

CONFIGURATION MANUAL

MSc Internship

MSC IN CYBERSECURITY

SHUBHAM

Student ID: X21177163

School of Computing

National College of Ireland

Supervisor: Niall Heffernan

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: SHUBHAM.....
Student ID:X21177163.....
Programme: MSC IN CYBERSECURITY **Year:** ...2023..
Module: ACADEMIC INTERNSHIP
Supervisor: Niall Heffernan
Submission Due Date:14-08-2023.....
Project Title: CONFIGURATION MANUAL

Word Count: 969 **Page Count:** 9

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature:Shubham.....
Date:14-8-2023.....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

CONFIGURATION MANUAL

Contents

1. Introduction	3
2. System Configuration.....	3
2.1 Hardware Configuration	4
2.2 Software Configuration	4
3. Code Overview:.....	Error! Bookmark not defined.
4. Implementation and Evaluation.....	6
5. Conclusion.....	9

1. Introduction

This research presents an approach to enhance data encryption effectiveness and security through the use of a combination of techniques. The main objectives of the project are as follows:

- In this method, a hybrid approach is developed by combining AES encryption for the original text and ECC keys to re-encrypt the cipher text after retrieval. By adding an extra layer of security, this approach becomes particularly useful in situations where prioritizing security is more important than efficiency.
- Another technique employed in this project involves encrypting the original text message using a new AES key after the old AES key has been encrypted using ECC. The efficiency is improved because the encryption is done on the key itself rather than the plain text communication. This method is preferable when effectiveness is more crucial than data storage concerns.
- The research also utilizes a hybrid technique where the AES key is split into four parts, and one of those pieces is encrypted using the ECC algorithm. This process generates a new AES key, which is then used to encrypt the plain text. This approach reduces the encryption time and enhances security, as cybercriminals would need to decrypt the key before attempting to decrypt the encrypted content. This additional layer of security ensures efficiency while maintaining strong protection.

By implementing these innovative methods, the research aims to create a robust encryption algorithm that can be adapted to different scenarios based on the specific requirements of security and efficiency.

2. System Configuration

The Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) are combined in the provided code to create a hybrid method that increases the security of data encryption and decryption operations. There are particular sorts of equipment and resources needed to efficiently run this algorithm. A computer or other computing device that can run MATLAB or a similar programming environment is first and foremost required. Additionally, the device must have a trustworthy and secure storage medium in order to guarantee the security of the encrypted data. Overall, the hybrid method can offer a reliable and secure data encryption solution for a variety of applications because its performance is dependent on the device's processing power, memory, and storage capacity.

2.1 Hardware Configuration

A device with enough Random Access Memory (RAM) is advised to handle the processing of huge data sets successfully because the method uses memory resources. AES and ECC implementation software libraries, functions, and scripts may need to be downloaded and stored, which will add to the algorithm's potential storage space requirement. For both AES and ECC, sufficient computer capacity is required to carry out the intricate mathematical processes. The encryption and decryption procedures can be substantially sped up by a modern CPU with multiple cores.



2.2 Software Configuration

MATLAB: We choose MATLAB for our research after completing in-depth research on a number of testing environments for encryption techniques. This choice is being supported by a number of factors. First off, MATLAB is an effective software suite that offers a variety of tools and functions for testing and assessing encryption schemes. It is perfect for academics and developers with varied degrees of programming knowledge because it also has a user-friendly interface and simple syntax. A large number of encryption-related functions and toolboxes have also been developed by the MATLAB community, which has helped to save a lot of time and effort during the testing stage.

Requirement:

Operating System	<ul style="list-style-type: none"> • Windows 11 • Windows 10 (version 1909 or higher) • Windows Server 2019 <p>Note:</p> <ul style="list-style-type: none"> • Windows 7 is no longer supported • Windows Server 2016 is no longer supported
Processor	<ul style="list-style-type: none"> • Minimum: Any Intel or AMD x86-64 processor • Recommended: Any Intel or AMD x86-64 processor with four logical cores and AVX2 instruction set support
RAM	<ul style="list-style-type: none"> • Minimum: 4 GB • Recommended: 8 GB • For Polyspace, 4 GB per core is recommended
Storage	<ul style="list-style-type: none"> • 3.6 GB for just MATLAB • 5-8 GB for a typical installation • 31.5 GB for an all products installation • An SSD is strongly recommended
Graphics	<ul style="list-style-type: none"> • No specific graphics card is required, but a hardware accelerated graphics card supporting OpenGL 3.3 with 1GB GPU memory is recommended. • GPU acceleration using Parallel Computing Toolbox requires a GPU that has a compute capability 3.0 or higher. For more information, see GPU Support by Release.

Cryptool2: A range of cryptographic algorithms and techniques for encryption, decryption, and protocol analysis are available in the free and open-source cryptography application Cryptool 2.

Requirement:

Cryptool2 is an open-source software which is available for windows, Linux and macOS.

AIDA64:

Requirements:

You will need a computer running a compatible operating system, such as Windows or Linux, in order to install AIDA64 Extreme, a thorough system diagnostics and benchmarking program.

3. Steps to Run the Code:

A sequence of actions must be taken in order to start the code's execution and explore its functionality. These actions cover the preparation and setting up needed for a smooth code run. Following these guidelines will help consumers have a seamless and successful experience.

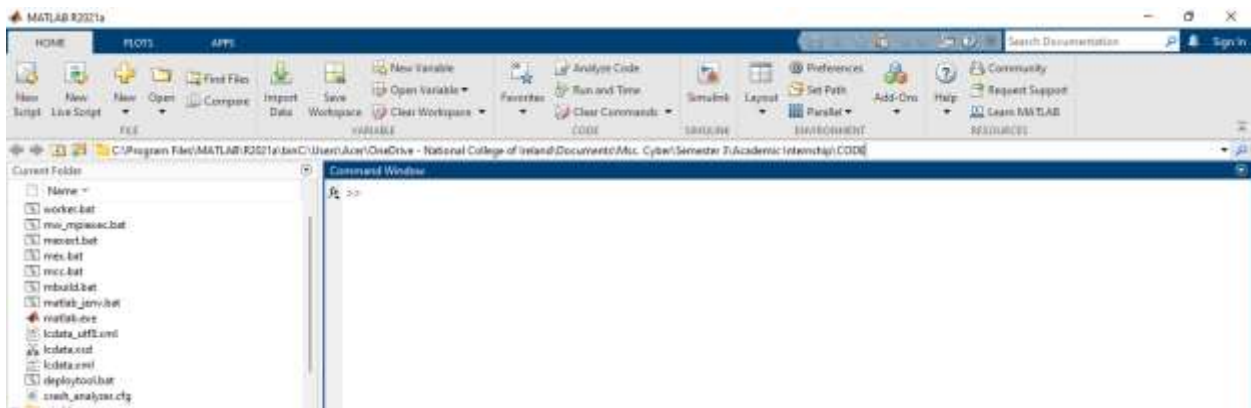
Step1: Install the MATLAB software from the website 'www.mathswork.com'.

Step2: Download the code zip file and extract the 'CODE' folder.

Step3: Open the installed MATLAB Software.



Step4: Now, click on browse or open folder button or paste the path of folder in the bar and click 'Enter'.



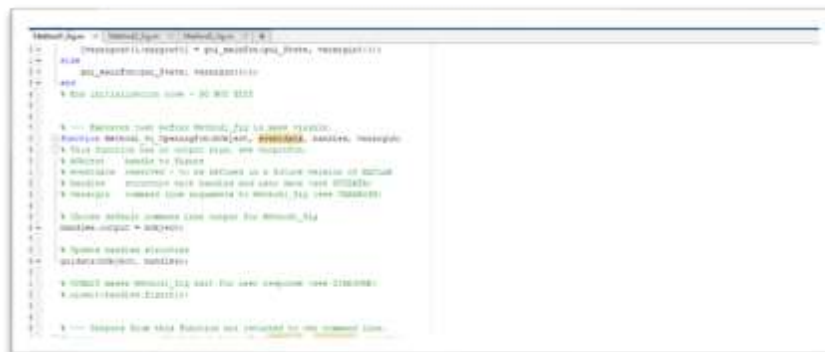
Step5: Now Run the Method1_fig.m, Method2_fig.m, Method3_fig.m file.

4. IMPLEMENTATION

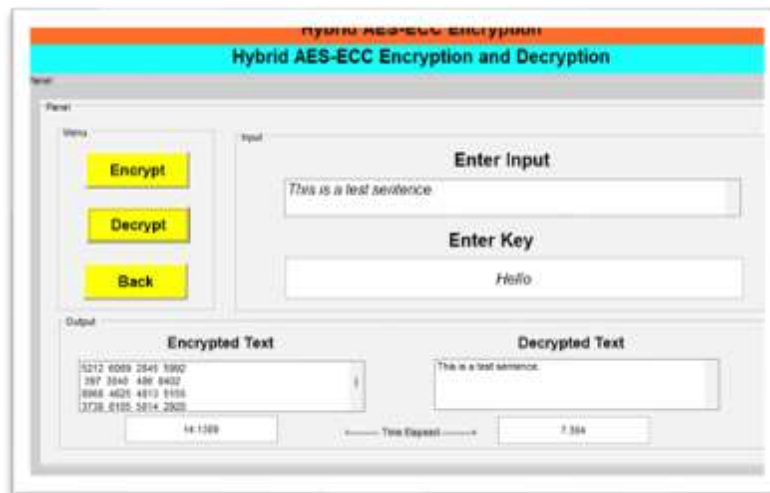
METHOD 1:

With the help of both keys, this method encrypts the plain text by first using AES and then using ECC to encrypt the cipher text that is produced. This is the most straightforward technique of encryption.

CODE:



OUTPUT:



Method 2:

In the Method 2, enter the key of 16 bytes because in this method key is divided into 4 parts and 4th part of the key is encrypted.

CODE:

```
121  
122 * --- Example of button click to Encrypt  
123 * function Encrypt_Click(object sender, EventArgs e)  
124 * object sender is Encrypt user click  
125 * EventArgs e.Handled = false to be defined in a future version of XAML  
126 * handle: encrypt with handle and user data (see OUTPUT)  
127 *  
128 *  
129 *  
130 *  
131 * get here condition and loop the splitting user data 16 bytes  
132 * text_length=lengthof(input)  
133 * extra_bytes=(text_length-16)/4 to get the end of each amount of bytes can be added  
134 * int*index=(16+extra_bytes)*4 and it's to make it divisible by 16  
135 * textinput*(textinput,0:1)  
136 * text_output=lengthof(textinput)*4 (same user length)  
137 * key = KeyFill(key)  
138 * key = KeyFill(key)  
139 * cipher_output =  
140 *  
141 * --- END part  
142 * if text_length  
143 *   text_output = KeyFill(key)  
144 *   key_output = KeyFill(key)
```

Output:



Method 3:

In this method, the AES key is encrypted first using ECC and then the new AES key is used to encrypt the plaintext.

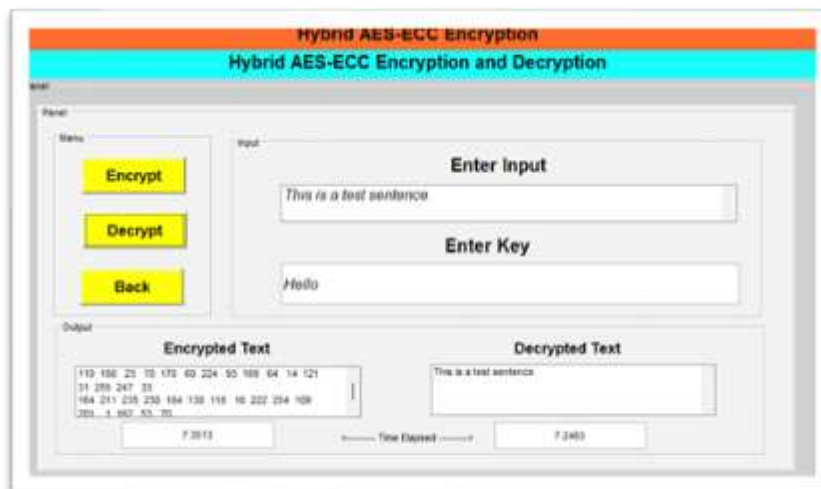
CODE:

```

22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

OUTPUT:



5. Conclusion

The researcher investigated the impact of utilizing a combination of two encryption algorithms, namely symmetric and asymmetric encryption. This study involved the fusion of AES and ECC encryption methods in various manners, some of which demonstrated superior outcomes compared to others. Initially, the first approach yielded commendable security and randomness characteristics; however, this was offset by prolonged execution times. Subsequently, the second approach led to enhanced execution times while marginally compromising on randomness compared to the first method. Lastly, the third approach offered equivalent execution times to the second method and comparable randomness to the first method. Consequently, the researcher recommended the adoption of hybrid encryption. When implemented effectively, this approach has the potential to harness the advantages of each method while mitigating their respective drawbacks.