ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών,
Τομέας Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής
Ροή Δ, Μάθημα: *Ασφάλεια Δικτύων Υπολογιστών* (Εξάμηνο 8ο)

Δεύτερη Εργαστηριακή Άσκηση: Φύλλο Απαντήσεων
Σύγχρονοι Αλγόριθμοι Κρυπτογράφησης

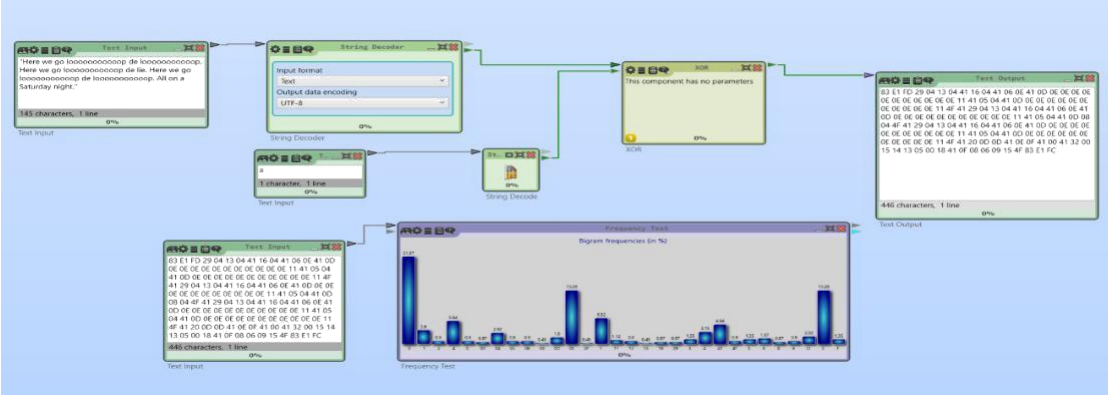
Ονοματεπώνυμο: Ειρήνη Δόντη
Αριθμός Μητρώου: 03119839
Εξάμηνο: 8ο

Ερώτηση 2.1

"***Here we go looooooooooop de looooooooooop. Here we go looooooooooop de lie. Here we go looooooooooop de looooooooooop. All on a Saturday night.***"

	Ciphertext/K1	**Ciphertext/K2**	**Ciphertext/K3**	**Ciphertext/ K4**	**Ciphertext/K5**
Key → char	a	ab	abcd	abcdefgh	abcdefghijklmnop
Key → Hex	0x61	0x61 62	0x61 62 63 64	0x61 62 63 64 65 66 67 68	0x61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70
Key → Bits	01100001	01100001011 00010	01100001011 00010011000 1101100100	01100001011 00010011000 11011001000 11001010110 01100110011 101101000	01100001011000 10011000110110 01000110010101 10011001100111 01101000011010 01011010100110 10110110110001 10110101101110 01101111011100 00
Συχνότερο δίγραμμα	0E, E	0E, E	4	4	4
Πλήθος εμφανίσεών του	13.26%	7.87%	5.84%	5.84%	5.84%

Για παράδειγμα, παραθέτουμε τη διάταξη για το κλειδί "α":



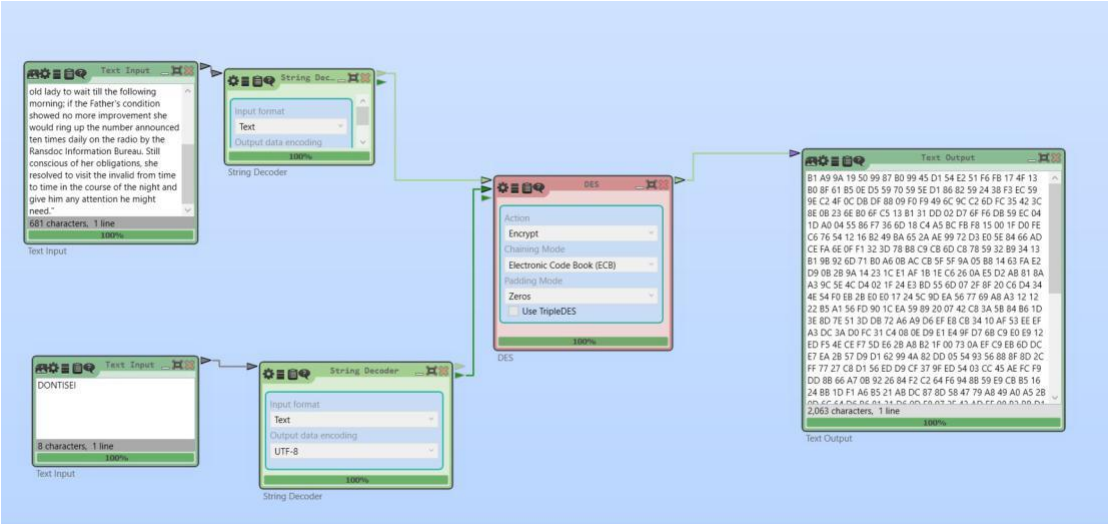
Στο μη κρυπτογραφημένο, το γράμμα που κυριαρχεί είναι το “ο”. Παρατηρούμε, ότι όσο αυξάνεται το μήκος του κλειδιού, τόσο μειώνεται η συχνότητα εμφάνισης του γράμματος που παρατηρείται περισσότερες φορές.

Για παράδειγμα, με κλειδί “α” το κρυπτοκείνο είναι το εξής:

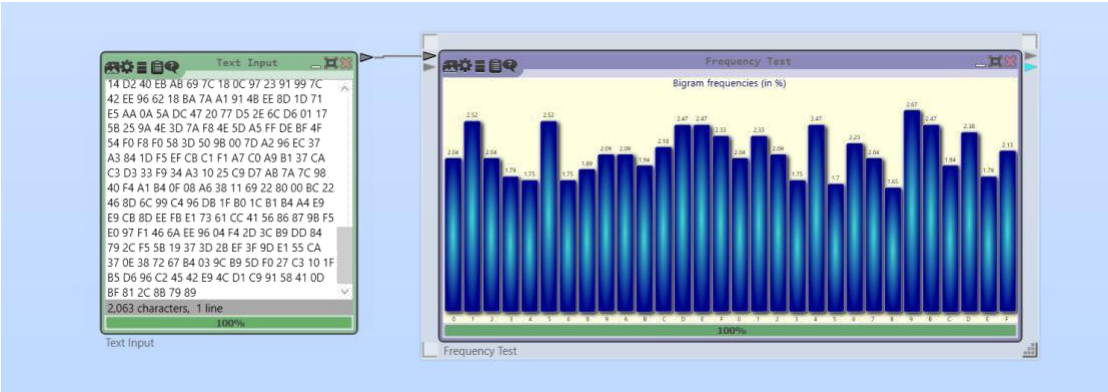
83 E1 FD 29 04 13 04 41 16 04 41 06 0E 41 0D 0E 0E 0E 0E 0E 0E 0E 0E 0E 0E 11 41 05 04 41 0D 0E 0E 0E 0E 0E 0E 0E 0E 0E 0E 11 4F 41 29 04 13 04 41 16 04 41 06 0E 41 0D 0E 0E 0E 0E 0E 0E 0E 0E 0E 0E 11 41 05 04 41 0D 08 04 4F 41 29 04 13 04 41 16 04 41 06 0E 41 0D 0E 0E 0E 0E 0E 0E 0E 0E 0E 0E 11 41 05 04 41 0D 0E 0E 0E 0E 0E 0E 0E 0E 0E 0E 11 4F 41 20 0D 0D 41 0E 0F 41 00 41 32 00 15 14 13 05 00 18 41 0F 08 06 09 15 4F 83 E1 FC

Ερώτηση 2.2

“***However, in the afternoon she made another attempt to talk to the priest, but she could get out of him no more than a few rambling phrases. She renewed her proposal to call in the doctor. Whereat Paneloux sat up and in a stifled voice emphatically declined to see a doctor. Under these circumstances it seemed best to the old lady to wait till the following morning; if the Father's condition showed no more improvement she would ring up the number announced ten times daily on the radio by the Ransdoc Information Bureau. Still conscious of her obligations, she resolved to visit the invalid from time to time in the course of the night and give him any attention he might need.***”



Το διάγραμμα συχνοτήτων:



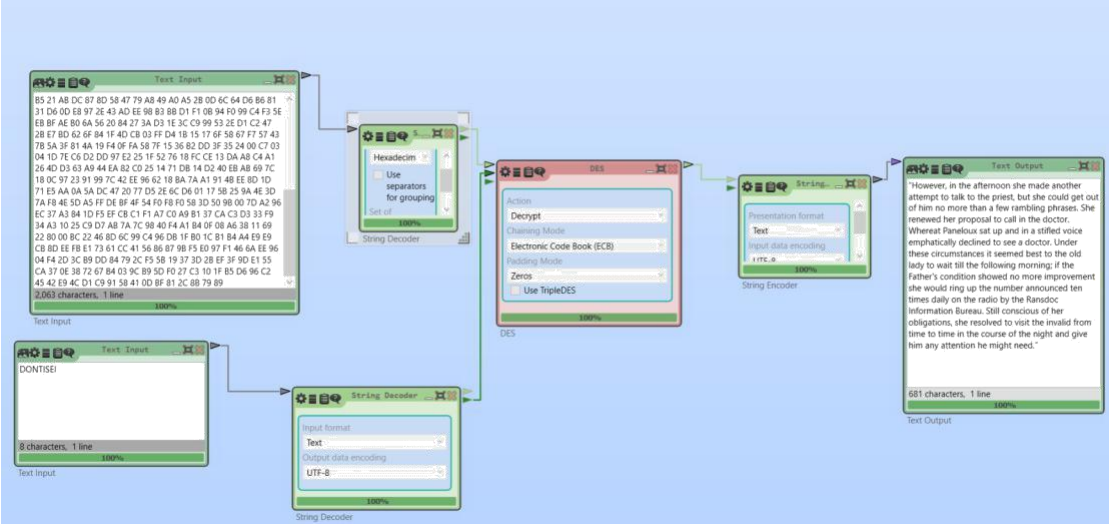
Χρησιμοποιούμε κλειδί μήκους 64/8 = 8 χαρακτήρες (DONTISEI) ή 64 bits. Το κείμενο δεν έχει το ίδιο μήκος με το αρχικό, λόγω padding. Το πιο συχνό γράμμα που παρατηρείται είναι το 9 (HEX).

Κρυπτογραφημένο κείμενο:

B1 A9 9A 19 50 99 87 B0 99 45 D1 54 E2 51 F6 FB 17 4F 13 B0 8F 61 B5 0E D5 59 70 59 5E D1 86 82 59 24 38 F3 EC 59 9E C2 4F 0C DB DF 88 09 F0 F9 49 6C 9C C2 6D FC 35 42 3C 8E 0B 23 6E B0 6F C5 13 B1 31 DD 02 D7 6F F6 DB 59 EC 04 1D A0 04 55 86 F7 36 6D 18 C4 A5 BC FB F8 15 00 1F D0 FE C6 76 54 12 16 B2 49 BA 65 2A AE 99 72 D3 E0 5E 84 66 AD CE FA 6E 0F F1 32 3D 78 B8 C9 CB 6D C8 78 59 32 B9 34 13 B1 9B 92 6D 71 B0 A6 0B AC CB 5F 5F 9A 05 B8 14 63 FA E2 D9 0B 2B 9A 14 23 1C E1 AF 1B 1E C6 26 0A E5 D2 AB 81 8A A3 9C 5E 4C D4 02 1F 24 E3 BD 55 6D 07 2F 8F 20 C6 D4 34 4E 54 F0 EB 2B E0 E0 17 24 5C 9D EA 56 77 69 A8 A3 12 12 22 B5 A1 56 FD 90 1C EA 59 89 20 07 42 C8 3A 5B 84 B6 1D 3E 8D 7E 51 3D DB 72 A6 A9 D6 EF E8 CB 34 10 AF 53 EE EF A3 DC 3A D0 FC 31 C4 08 0E D9 E1 E4 9F D7 6B C9 E0 E9 12 ED F5 4E CE F7 5D E6 2B A8 B2 1F 00 73 0A EF C9 EB 6D DC E7 EA 2B 57 D9 D1 62 99 4A 82 DD 05 54 93 56 88 8F 8D 2C FF 77 27 C8 D1 56 ED D9 CF 37 9F ED 54 03 CC 45 AE FC F9 DD 8B 66 A7 0B 92 26 84 F2 C2 64 F6 94 8B 59 E9 CB B5 16 24 BB 1D F1 A6 B5 21 AB DC 87 8D 58 47 79 A8 49 A0 A5 2B 0D 6C 64 D6 B6 81 31 D6 0D E8 97 2E 43 AD EE 98 B3 BB D1 F1 0B 94 F0 99 C4 F3 5E EB BF AE B0 6A 56 20 84 27 3A D3 1E 3C C9 99 53 2E D1 C2 47 2B E7 BD 62 6F 84 1F 4D CB 03 FF D4 1B 15 17 6F 58 67 F7 57 43 7B 5A 3F 81 4A 19 F4 0F FA 58 7F 15 36 B2 DD 3F 35 24 00 C7 03 04 1D 7E C6 D2 DD 97 E2 25 1F 52 76 18 FC CE 13 DA A8 C4 A1 26 4D D3 63 A9 44 EA 82 C0 25 14 71 DB 14 D2 40 EB AB 69 7C 18 0C 97 23 91 99 7C 42 EE 96 62 18 BA 7A A1 91 4B EE 8D 1D 71 E5 AA 0A 5A DC 47 20 77 D5 2E 6C D6 01 17 5B 25 9A 4E 3D 7A F8 4E 5D A5 FF DE BF 4F 54 F0 F8 F0 58 3D 50 9B 00 7D A2 96 EC 37 A3 84 1D F5 EF CB C1 F1 A7 C0 A9 B1 37 CA C3 D3 33 F9 34 A3 10 25 C9 D7 AB 7A 7C 98 40 F4 A1 B4 0F 08 A6 38 11 69 22 80 00 BC 22 46 8D 6C 99 C4 96 DB 1F B0 1C B1 B4 A4 E9 E9 CB 8D EE FB E1 73 61 CC 41 56 86 87 9B F5 E0 97 F1 46 6A EE 96 04 F4 2D 3C B9 DD 84 79 2C F5 5B 19 37 3D 2B EF 3F 9D E1 55 CA 37 0E 38 72 67 B4 03 9C B9 5D F0 27 C3 10 1F B5 D6 96 C2 45 42 E9 4C D1 C9 91 58 41 0D BF 81 2C 8B 79 89

Ερώτηση 2.3

Παραθέτουμε την παρακάτω διάταξη:



Χρησιμοποιήσαμε το ίδιο κλειδί με την κρυπτοφράφηση (DONTISEI). Το mode of operation είναι το ίδιο με εκείνο της κρυπτογράφησης ECB.

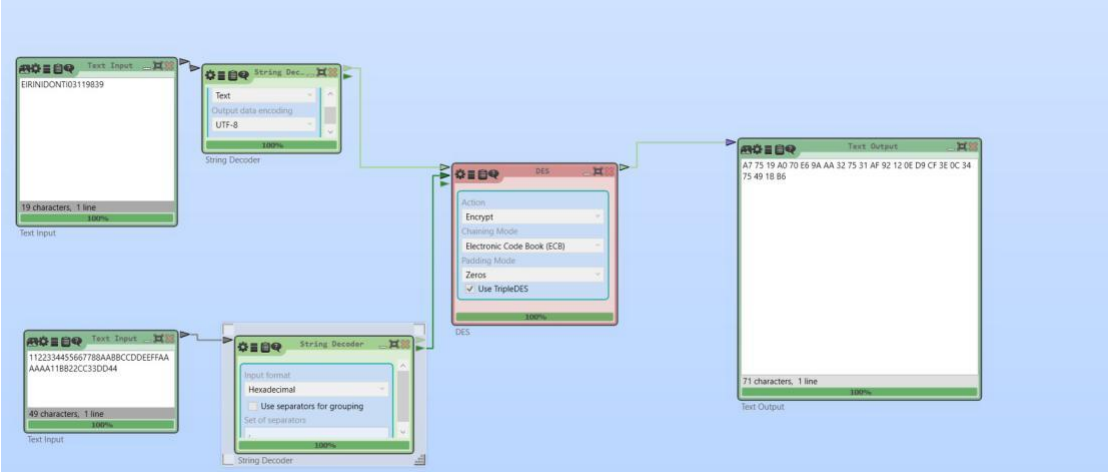
Ερώτηση 2.4

“***ComputerNetworkSecurity*** ***ComputerNetworkSecurity*** ***ComputerNetworkSecurity***
ComputerNetworkSecurity ***ComputerNetworkSecurity*** ***ComputerNetworkSecurity***
ComputerNetworkSecurity ***ComputerNetworkSecurity*** ***ComputerNetworkSecurity***
ComputerNetworkSecurity”

Παρατηρούμε ότι, στο κρυπτοκείμενο, υπάρχει επανάληψη μοτίβων της ακολουθίας “F1 4A 38 1B 21 40 29 88 AC 9B D0 69 0A 58 42 2D 73 62 A9 7F 30 C9 BA 93 F1 4A 38 1B 21 40 29 88 AC 9B D0 69 0A 58 42 2D 73 62 A9 7F 30 C9 BA 93”. Αυτό συμβαίνει, καθώς το ECB χωρίζει το κείμενο σε blocks (που στη συγκεκριμένη είναι ίδια) και χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση. Αυτό σημαίνει λιγότερη ασφάλεια του αλγορίθμου. Αυτό μπορεί να αποφευχθεί, χρησιμοποιώντας τον τρόπο λειτουργίας αλγορίθμου CBC ή OF

Ερώτηση 2.7

Η διάταξη φαίνεται παρακάτω:

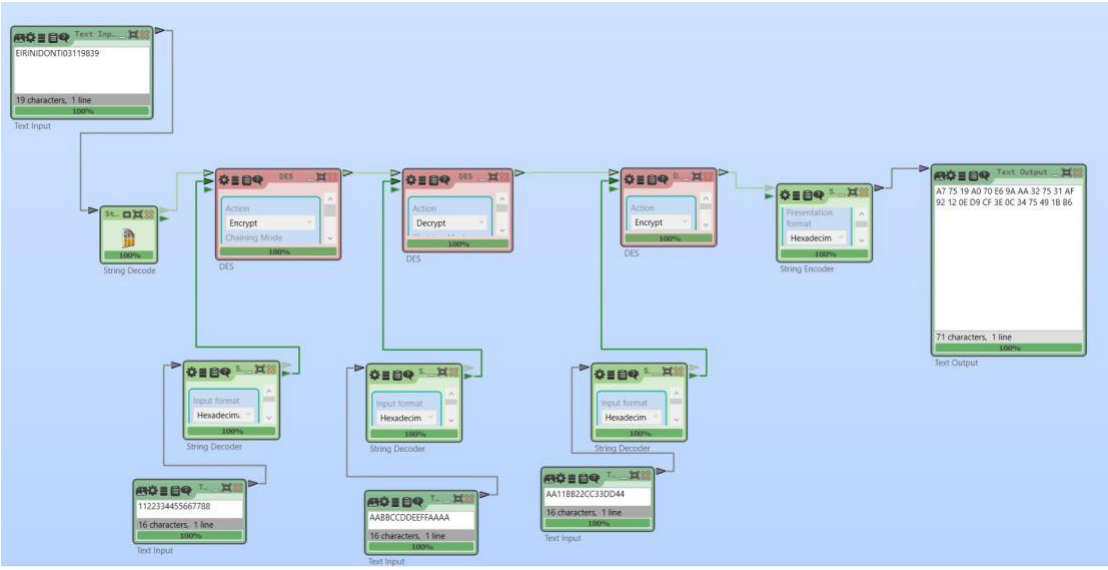


Κρυπτογραφημένο κείμενο:

A7 75 19 A0 70 E6 9A AA 32 75 31 AF 92 12 0E D9 CF 3E 0C 34 75 49 1B B6

Ερώτηση 2.8

Η διάταξη φαίνεται παρακάτω:



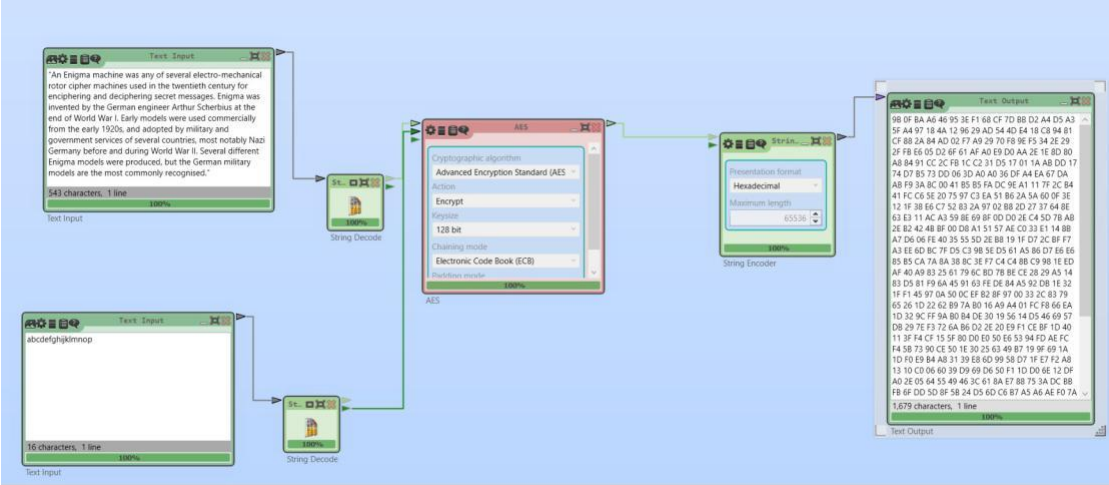
Κρυπτογραφημένο κείμενο:

A7 75 19 A0 70 E6 9A AA 32 75 31 AF 92 12 0E D9 CF 3E 0C 34 75 49 1B B6

Ερώτηση 2.12

"***An Enigma machine was any of several electro-mechanical rotor cipher machines used in the twentieth century for enciphering and deciphering secret messages. Enigma was invented by the German engineer Arthur Scherbius at the end of World War I. Early models were used commercially from the early 1920s, and adopted by military and government services of several countries, most notably Nazi Germany before and during World War II. Several different Enigma models were produced, but the German military models are the most commonly recognised.***"

Χρησιμοποιούμε το κλειδί "abcdefghijklmnop". Παραθέτουμε τη ζητούμενη διάταξη:



Κρυπτογραφημένο κείμενο:

9B 0F BA A6 46 95 3E F1 68 CF 7D BB D2 A4 D5 A3 5F A4 97 18 4A 12 96 29 AD 54 4D E4 18 C8 94 81 CF 88 2A 84 AD 02 F7 A9 29 70 F8 9E F5 34 2E 29 2F FB E6 05 D2 6F 61 AF A0 E9 D0 AA 2E 1E 8D 80 A8 84 91 CC 2C FB 1C C2 31 D5 17 01 1A AB DD 17 74 D7 B5 73 DD 06 3D A0 A0 36 DF A4 EA 67 DA AB F9 3A 8C 00 41 B5 B5 FA DC 9E A1 11 7F 2C B4 41 FC C6 5E 20 75 97 C3 EA 51 B6 2A 5A 60 0F 3E 12 1F 38 E6 C7 52 83 2A 97 02 B8 2D 27 37 64 8E 63 E3 11 AC A3 59 8E 69 8F 0D D0 2E C4 5D 7B AB 2E B2 42 4B BF 00 D8 A1 51 57 AE C0 33 E1 14 8B A7 D6 06 FE 40 35 55 5D 2E B8 19 1F D7 2C BF F7 A3 EE 6D BC 7F D5 C3 9B 5E D5 61 A5 86 D7 E6 E6 85 B5 CA 7A 8A 38 8C 3E F7 C4 C4 8B C9 98 1E ED AF 40 A9 83 25 61 79 6C BD 7B BE CE 28 29 A5 14 83 D5 81 F9 6A 45 91 63 FE DE 84 A5 92 DB 1E 32 1F F1 45 97 0A 50 0C EF B2 8F 97 00 33 2C 83 79 65 26 1D 22 62 B9 7A B0 16 A9 A4 01 FC F8 66 EA 1D 32 9C FF 9A B0 B4 DE 30 19 56 14 D5 46 69 57 DB 29 7E F3 72 6A B6 D2 2E 20 E9 F1 CE BF 1D 40 11 3F F4 CF 15 5F 80 D0 E0 50 E6 53 94 FD AE FC F4 5B 73 90 CE 50 1E 30 25 63 49 B7 19 9F 69 1A 1D F0 E9 B4 A8

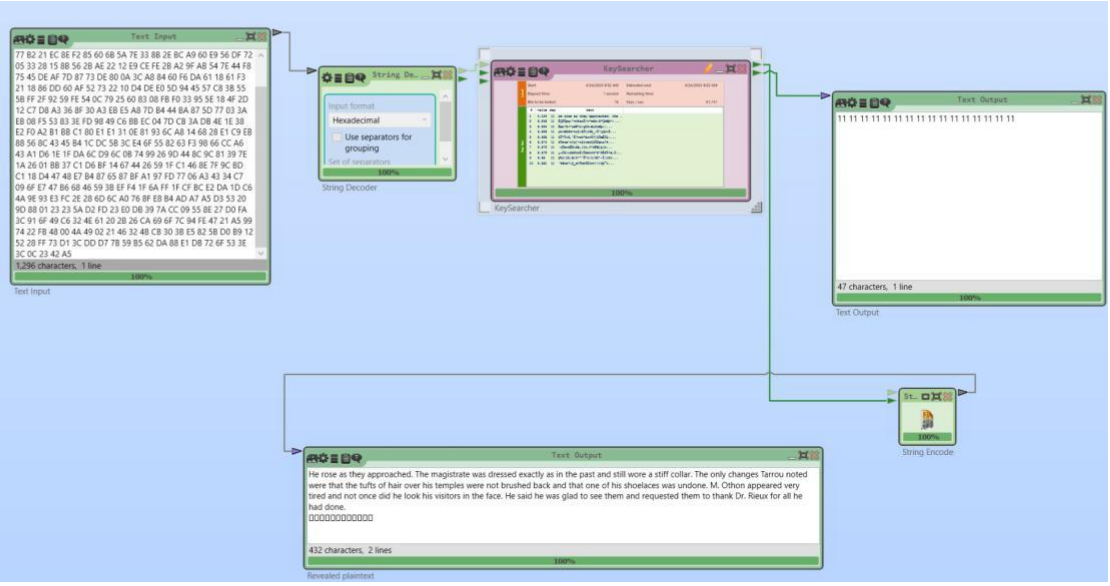
31 39 E8 6D 99 58 D7 1F E7 F2 A8 13 10 C0 06 60 39 D9 69 D6 50 F1 1D D0 6E 12 DF A0 2E 05 64 55 49 46 3C 61 8A E7 88 75 3A DC BB FB 6F DD 5D 8F 5B 24 D5 6D C6 B7 A5 A6 AE F0 7A F0 85 B8 5C 77 BE 84 47 C9 F0 B9 29 34 FB 85 A4 AE 64 7E F2 27 AF 5A C7 D6 A9 D9 72 C9 DF E4 75 E5 8F 27 79 AE 09 42 D3 65 C0 C3 1A A1 44 B0 05 76 F5 B5 84 1C B4 91 3C 78 26 DD E2 13 FB 9D D0 DE E2 50 B1 6E C7 D6 42 9E DA E6 13 A9 5E 4F B5 46 51 91 18 F6 52 5B BD C5 4C 89 11 C3 56 49 71 2C CD 45 BE C5 B5 AB B3 B0 6D D4 25 05 30 9A FA 39 40 6D 96 36 C7 B6 FD AB 84 95 27 26 2F 30 F7 5C 5D C5 4E 92 08 74 8B 8A FA 38 F9 64 0A 5F 2E A8

Ερώτηση 2.13

"***1A F0 28 83 AF AF 80 40 52 57 B0 00 F7 52 E4 50 ED E6 2A 90 A9 31 3A F7 A2 B8 A8 BB 3A 58 25 7D 59 8D CC 66 53 9F F3 22 C2 96 35 57 8D EC 7A 0C DA 4A B5 D0 14 A9 AF 26 17 34 FF F3 77 B2 21 EC 8E F2 85 60 6B 5A 7E 33 8B 2E BC A9 60 E9 56 DF 72 05 33 28 15 8B 56 2B AE 22 12 E9 CE FE 2B A2 9F AB 54 7E 44 F8 75 45 DE AF 7D 87 73 DE 80 0A 3C A8 84 60 F6 DA 61 18 61 F3 21 18 86 DD 60 AF 52 73 22 10 D4 DE E0 5D 94 45 57 C8 3B 55 5B FF 2F 92 59 FE 54 0C 79 25 60 83 08 FB F0 33 95 5E 18 4F 2D 12 C7 D8 A3 36 8F 30 A3 EB E5 A8 7D B4 44 BA 87 5D 77 03 3A EB 08 F5 53 83 3E FD 98 49 C6 BB EC 04 7D CB 3A DB 4E 1E 38 E2 F0 A2 B1 BB C1 80 E1 E1 31 0E 81 93 6C A8 14 68 28 E1 C9 EB 88 56 8C 43 45 B4 1C DC 5B 3C E4 6F 55 82 63 F3 98 66 CC A6 43 A1 D6 1E 1F DA 6C D9 6C 0B 74 99 26 9D 44 8C 9C 81 39 7E 1A 26 01 BB 37 C1 D6 BF 14 67 44 26 59 1F C1 46 8E 7F 9C BD C1 18 D4 47 48 E7 B4 87 65 87 BF A1 97 FD 77 06 A3 43 34 C7 09 6F E7 47 B6 68 46 59 3B EF F4 1F 6A FF 1F CF BC E2 DA 1D C6 4A 9E 93 E3 FC 2E 28 6D 6C A0 76 8F E8 B4 AD A7 A5 D3 53 20 9D 88 01 23 23 5A D2 FD 23 E0 DB 39 7A CC 09 55 8E 27 D0 FA 3C 91 6F 49 C6 32 4E 61 20 2B 26 CA 69 6F 7C 94 FE 47 21 A5 99 74 22 FB 48 00 4A 49 02 21 46 32 4B CB 30 3B E5 82 5B D0 B9 12 52 28 FF 73 D1 3C DD D7 7B 59 B5 62 DA 88 E1 DB 72 6F 53 3E 3C 0C 23 42 A5***"

Bytes γνωστού μέρους κλειδιού	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Χρόνος κρυπτανάλυσης	In a galaxy far, far away	In a galaxy far, far away	In a galaxy far, far away	In a galaxy far, far away	In a galaxy far, far away	In a galaxy far, far away	In a galaxy far, far away	15545 days and 10 hours	629 days and 12 hours	2 days and 11hours	13 mins	5 secs	4 secs	1 secs	1 secs

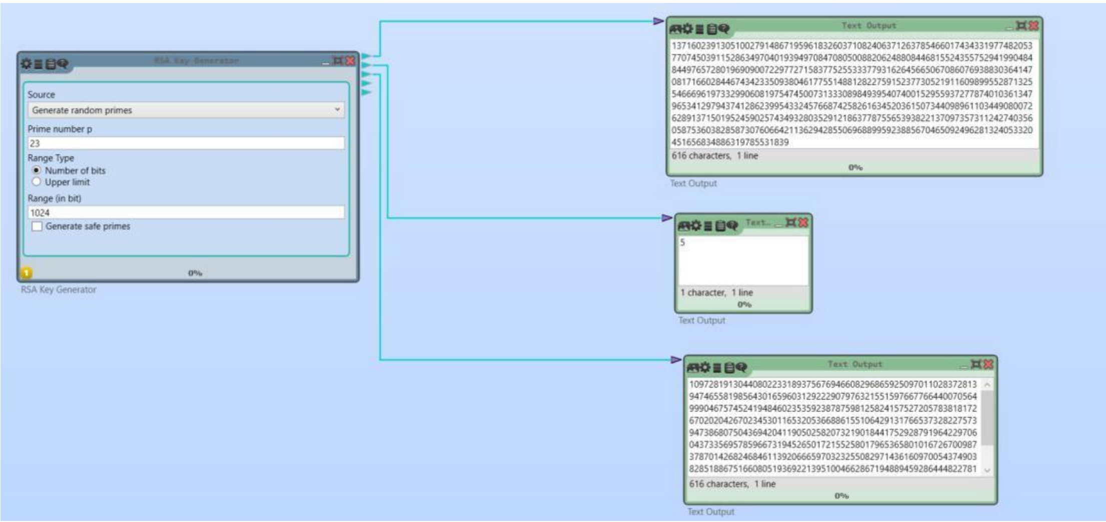
Η διάταξη που χρησιμοποιήσαμε είναι η εξής:



Παρατηρούμε ότι, όσο μειώνεται το γνωστό μήκος του κλειδιού, τόσο περισσότερος χρόνος χρειάζεται για την εύρεση του κρυπτοκειμένου. Αυτό συμβαίνει, καθώς πρέπει να βρεθούν όλοι οι συνδιασμοί κλειδιών για την αποκρυπτογράφηση. Οπότε, μικρό μήκος κλειδιού, σημαίνει ότι πρέπει να γίνουν περισσότερες αναζητήσεις ώστε να βρεθεί το κλειδί που αποκρυπτογραφεί το κρυπτοκείμενο.

Ερώτηση 2.14

Η διάταξη που χρησιμοποιήθηκε είναι η εξής:



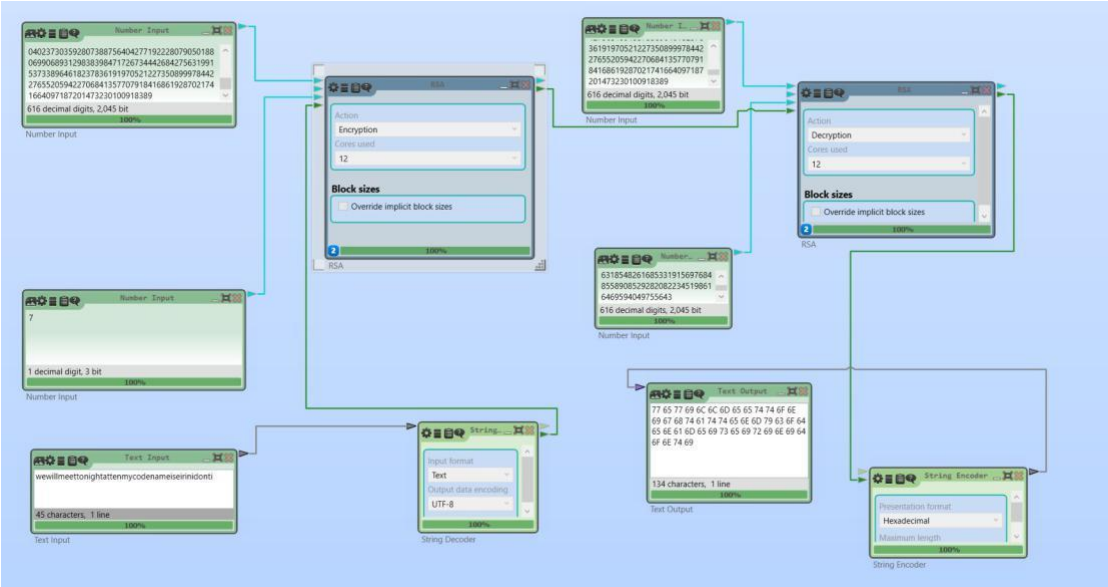
PUa = {e,N}	{7, 3285191352247885795058761667612010793272583966370123439676345183174684321594298378877771669552295144751071751497929670234132423681738215830146782022276204855402720360500530584569903188849223909017472675032219472610708582196747908273285636945458304589976856570766670375476603109779541100290481074422659633285589839437207887585783442562506723829846483370235417269962184877563892858788742199203170202808827522685760257567530402373035928073887564042771922280790501880699068931298383984717267344426842756319919</td>

	5373389646182378361919705212273508999784422765520594227068413577079184168619287021741664097187201473230100918389}
PRa = {d,N}	{2346565251605632710756258334008579138051845690264373885483103702267631658281641699198408335394496531965051251069949764452951731201241582735819130015911574896716228828928950417549930849178017077869623339308728194721934701569105648766632597818184503278554897550547621696769002221271100785921772196016185452346758618911275124878489921250544504484234394762322193869067966632164777874780012820817627168525081290656519695381704132623045489204236467535191406546077788503081519316645566979133669050053439783375844781190612814276099253174836575376251873431177631854826168533191569768485589085292820822345198616469594049755643,328519135224788579505876166761201079327258396637012343967634518317468432159429837887777166955229514475107175149792967023413242368173821583014678202227620485540272036050053058456990318884922390901747267503221947261070858219674790827328563694545830458997685657076667037547660310977954110029048107442265963328558983943720788758578344256250672382984648337023541726996218487756389285878874219920317020280882752268576025756753040237303592807388756404277192228079050188069906893129838398471726734442684275631991537338964618237836191970521227350899978442276552059422706841357707918416861928702174166409718720147323010091838
Pub = {e,N}	{5,137160239130510027914867195961832603710824063712637854660174343319774820537707450391152863497040193949708470805008820624880844681552435575294199048484497657280196909007229772715837752553337793162645665067086076938830364147081716602844674342335093804617755148812822759152377305219116098995528713255466696197332990608197547450073133308984939540740015295593727787401036134796534129794374128623995433245766874258261634520361507344098961103449080072628913715019524590257434932803529121863778755653938221370973573112427403560587536038285873076066421136294285506968899592388567046509249628132405332045165683488631978553183 9}
PRb = {d,N}	{1097281913044080223318937567694660829686592509701102837281394746558198564301659603129222907976321551597667766440070564999046757452419484602353592387875981258241575272057838181726702020426702345301165320536688615510642913176653732822757394738680750436942041190502582073219018441752928791964229706043733569578596673194526501721552580179653658010167267009873787014268246846113920666597032325508297143616097005437490382851886751660805193692213951004662867194889459286444822781685919752100371926845815785680326713956794529806627686089926233171846695203210300163040178008751282216049806455135146518283995141659754744195725,137160239130510027914867195961832603710824063712637854660174343319774820537707450391152863497040193949708470805008820624880844681552435575294199048484497657280196909007229772715837752553337793162645665067086076938830364147081716602844674342335093804617755148812822759152377305219116098995528713255466696197332990608197547450073133308984939540740015295593727787401036134796534129794374128623995433245766874258261634520361507344098961103449080072628913715019524590257434932803529121863778755653938221370973573112427

	74035605875360382858730760664211362942855069688995923885670465092496281324053320451656834886319785531839}

Ερώτηση 2.15

Παραθέτουμε την ζητούμενη διάταξη:



Επειδή η τιμή N έχει μεγάλο μήκος, τότε είναι πιο ασφαλής μέθοδος κρυπτογράφησης.