The due date for submitting this assignment has passed. Due on 2019-03-13, 23:59 IST.
As per our records you have not submitted this assignment.

Problem Statement

In this assignment you have to write the Difference of Mean (DoM) analysis codes on simulated power traces. The trace files are supplied here along with the corresponding ciphertext files. The traces are compressed using the trick mentioned in the video. There are total 3 input files:

i. CIPHERFILE.dat: Ciphertext file.

ii. SAMPLEFILE.dat: Compressed trace file. One may observe that the ciphertexts for which the target byte value (in the ciphertext) is same, always goes to the same bin. Here the traces are compressed utilizing the fact that only 256 values are possible for the corresponding ciphertext byte. We also maintain a file to store the number of times each byte-value appears.

iii. SAMPLEFREQFILE.dat: Number of times a trace corresponding to a specific byte has appeared.
You need to do the following:

i. Download the “DOM_simulate_wrapper.c” code.
ii. All the necessary functions are already supplied in the code. You just need to update three functions: “UpdateBin0”, “UpdateBin1” and “GetKeyBias”.
iii. Update variable “SumBin0”, “CountBin0” in the “UpdateBin0” function.
iv. Update variable “SumBin1”, “CountBin1” in the “UpdateBin1” function.
v. Update variable “meandiff” in the “GetKeyBias” function.
vi. If everything is done correctly, you should recover the correct key byte.

Now, answer the multiple choice questions in the portal.

1) Choose the correct statement to calculate SumBin0 for Bin 0 recursively

   a. SumBin0[i] += Sample[cipherCount][i];
   b. SumBin0[i] += FreqSample[cipherCount + i];
   c. SumBin0[i] += Sample[FreqSample[cipherCount]][i];
   d. SumBin0[i] += FreqSample[cipherCount + 1];

   No, the answer is incorrect.
   Score: 0
   Accepted Answers:
   a.

2) Choose the correct statement to calculate CountBin0 for Bin 0 recursively

   a. CountBin0 += Sample[cipherCount][i];
   b. CountBin0 += FreqSample[cipherCount];
   c. CountBin0 += FreqSample[Sample[cipherCount][i]]; 
   d. CountBin0 += Sample[cipherCount][i];

   No, the answer is incorrect.
   Score: 0
   Accepted Answers:
3) Choose the correct statement to calculate SumBin1 for Bin 1 recursively

- a. $\text{SumBin1}[i] += \text{Sample[cipherCount}][i]$;
- b. $\text{SumBin1}[i] += \text{FreqSample[cipherCount + i]}$;
- c. $\text{SumBin1}[i] += \text{Sample[FreqSample[cipherCount + 1]}][i]$;
- d. $\text{SumBin1}[i] += \text{Sample[cipherCount + 1]}[i]$;

No, the answer is incorrect.
Score: 0
Accepted Answers: 

4) Choose the correct statement to calculate CountBin1 for Bin 1 recursively

- a. $\text{CountBin1} += \text{Sample[cipherCount}][i]$;
- b. $\text{CountBin1} += \text{FreqSample[cipherCount]}$;
- c. $\text{CountBin1} += \text{FreqSample[cipherCount + 1]}$;
- d. $\text{CountBin1} += \text{Sample[cipherCount + 1]}[i]$;

No, the answer is incorrect.
Score: 0
Accepted Answers: 

5) Choose the correct statement to calculate meanDiff (difference in mean of Bin and Bin 1)

- a. $\text{meanDiff} = (\text{SumBin1}[i] / \text{CountBin1}) - (\text{SumBin0}[i] / \text{CountBin0})$;
- b. $\text{meanDiff} = (\text{SumBin0}[i] + \text{SumBin1}[i]) / (\text{CountBin0} + \text{CountBin1})$;
- c. $\text{meanDiff} = (\text{SumBin0}[i] * 1.0 / (\text{CountBin0}) - (\text{SumBin1}[i] 1.0) / \text{CountBin1})$;
- d. $\text{meanDiff} = (\text{SumBin1}[i] * \text{CountBin1}) / (\text{SumBin0}[i] * \text{CountBin0})$;

No, the answer is incorrect.
6) In this experiment, we will be targeting the 3rd byte of the AES state. You may observe that the TARGETBYTE variable here is set to 3. The correct keybyte value obtained is:

   a. c4
   b. 86
   c. 01
   d. a8

No, the answer is incorrect.
Score: 0
Accepted Answers: c.