VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Analysis and Audit

J-COMPONENT

REVIEW-3

NAME – GUNJAN KUMAR

REGISTRATION NO. – 18BIT0070

GITHUB LINK - https://github.com/Gunjan2202/18BIT0070

Demo of the running project(2min length only):https://youtu.be/z0bK9h3Qz10

Video of Individual work: https://drive.google.com/drive/folders/1YbuFm1lgmPuwSQdq-2meUBISRy-1Y6rS?usp=sharing

1. <u>Comparison of our cryptographic model with the models used in survey paper</u>:

We have used paillier encryption method which is a homomorphic encryption technique in our project. This technique enables us to perform operation on encrypted data and the generated result is same as the result that is obtained when the operation is performed on normal data.

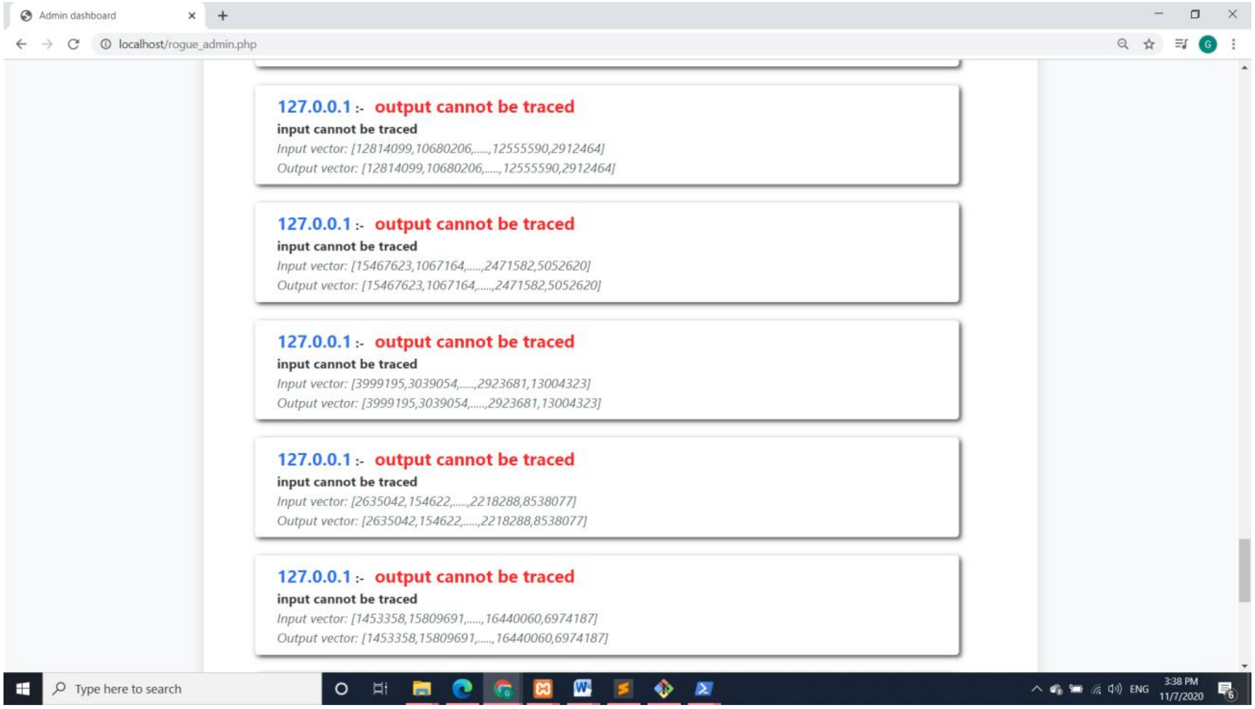
Due to this, **even the server is not able to get hold of our data** which indeed increases our privacy a lot unlike the **traditional encryption model which provide security from third party only** while the **server has the knowledge of all our data as they have the key for decrypting** the data. The **data can be used for eavesdropping or even voice-mimicking.**

A comparison of the traditional and our way of encryption is shown below:

In the traditional way all the data are stored in the database. I have tried to recreate the same scenario.

- **<u>When we use homomorphism (our model):</u>**

The **screenshot below shows the data fetch from the database at the server side**. It is clear that the input and the output vector are in encrypted from and hence the people handling the data at the sever side are unable to trace the output out of the input and the output vector.



127.0.0.1 :- output cannot be traced
input cannot be traced
Input vector: [12814099,10680206,.....,12555590,2912464]
Output vector: [12814099,10680206,.....,12555590,2912464]

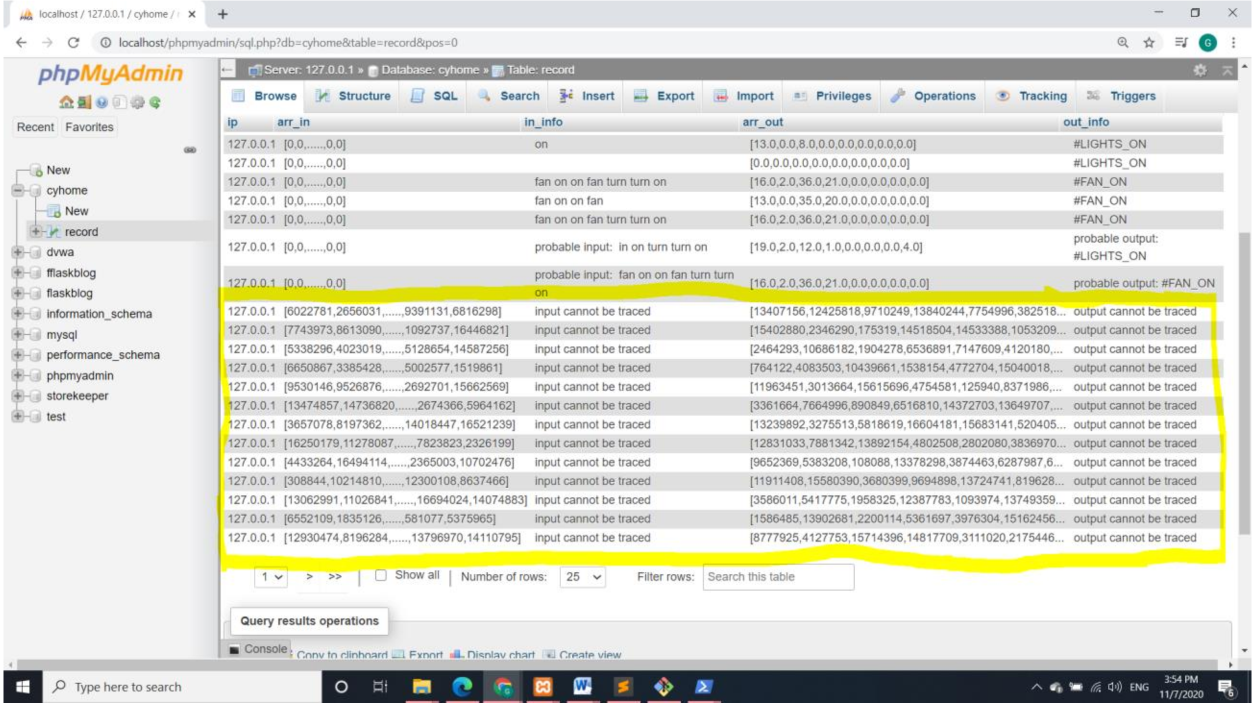
127.0.0.1 :- output cannot be traced
input cannot be traced
Input vector: [15467623,1067164,.....,2471582,5052620]
Output vector: [15467623,1067164,.....,2471582,5052620]

127.0.0.1 :- output cannot be traced
input cannot be traced
Input vector: [3999195,3039054,.....,2923681,13004323]
Output vector: [3999195,3039054,.....,2923681,13004323]

127.0.0.1 :- output cannot be traced
input cannot be traced
Input vector: [2635042,154622,.....,2218288,8538077]
Output vector: [2635042,154622,.....,2218288,8538077]

127.0.0.1 :- output cannot be traced
input cannot be traced
Input vector: [1453358,15809691,.....,16440060,6974187]
Output vector: [1453358,15809691,.....,16440060,6974187]

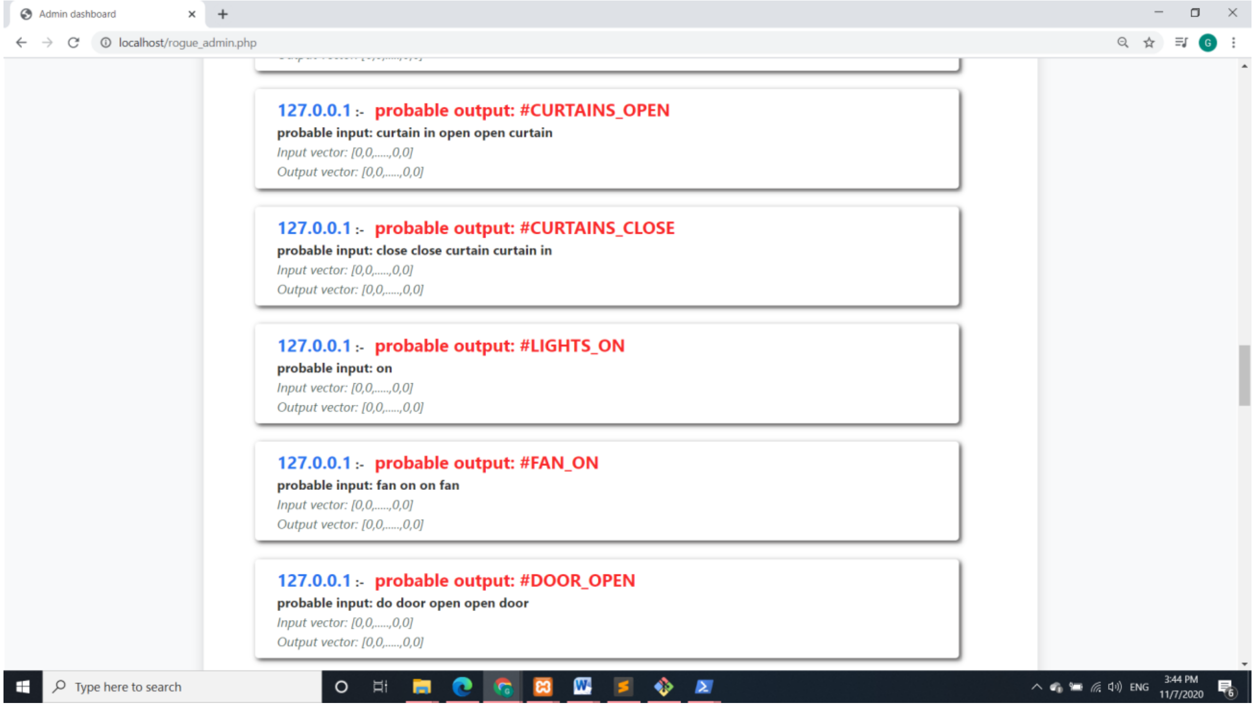
Screenshot of database:



ip	arr_in	in_info	arr_out	out_info
127.0.0.1	[0,0,......,0,0]	on	[13.0,0.0,8.0,0.0,0.0,0.0,0.0,0.0]	#LIGHTS_ON
127.0.0.1	[0,0,......,0,0]		[0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0]	#LIGHTS_ON
127.0.0.1	[0,0,......,0,0]	fan on on fan turn turn on	[16.0,2.0,36.0,21.0,0.0,0.0,0.0,0.0]	#FAN_ON
127.0.0.1	[0,0,......,0,0]	fan on on fan	[13.0,0.0,35.0,20.0,0.0,0.0,0.0,0.0]	#FAN_ON
127.0.0.1	[0,0,......,0,0]	fan on on fan turn turn on	[16.0,2.0,36.0,21.0,0.0,0.0,0.0,0.0]	#FAN_ON
127.0.0.1	[0,0,......,0,0]	probable input: in on turn turn on	[19.0,2.0,12.0,1.0,0.0,0.0,0.0,4.0]	probable output: #LIGHTS_ON
127.0.0.1	[0,0,......,0,0]	probable input: fan on on fan turn turn on	[16.0,2.0,36.0,21.0,0.0,0.0,0.0,0.0]	probable output: #FAN_ON
127.0.0.1	[6022781,2656031,......,9391131,6816298]	input cannot be traced	[13407156,12425818,9710249,13840244,7754996,382518...	output cannot be traced
127.0.0.1	[7743973,8613090,......,1092737,16446821]	input cannot be traced	[15402880,2346290,175319,14518504,14533388,1053209...	output cannot be traced
127.0.0.1	[5338296,4023019,......,5128654,14587256]	input cannot be traced	[2464293,10686182,1904278,6536891,7147609,4120180,...	output cannot be traced
127.0.0.1	[6650867,3385428,......,5002577,1519861]	input cannot be traced	[764122,4083503,10439661,1538154,4772704,15040018,...	output cannot be traced
127.0.0.1	[9530146,9526876,......,2692701,15662569]	input cannot be traced	[11963451,3013664,15615696,4754581,125940,8371986,...	output cannot be traced
127.0.0.1	[13474857,14736820,......,2674366,5964162]	input cannot be traced	[3361664,7664996,890849,6516810,14372703,13649707,...	output cannot be traced
127.0.0.1	[3657078,8197362,......,14018447,16521239]	input cannot be traced	[13239892,3275513,5818619,16604181,15683141,520405...	output cannot be traced
127.0.0.1	[16250179,11278087,......,7823823,2326199]	input cannot be traced	[12831033,7881342,13892154,4802508,2802080,3836970...	output cannot be traced
127.0.0.1	[4433264,16494114,......,2365003,10702476]	input cannot be traced	[9652369,5383208,108088,13378298,3874463,6287987,6...	output cannot be traced
127.0.0.1	[308844,10214810,......,12300108,8637466]	input cannot be traced	[11911408,15580390,3680399,9694898,13724741,819628...	output cannot be traced
127.0.0.1	[13062991,11026841,......,16694024,14074883]	input cannot be traced	[3586011,5417775,1958325,12387783,1093974,13749359...	output cannot be traced
127.0.0.1	[6552109,1835126,......,581077,5375965]	input cannot be traced	[1586485,13902681,2200114,5361697,3976304,15162456...	output cannot be traced
127.0.0.1	[12930474,8196284,......,13796970,14110795]	input cannot be traced	[8777925,4127753,15714396,14817709,3111020,2175446...	output cannot be traced

- <u>**When traditional mode of encryption is used :**</u>

It is clear from the screenshot that the input and output vector stored by the server in their database are in decrypted form , the server can easily find out what the command was by analysing the input vector as it is just a preprocessed vector containing only 0 and 1.



127.0.0.1 :- probable output: #CURTAINS_OPEN
probable input: curtain in open open curtain
Input vector: [0,0,.....,0,0]
Output vector: [0,0,.....,0,0]

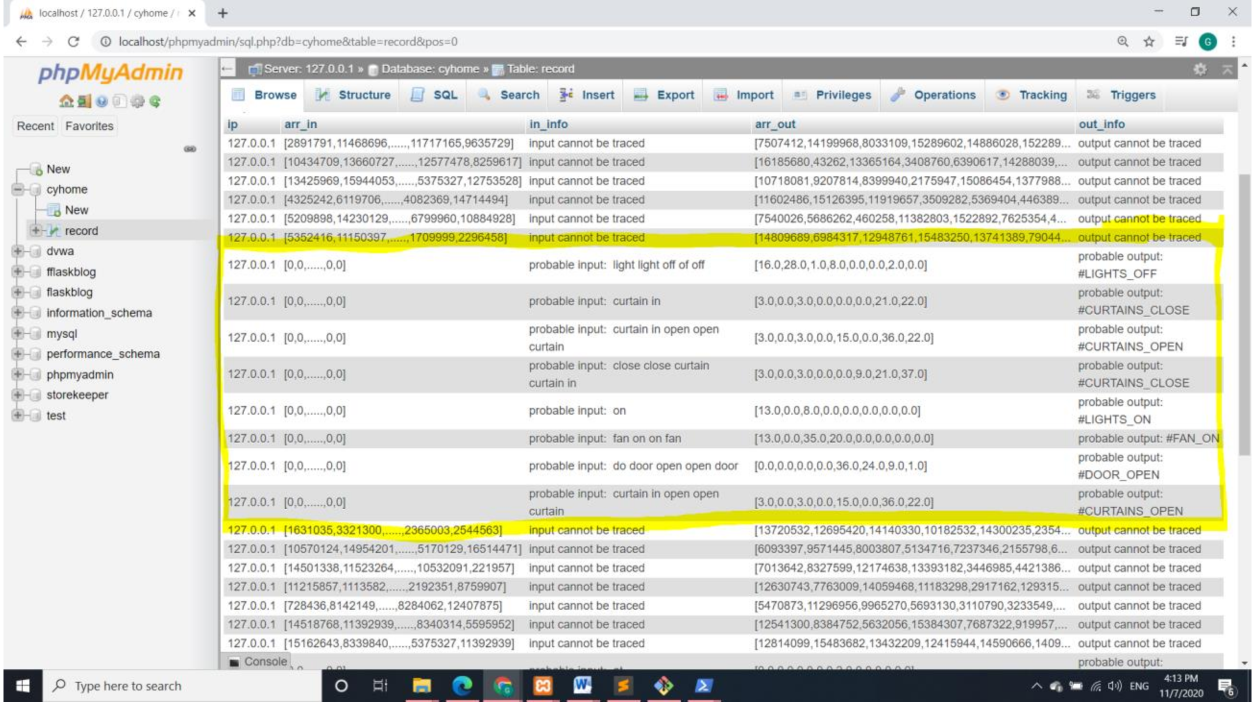
127.0.0.1 :- probable output: #CURTAINS_CLOSE
probable input: close close curtain curtain in
Input vector: [0,0,.....,0,0]
Output vector: [0,0,.....,0,0]

127.0.0.1 :- probable output: #LIGHTS_ON
probable input: on
Input vector: [0,0,.....,0,0]
Output vector: [0,0,.....,0,0]

127.0.0.1 :- probable output: #FAN_ON
probable input: fan on on fan
Input vector: [0,0,.....,0,0]
Output vector: [0,0,.....,0,0]

127.0.0.1 :- probable output: #DOOR_OPEN
probable input: do door open open door
Input vector: [0,0,.....,0,0]
Output vector: [0,0,.....,0,0]

Screenshot of Database:



ip	arr_in	in_info	arr_out	out_info
127.0.0.1	[2891791,11468696,......,11717165,9635729]	input cannot be traced	[7507412,14199968,8033109,15289602,14886028,152289...	output cannot be traced
127.0.0.1	[10434709,13660727,......,12577478,8259617]	input cannot be traced	[16185680,43262,13365164,3408760,6390617,14288039,...	output cannot be traced
127.0.0.1	[13425969,15944053,......,5375327,12753528]	input cannot be traced	[10718081,9207814,8399940,2175947,15086454,1377988...	output cannot be traced
127.0.0.1	[4325242,6119706,......,4082369,14714494]	input cannot be traced	[11602486,15126395,11919657,3509282,5369404,446389...	output cannot be traced
127.0.0.1	[5209898,14230129,......,6799960,10884928]	input cannot be traced	[7540026,5686262,460258,11382803,1522892,7625354,4...	output cannot be traced
127.0.0.1	[5352416,11150397,......,1709999,2296458]	input cannot be traced	[14809689,6984317,12948761,15483250,13741389,79044...	output cannot be traced
127.0.0.1	[0,0,......,0,0]	probable input: light light off of off	[16.0,28.0,1.0,8.0,0.0,0.0,2.0,0.0]	probable output: #LIGHTS_OFF
127.0.0.1	[0,0,......,0,0]	probable input: curtain in	[3.0,0.0,3.0,0.0,0.0,0.0,21.0,22.0]	probable output: #CURTAINS_CLOSE
127.0.0.1	[0,0,......,0,0]	probable input: curtain in open open curtain	[3.0,0.0,3.0,0.0,15.0,0.0,36.0,22.0]	probable output: #CURTAINS_OPEN
127.0.0.1	[0,0,......,0,0]	probable input: close close curtain curtain in	[3.0,0.0,3.0,0.0,0.0,9.0,21.0,37.0]	probable output: #CURTAINS_CLOSE
127.0.0.1	[0,0,......,0,0]	probable input: on	[13.0,0.0,8.0,0.0,0.0,0.0,0.0,0.0]	probable output: #LIGHTS_ON
127.0.0.1	[0,0,......,0,0]	probable input: fan on on fan	[13.0,0.0,35.0,20.0,0.0,0.0,0.0,0.0]	probable output: #FAN_ON
127.0.0.1	[0,0,......,0,0]	probable input: do door open open door	[0.0,0.0,0.0,0.0,36.0,24.0,9.0,1.0]	probable output: #DOOR_OPEN
127.0.0.1	[0,0,......,0,0]	probable input: curtain in open open curtain	[3.0,0.0,3.0,0.0,15.0,0.0,36.0,22.0]	probable output: #CURTAINS_OPEN
127.0.0.1	[1631035,3321300,......,2365003,2544563]	input cannot be traced	[13720532,12695420,14140330,10182532,14300235,2354...	output cannot be traced
127.0.0.1	[10570124,14954201,......,5170129,16514471]	input cannot be traced	[6093397,9571445,8003807,5134716,7237346,2155798,6...	output cannot be traced
127.0.0.1	[14501338,11523264,......,10532091,221957]	input cannot be traced	[7013642,8327599,12174638,13393182,3446985,4421386...	output cannot be traced
127.0.0.1	[11215857,1113582,......,2192351,8759907]	input cannot be traced	[12630743,7763009,14059468,11183298,2917162,129315...	output cannot be traced
127.0.0.1	[728436,8142149,......,8284062,12407875]	input cannot be traced	[5470873,11296956,9965270,5693130,3110790,3233549,...	output cannot be traced
127.0.0.1	[14518768,11392939,......,8340314,5595952]	input cannot be traced	[12541300,8384752,5632056,15384307,7687322,919957,...	output cannot be traced
127.0.0.1	[15162643,8339840,......,5375327,11392939]	input cannot be traced	[12814099,15483682,13432209,12415944,14590666,1409...	output cannot be traced

2. POSSIBILITY OF CRYPTANALYTIC ATTACK :

The introduction of **randomness** into Pallier-encryption ’s formula (which enables paillier encryption to produce **polyalphabetic ciphers**) makes it **almost impossible to perform brute-force attack**. The statistical distribution of encryption of 0 and 1 is presented in the graph, as follows:

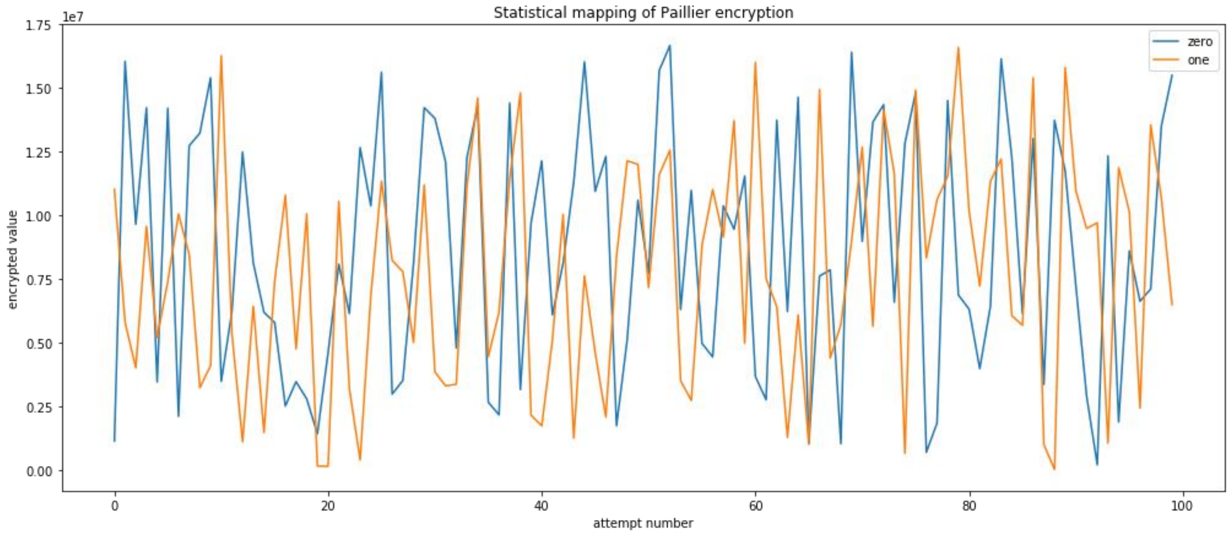
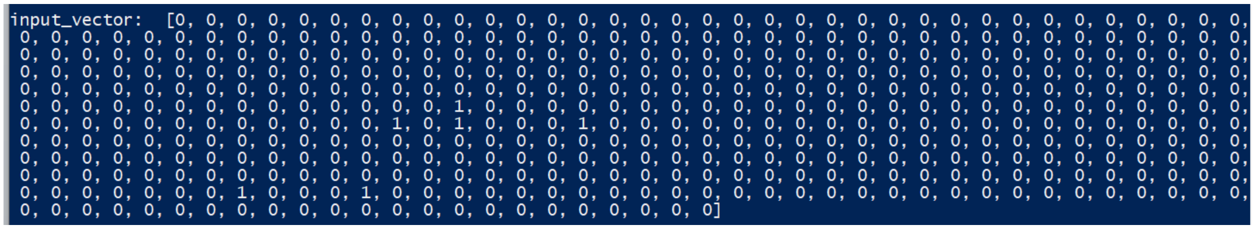


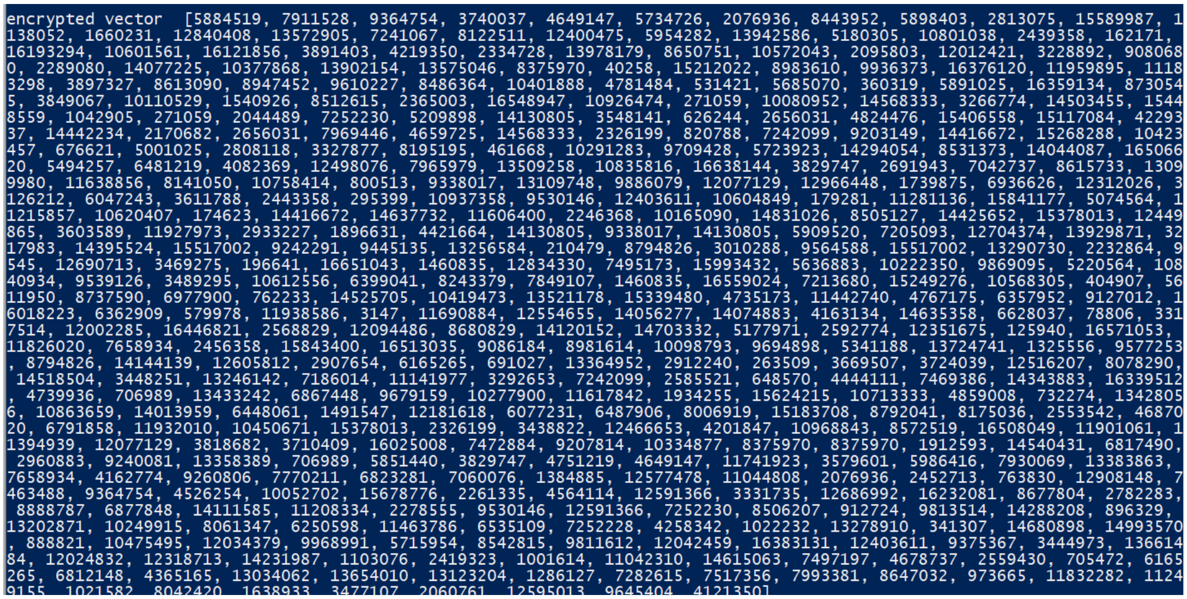
Figure : statistical distribution of encryption range for zero and one

From the figure, it is clear that there can be no distinct relationship that can be derived from the encryption of the two values. The blue graph shows that there is no pattern in the way “0” is encrypted . Also the graph shows that **the range of encrypted values lies between 10^5 to 1.75 × 10^7** . **The range of encryption is so sparse that it's almost impossible to perform crypt-analysis, thanks to addition of entropy and randomness within the Paillier encryption formula.**



```
input_vector:  [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

Figure : input vector containing 0 and 1



```
encrypted vector  [5884519, 7911528, 9364754, 3740037, 4649147, 5734726, 2076936, 8443952, 5898403, 2813075, 15589987, 1
138052, 1660231, 12840408, 13572905, 7241067, 8122511, 12400475, 5954282, 13942586, 5180305, 10801038, 2439358, 162171,
16193294, 10601561, 16121856, 3891403, 4219350, 2334728, 13978179, 8650751, 10572043, 2095803, 12012421, 3228892, 908068
0, 2289080, 14077225, 10377868, 13902154, 13575046, 8375970, 40258, 15212022, 8983610, 9936373, 16376120, 11959895, 1118
3298, 3897327, 8613090, 8947452, 9610227, 8486364, 10401888, 4781484, 531421, 5685070, 360319, 5891025, 16359134, 873054
5, 3849067, 10110529, 1540926, 8512615, 2365003, 16548947, 10926474, 271059, 10080952, 14568333, 3266774, 14503455, 1544
8559, 1042905, 271059, 2044489, 7252230, 5209898, 14130805, 3548141, 626244, 2656031, 4824476, 15406558, 15117084, 42293
37, 14442234, 2170682, 2656031, 7969446, 4659725, 14568333, 2326199, 820788, 7242099, 9203149, 14416672, 15268288, 10423
457, 676621, 5001025, 2808118, 3327877, 8195195, 461668, 10291283, 9709428, 5723923, 14294054, 8531373, 14044087, 165066
20, 5494257, 6481219, 4082369, 12498076, 7965979, 13509258, 10835816, 16638144, 3829747, 2691943, 7042737, 8615733, 1309
9980, 11638856, 8141050, 10758414, 800513, 9338017, 13109748, 9886079, 12077129, 12966448, 1739875, 6936626, 12312026, 3
126212, 6047243, 3611788, 2443358, 295399, 10937358, 9530146, 12403611, 10604849, 179281, 11281136, 15841177, 5074564, 1
1215857, 10620407, 174623, 14416672, 14637732, 11606400, 2246368, 10165090, 14831026, 8505127, 14425652, 15378013, 12449
865, 3603589, 11927973, 2933227, 1896631, 4421664, 14130805, 9338017, 14130805, 5909520, 7205093, 12704374, 13929871, 32
17983, 14395524, 15517002, 9242291, 9445135, 13256584, 210479, 8794826, 3010288, 9564588, 15517002, 13290730, 2232864, 9
545, 12690713, 3469275, 196641, 16651043, 1460835, 12834330, 7495173, 15993432, 5636883, 10222350, 9869095, 5220564, 108
40934, 9539126, 3489295, 10612556, 6399041, 8243379, 7849107, 1460835, 16559024, 7213680, 15249276, 10568305, 404907, 56
11950, 8737590, 6977900, 762233, 14525705, 10419473, 13521178, 15339480, 4735173, 11442740, 4767175, 6357952, 9127012, 1
6018223, 6362909, 579978, 11938586, 3147, 11690884, 12554655, 14056277, 14074883, 4163134, 14635358, 6628037, 78806, 331
7514, 12002285, 16446821, 2568829, 12094486, 8680829, 14120152, 14703332, 5177971, 2592774, 12351675, 125940, 16571053,
11826020, 7658934, 2456358, 15843400, 16513035, 9086184, 8981614, 10098793, 9694898, 5341188, 13724741, 1325556, 9577253
, 8794826, 14144139, 12605812, 2907654, 6165265, 691027, 13364952, 2912240, 263509, 3669507, 3724039, 12516207, 8078290,
 14518504, 3448251, 13246142, 7186014, 11141977, 3292653, 7242099, 2585521, 648570, 4444111, 7469386, 14343883, 16339512
, 4739936, 706989, 13433242, 6867448, 9679159, 10277900, 11617842, 1934255, 15624215, 10713333, 4859008, 732274, 1342805
6, 10863659, 14013959, 6448061, 1491547, 12181618, 6077231, 6487906, 8006919, 15183708, 8792041, 8175036, 2553542, 46870
20, 6791858, 11932010, 10450671, 15378013, 2326199, 3438822, 12466653, 4201847, 10968843, 8572519, 16508049, 11901061, 1
1394939, 12077129, 3818682, 3710409, 16025008, 7472884, 9207814, 10334877, 8375970, 8375970, 1912593, 14540431, 6817490,
 2960883, 9240081, 13358389, 706989, 5851440, 3829747, 4751219, 4649147, 11741923, 3579601, 5986416, 7930069, 13383863,
7658934, 4162774, 9260806, 7770211, 6823281, 7060076, 1384885, 12577478, 11044808, 2076936, 2452713, 763830, 12908148, 7
463488, 9364754, 4526254, 10052702, 15678776, 2261335, 4564114, 12591366, 3331735, 12686992, 16232081, 8677804, 2782283,
 8888787, 6877848, 14111585, 11208334, 2278555, 9530146, 12591366, 7252230, 8506207, 912724, 9813514, 14288208, 896329,
13202871, 10249915, 8061347, 6250598, 11463786, 6535109, 7252228, 4258342, 1022232, 13278910, 341307, 14680898, 14993570
, 888821, 10475495, 12034379, 9968991, 5715954, 8542815, 9811612, 12042459, 16383131, 12403611, 9375367, 3444973, 136614
84, 12024832, 12318713, 14231987, 1103076, 2419323, 1001614, 11042310, 14615063, 7497197, 4678737, 2559430, 705472, 6165
265, 6812148, 4365165, 13034062, 13654010, 13123204, 1286127, 7282615, 7517356, 7993381, 8647032, 973665, 11832282, 1124
9155, 1021582, 8042420, 1638933, 3477107, 2060761, 12595013, 9645404, 4121350]
```

Figure : Encrypted output vector

3. BRUTE FORCE ATTACK ON OUR MODEL :

Number of key-variables	:	4 (n,g,ƛ,μ)
Size of each variable	:	128 bit
TOTAL BRUTE FORCE TIME	:	422 years (considering 1 ns per value)

There are 2 keys, public key and private key, each having 2 variables and each variable is of 128 bit. And assuming that it takes 1ns for calculation, which only the supercomputer is capable of, it comes out that it will take 422 years to brute force in our system.

4. Computational analysis of our algorithm with other algorithms used in literature survey:

The encryption and decryption time of all the algorithms used in literature survey as well as my model is shown below. The encryption and decryption is performed on a data of 3748 Bytes.

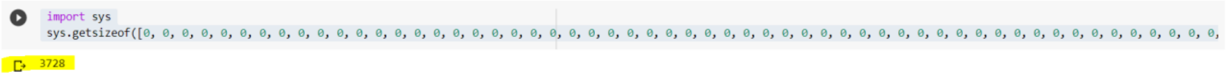
	El-Gamal **(paper 1)**	**SDC** **(paper – 3)**	**RSA** **(paper 4)**	**Paillier** **(My model)**
Encryption time **(milliseconds)**	2.710	2.001	2.010	3.023
Decryption time **(milliseconds)**	1.610	1.100	3.84	1.864
Key size **(Bytes)**	1024	N/A	1024	224

As observed from the table it is evident that SDC and El-Gamal are very good encryption technique in terms of encryption time and decryption time. And even though Paillier algorithm lags behind the other three in encryption time yet it is quite fast when it comes to decryption.

We can surely try to use other encryption techniques like SDC and El-Gamal instead of paillier in our model as they are quite fast. We will keep that as our future work.

5. Detailed computational analysis of my model:

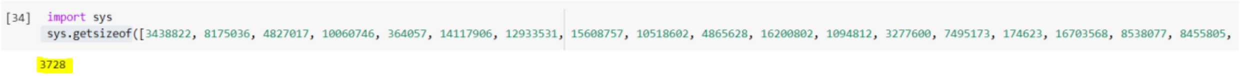
The size of input vector of length 458 is **3728 Bytes**



```
import sys
sys.getsizeof([0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

3728
```

The size of output encrypted vector of length 458 is **3748 Bytes**

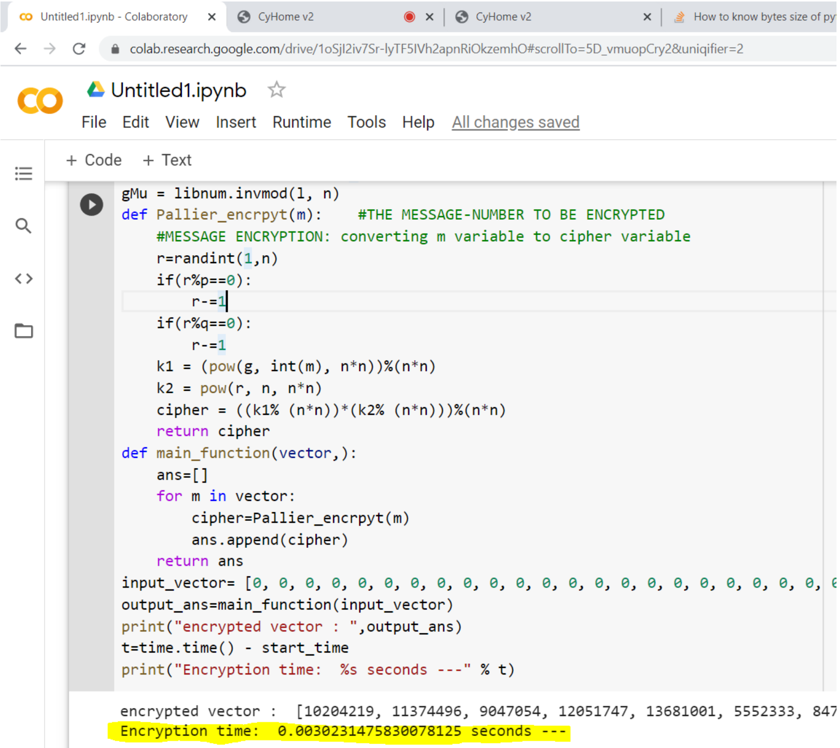


```
[34] import sys
     sys.getsizeof([3438822, 8175036, 4827017, 10060746, 364057, 14117906, 12933531, 15608757, 10518602, 4865628, 16200802, 1094812, 3277600, 7495173, 174623, 16703568, 8538077, 8455805,

3728
```

Key size : **224 bits**

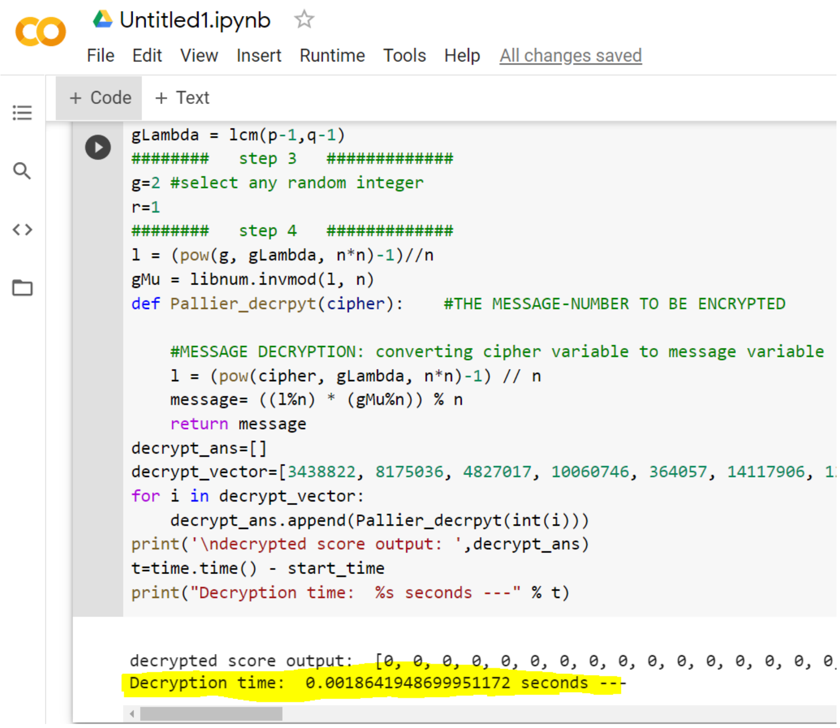
Encryption time: **0.0030232 seconds** or **3.0232 milliseconds**


Untitled1.ipynb - Colaboratory
CyHome v2
CyHome v2
How to know bytes size of py
colab.research.google.com/drive/1oSjI2iv7Sr-lyTF5IVh2apnRiOkzemhO#scrollTo=5D_vmuopCry2&uniqifier=2
Untitled1.ipynb
File Edit View Insert Runtime Tools Help All changes saved
+ Code + Text

```
gMu = libnum.invmod(l, n)
def Pallier_encrpyt(m):    #THE MESSAGE-NUMBER TO BE ENCRYPTED
    #MESSAGE ENCRYPTION: converting m variable to cipher variable
    r=randint(1,n)
    if(r%p==0):
        r-=1
    if(r%q==0):
        r-=1
    k1 = (pow(g, int(m), n*n))%(n*n)
    k2 = pow(r, n, n*n)
    cipher = ((k1% (n*n))*(k2% (n*n)))%(n*n)
    return cipher
def main_function(vector,):
    ans=[]
    for m in vector:
        cipher=Pallier_encrpyt(m)
        ans.append(cipher)
    return ans
input_vector= [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
output_ans=main_function(input_vector)
print("encrypted vector : ",output_ans)
t=time.time() - start_time
print("Encryption time:  %s seconds ---" % t)
```

```
encrypted vector :  [10204219, 11374496, 9047054, 12051747, 13681001, 5552333, 847
Encryption time:  0.0030231475830078125 seconds ---
```

Decryption Time: **0.001864 seconds** or **1.864 milliseconds**



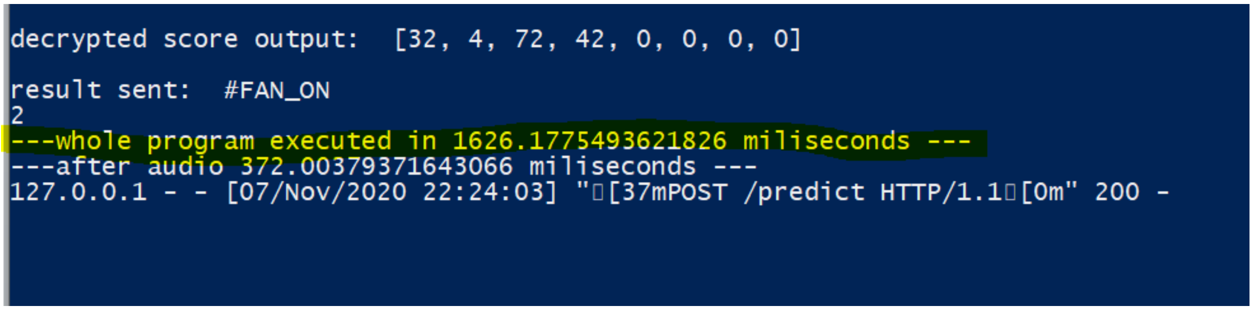
```
gLambda = lcm(p-1,q-1)
########    step 3    #############
g=2 #select any random integer
r=1
########    step 4    #############
l = (pow(g, gLambda, n*n)-1)//n
gMu = libnum.invmod(l, n)
def Pallier_decrpyt(cipher):    #THE MESSAGE-NUMBER TO BE ENCRYPTED

    #MESSAGE DECRYPTION: converting cipher variable to message variable
    l = (pow(cipher, gLambda, n*n)-1) // n
    message= ((l%n) * (gMu%n)) % n
    return message
decrypt_ans=[]
decrypt_vector=[3438822, 8175036, 4827017, 10060746, 364057, 14117906, 1
for i in decrypt_vector:
    decrypt_ans.append(Pallier_decrpyt(int(i)))
print('\ndecrypted score output: ',decrypt_ans)
t=time.time() - start_time
print("Decryption time:  %s seconds ---" % t)
```

```
decrypted score output:  [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
Decryption time:  0.0018641948699951172 seconds ---
```

Running time of whole integrated project:

The whole integrated model processes the whole thing , right from converting audio to text , text to encrypted form , sending it to server , processing it and performing its task in 1.62 seconds.



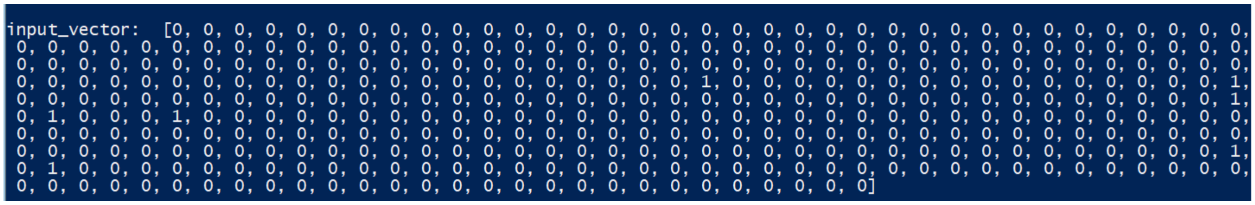
```
decrypted score output:  [32, 4, 72, 42, 0, 0, 0, 0]

result sent:  #FAN_ON
2
---whole program executed in 1626.1775493621826 miliseconds ---
---after audio 372.00379371643066 miliseconds ---
127.0.0.1 - - [07/Nov/2020 22:24:03] "[37mPOST /predict HTTP/1.1[0m" 200 -
```

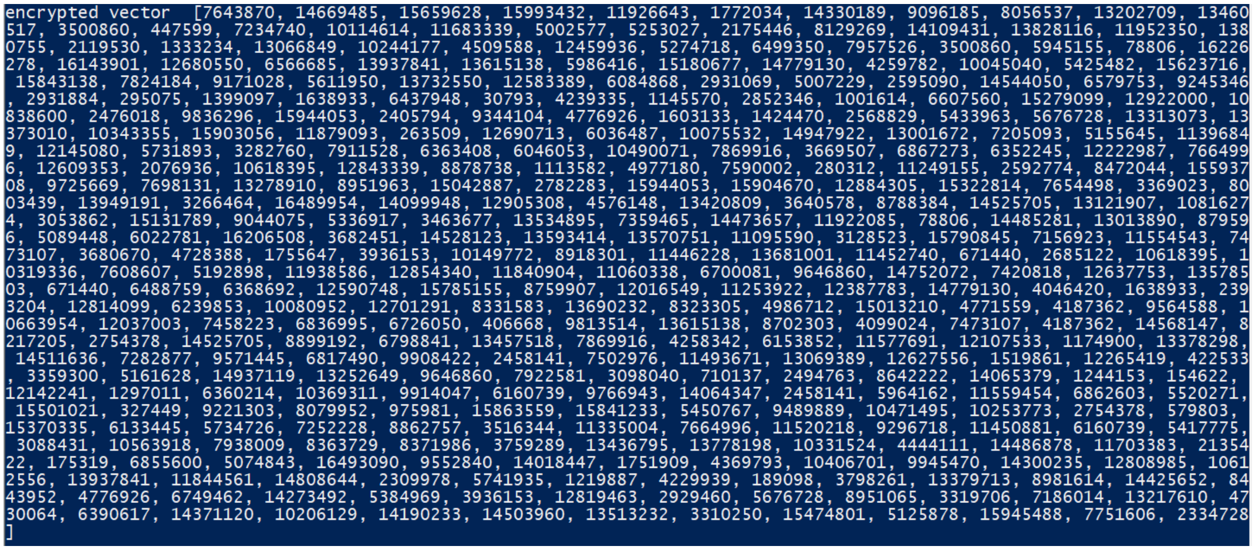
6. Comparison of my Review-III cryptographic model with Review-II model

There hasn’t been any major changes in the cryptographic model (paillier encryption) since review-II. Only **one change in the size of the input and output encrypted vector was made.** Earlier I was using a **vector of 383 length which has been increased this time to 458 length vector.**

Review-II:

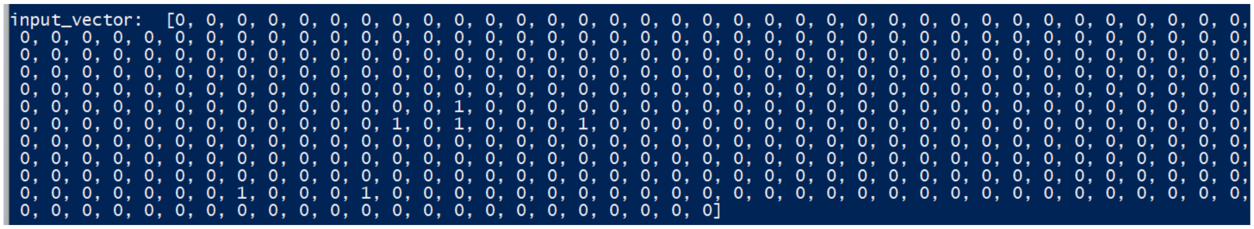


```
input_vector:  [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1,
 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1,
 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

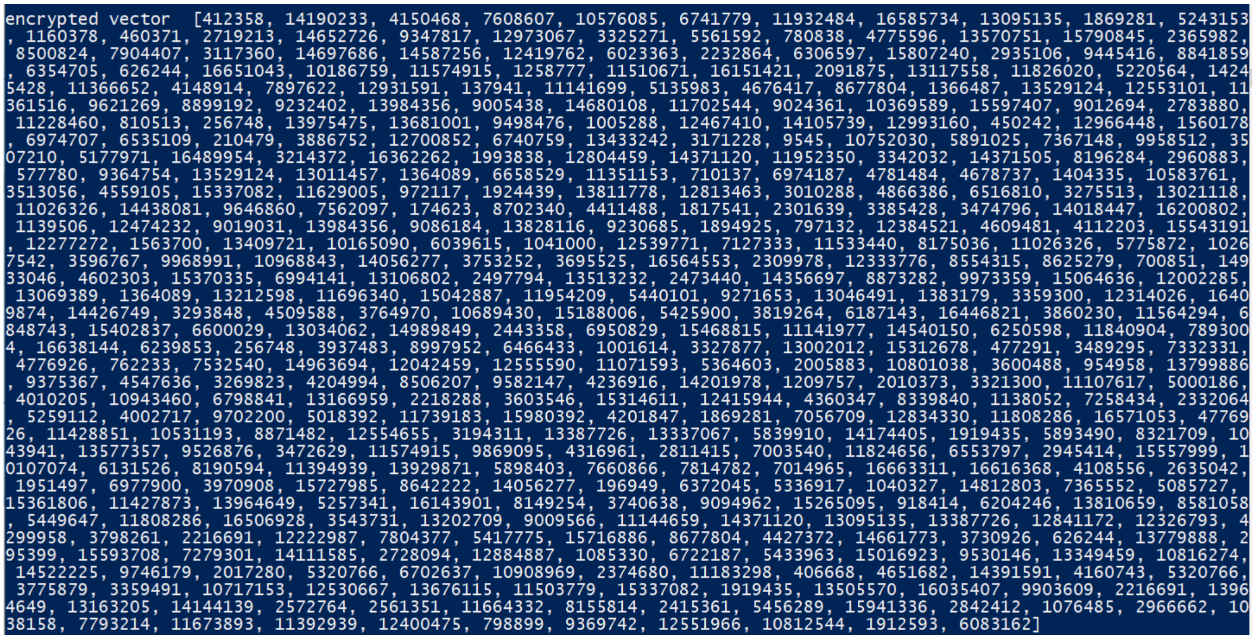


```
encrypted vector  [7643870, 14669485, 15659628, 15993432, 11926643, 1772034, 14330189, 9096185, 8056537, 13202709, 13460
517, 3500860, 447599, 7234740, 10114614, 11683339, 5002577, 5253027, 2175446, 8129269, 14109431, 13828116, 11952350, 138
0755, 2119530, 1333234, 13066849, 10244177, 4509588, 12459936, 5274718, 6499350, 7957526, 3500860, 5945155, 78806, 16226
278, 16143901, 12680550, 6566685, 13937841, 13615138, 5986416, 15180677, 14779130, 4259782, 10045040, 5425482, 15623716,
 15843138, 7824184, 9171028, 5611950, 13732550, 12583389, 6084868, 2931069, 5007229, 2595090, 14544050, 6579753, 9245346
, 2931884, 295075, 1399097, 1638933, 6437948, 30793, 4239335, 1145570, 2852346, 1001614, 6607560, 15279099, 12922000, 10
838600, 2476018, 9836296, 15944053, 2405794, 9344104, 4776926, 1603133, 1424470, 2568829, 5433963, 5676728, 13313073, 13
373010, 10343355, 15903056, 11879093, 263509, 12690713, 6036487, 10075532, 14947922, 13001672, 7205093, 5155645, 1139684
9, 12145080, 5731893, 3282760, 7911528, 6363408, 6046053, 10490071, 7869916, 3669507, 6867273, 6352245, 12222987, 766499
6, 12609353, 2076936, 10618395, 12843339, 8878738, 1113582, 4977180, 7590002, 280312, 11249155, 2592774, 8472044, 155937
08, 9725669, 7698131, 13278910, 8951963, 15042887, 2782283, 15944053, 15904670, 12884305, 15322814, 7654498, 3369023, 80
03439, 13949191, 3266464, 16489954, 14099948, 12905308, 4576148, 13420809, 3640578, 8788384, 14525705, 13121907, 1081627
4, 3053862, 15131789, 9044075, 5336917, 3463677, 13534895, 7359465, 14473657, 11922085, 78806, 14485281, 13013890, 87959
6, 5089448, 6022781, 16206508, 3682451, 14528123, 13593414, 13570751, 11095590, 3128523, 15790845, 7156923, 11554543, 74
73107, 3680670, 4728388, 1755647, 3936153, 10149772, 8918301, 11446228, 13681001, 11452740, 671440, 2685122, 10618395, 1
0319336, 7608607, 5192898, 11938586, 12854340, 11840904, 11060338, 6700081, 9646860, 14752072, 7420818, 12637753, 135785
03, 671440, 6488759, 6368692, 12590748, 15785155, 8759907, 12016549, 11253922, 12387783, 14779130, 4046420, 1638933, 239
3204, 12814099, 6239853, 10080952, 12701291, 8331583, 13690232, 8323305, 4986712, 15013210, 4771559, 4187362, 9564588, 1
0663954, 12037003, 7458223, 6836995, 6726050, 406668, 9813514, 13615138, 8702303, 4099024, 7473107, 4187362, 14568147, 8
217205, 2754378, 14525705, 8899192, 6798841, 13457518, 7869916, 4258342, 6153852, 11577691, 12107533, 1174900, 13378298,
 14511636, 7282877, 9571445, 6817490, 9908422, 2458141, 7502976, 11493671, 13069389, 12627556, 1519861, 12265419, 422533
, 3359300, 5161628, 14937119, 13252649, 9646860, 7922581, 3098040, 710137, 2494763, 8642222, 14065379, 1244153, 154622,
12142241, 1297011, 6360214, 10369311, 9914047, 6160739, 9766943, 14064347, 2458141, 5964162, 11559454, 6862603, 5520271,
 15501021, 327449, 9221303, 8079952, 975981, 15863559, 15841233, 5450767, 9489889, 10471495, 10253773, 2754378, 579803,
15370335, 6133445, 5734726, 7252228, 8862757, 3516344, 11335004, 7664996, 11520218, 9296718, 11450881, 6160739, 5417775,
 3088431, 10563918, 7938009, 8363729, 8371986, 3759289, 13436795, 13778198, 10331524, 4444111, 14486878, 11703383, 21354
22, 175319, 6855600, 5074843, 16493090, 9552840, 14018447, 1751909, 4369793, 10406701, 9945470, 14300235, 12808985, 1061
2556, 13937841, 11844561, 14808644, 2309978, 5741935, 1219887, 4229939, 189098, 3798261, 13379713, 8981614, 14425652, 84
43952, 4776926, 6749462, 14273492, 5384969, 3936153, 12819463, 2929460, 5676728, 8951065, 3319706, 7186014, 13217610, 47
30064, 6390617, 14371120, 10206129, 14190233, 14503960, 13513232, 3310250, 15474801, 5125878, 15945488, 7751606, 2334728
]
```

Review-III:



```
input_vector:  [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```



```
encrypted vector  [412358, 14190233, 4150468, 7608607, 10576085, 6741779, 11932484, 16585734, 13095135, 1869281, 5243153
, 1160378, 460371, 2719213, 14652726, 9347817, 12973067, 3325271, 5561592, 780838, 4775596, 13570751, 15790845, 2365982,
 8500824, 7904407, 3117360, 14697686, 14587256, 12419762, 6023363, 2232864, 6306597, 15807240, 2935106, 9445416, 8841859
, 6354705, 626244, 16651043, 10186759, 11574915, 1258777, 11510671, 16151421, 2091875, 13117558, 11826020, 5220564, 1424
5428, 11366652, 4148914, 7897622, 12931591, 137941, 11141699, 5135983, 4676417, 8677804, 1366487, 13529124, 12553101, 11
361516, 9621269, 8899192, 9232402, 13984356, 9005438, 14680108, 11702544, 9024361, 10369589, 15597407, 9012694, 2783880,
 11228460, 810513, 256748, 13975475, 13681001, 9498476, 1005288, 12467410, 14105739, 12993160, 450242, 12966448, 1560178
, 6974707, 6535109, 210479, 3886752, 12700852, 6740759, 13433242, 3171228, 9545, 10752030, 5891025, 7367148, 9958512, 35
07210, 5177971, 16489954, 3214372, 16362262, 1993838, 12804459, 14371120, 11952350, 3342032, 14371505, 8196284, 2960883,
 577780, 9364754, 13529124, 13011457, 1364089, 6658529, 11351153, 710137, 6974187, 4781484, 4678737, 1404335, 10583761,
3513056, 4559105, 15337082, 11629005, 972117, 1924439, 13811778, 12813463, 3010288, 4866386, 6516810, 3275513, 13021118,
 11026326, 14438081, 9646860, 7562097, 174623, 8702340, 4411488, 1817541, 2301639, 3385428, 3474796, 14018447, 16200802,
 1139506, 12474232, 9019031, 13984356, 9086184, 13828116, 9230685, 1894925, 797132, 12384521, 4609481, 4112203, 15543191
, 12277272, 1563700, 13409721, 10165090, 6039615, 1041000, 12539771, 7127333, 11533440, 8175036, 11026326, 5775872, 1026
7542, 3596767, 9968991, 10968843, 14056277, 3753252, 3695525, 16564553, 2309978, 12333776, 8554315, 8625279, 700851, 149
33046, 4602303, 15370335, 6994141, 13106802, 2497794, 13513232, 2473440, 14356697, 8873282, 9973359, 15064636, 12002285,
 13069389, 1364089, 13212598, 11696340, 15042887, 11954209, 5440101, 9271653, 13046491, 1383179, 3359300, 12314026, 1640
9874, 14426749, 3293848, 4509588, 3764970, 10689430, 15188006, 5425900, 3819264, 6187143, 16446821, 3860230, 11564294, 6
848743, 15402837, 6600029, 13034062, 14989849, 2443358, 6950829, 15468815, 11141977, 14540150, 6250598, 11840904, 789300
4, 16638144, 6239853, 256748, 3937483, 8997952, 6466433, 1001614, 3327877, 13002012, 15312678, 477291, 3489295, 7332331,
 4776926, 762233, 7532540, 14963694, 12042459, 12555590, 11071593, 5364603, 2005883, 10801038, 3600488, 954958, 13799886
, 9375367, 4547636, 3269823, 4204994, 8506207, 9582147, 4236916, 14201978, 1209757, 2010373, 3321300, 11107617, 5000186,
 4010205, 10943460, 6798841, 13166959, 2218288, 3603546, 15314611, 12415944, 4360347, 8339840, 1138052, 7258434, 2332064
, 5259112, 4002717, 9702200, 5018392, 11739183, 15980392, 4201847, 1869281, 7056709, 12834330, 11808286, 16571053, 47769
26, 11428851, 10531193, 8871482, 12554655, 3194311, 13387726, 13337067, 5839910, 14174405, 1919435, 5893490, 8321709, 10
43941, 13577357, 9526876, 3472629, 11574915, 9869095, 4316961, 2811415, 7003540, 11824656, 6553797, 2945414, 15557999, 1
0107074, 6131526, 8190594, 11394939, 13929871, 5898403, 7660866, 7814782, 7014965, 16663311, 16616368, 4108556, 2635042,
 1951497, 6977900, 3970908, 15727985, 8642222, 14056277, 196949, 6372045, 5336917, 1040327, 14812803, 7365552, 5085727,
15361806, 11427873, 13964649, 5257341, 16143901, 8149254, 3740638, 9094962, 15265095, 918414, 6204246, 13810659, 8581058
, 5449647, 11808286, 16506928, 3543731, 13202709, 9009566, 11144659, 14371120, 13095135, 13387726, 12841172, 12326793, 4
299958, 3798261, 2216691, 12222987, 7804377, 5417775, 15716886, 8677804, 4427372, 14661773, 3730926, 626244, 13779888, 2
95399, 15593708, 7279301, 14111585, 2728094, 12884887, 1085330, 6722187, 5433963, 15016923, 9530146, 13349459, 10816274,
 14522225, 9746179, 2017280, 5320766, 6702637, 10908969, 2374680, 11183298, 406668, 4651682, 14391591, 4160743, 5320766,
 3775879, 3359491, 10717153, 12530667, 13676115, 11503779, 15337082, 1919435, 13505570, 16035407, 9903609, 2216691, 1396
4649, 13163205, 14144139, 2572764, 2561351, 11664332, 8155814, 2415361, 5456289, 15941336, 2842412, 1076485, 2966662, 10
38158, 7793214, 11673893, 11392939, 12400475, 798899, 9369742, 12551966, 10812544, 1912593, 6083162]
```