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: ΚΥΡΙΑΚΟΠΟΥΛΟΣ ΓΙΩΡΓΟΣ
Αριθμός Μητρώου: 03118153
Εξάμηνο: 8ο

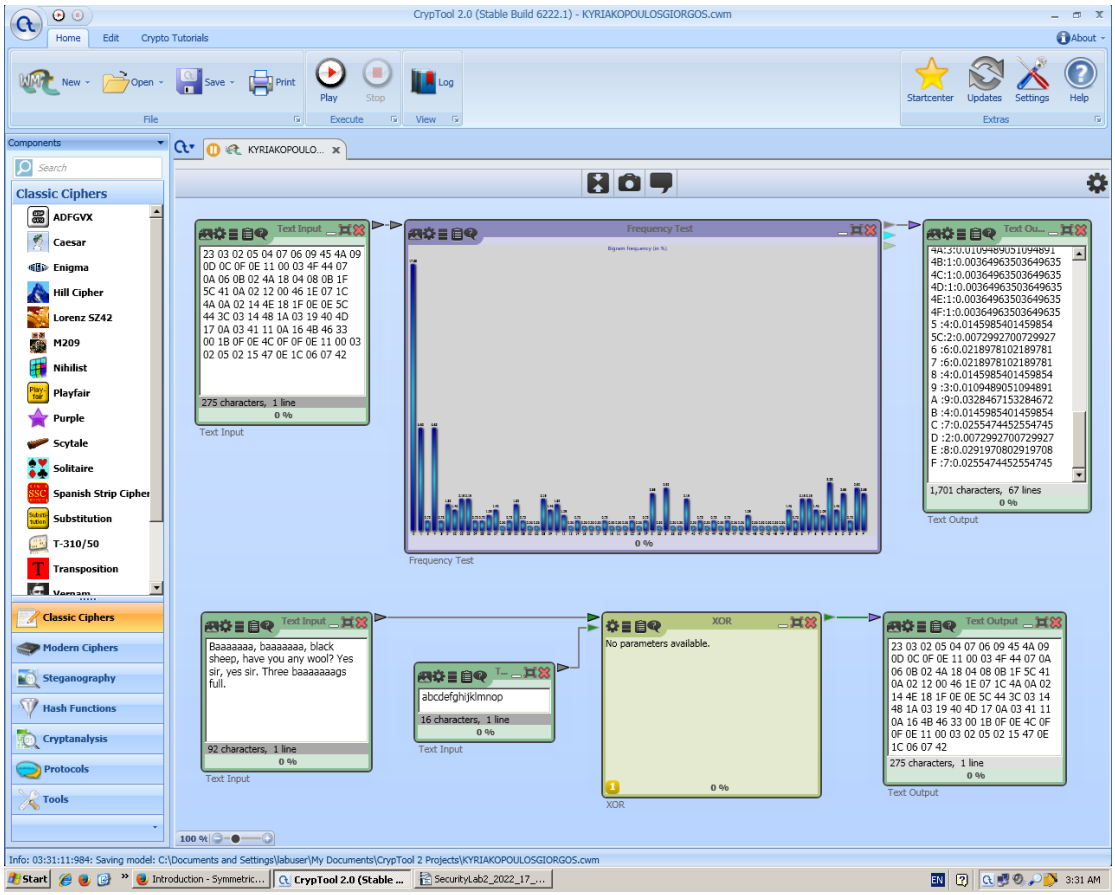
Ερώτηση 2.1

"***Baaaaaaa, baaaaaaa, black sheep, have you any wool? Yes sir, yes sir. Three baaaaaaags full.***"

Φαίνεται ότι ο χαρακτήρας a εμφανίζεται συχνότερα στο μη κρυπτογραφημένο κείμενο.

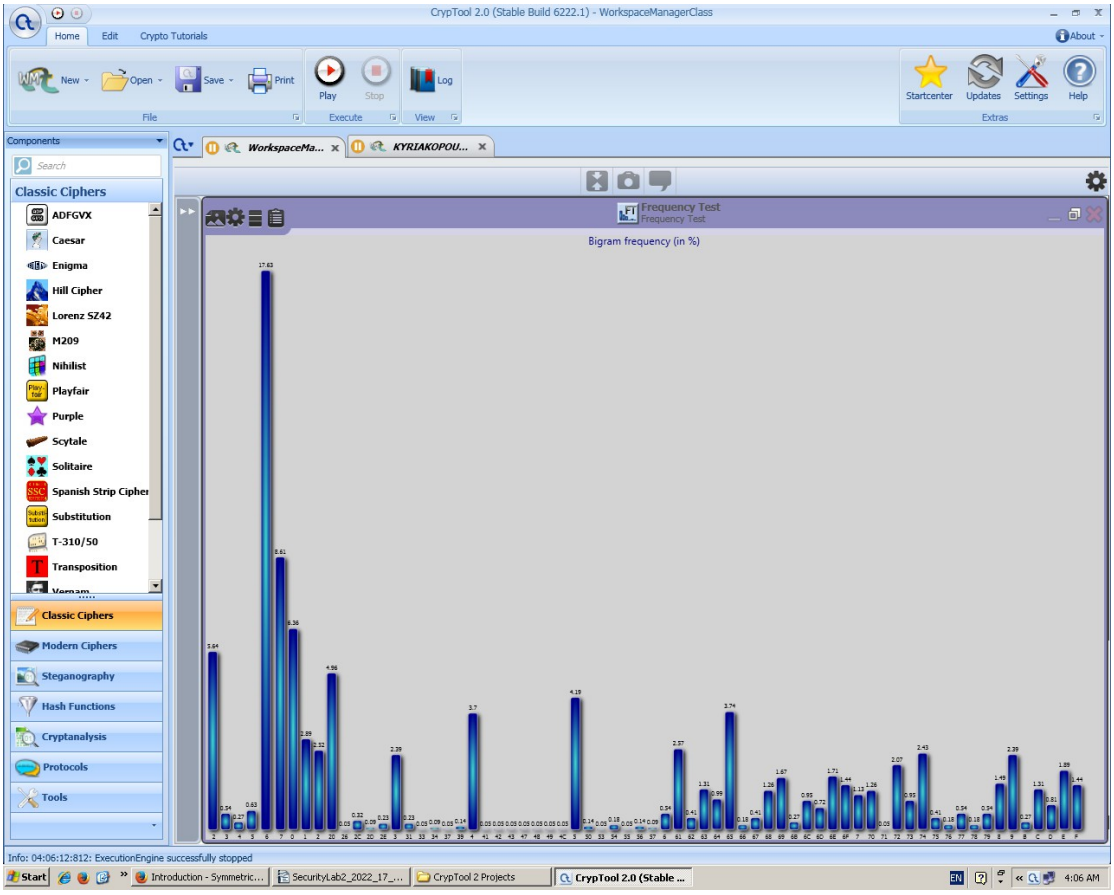
	Ciphertext/ K1	**Ciphertext/ K2**	**Ciphertext/ K3**	**Ciphertext/ K4**	**Ciphertext/K5**
Key → char	a	ab	abcd	abcdefgh	abcdefghijklmnop
Key → Hex	61	61 62	61 62 63 64	61 62 63 64 65 66 67 68	61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70
Key → Bits	0110 0001	0110 0001 0110 0010	0110 0001 0110 0010 0110 0011 0110 0100	-	-
Συχνότερο δίγραμμα	00	03	02	07	02 - 03 - 0E

Πλήθος εμφανίσεών του	24	15	9	8	6



Ερώτηση 2.2

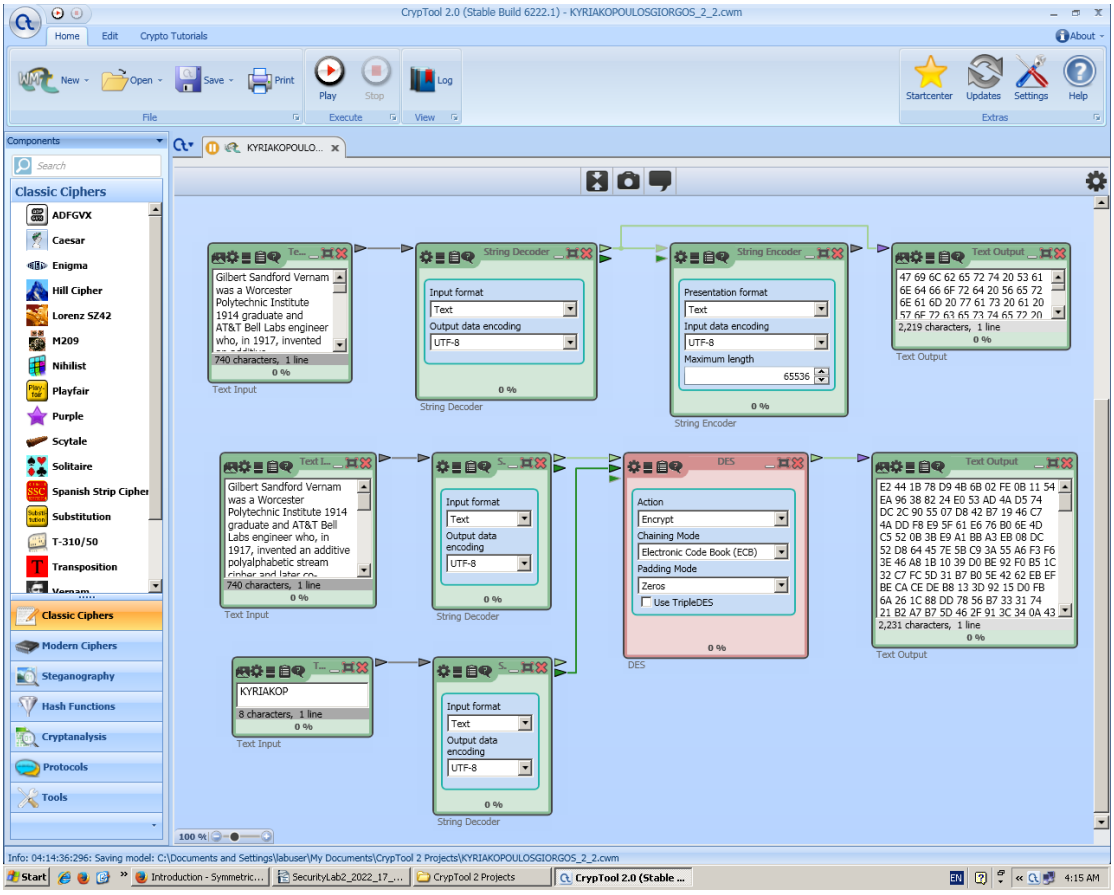
"***Gilbert Sandford Vernam was a Worcester Polytechnic Institute 1914 graduate and AT&T Bell Labs engineer who, in 1917, invented an additive polyalphabetic stream cipher and later co-invented an automated one-time pad cipher. Vernam proposed a teleprinter cipher in which a previously prepared key, kept on paper tape, is combined character by character with the plaintext message to produce the ciphertext. To decipher the ciphertext, the same key would be again combined character by character, producing the plaintext. Vernam later worked for the Postal Telegraph Company, and became an employee of Western Union when that company acquired Postal in 1943. His later work was largely with automatic switching systems for telegraph networks.***"



Το δίγραμμα 20 που αντιστοιχεί στο κενό εμφανίζει υψηλή συχνότητα όπως αναμενόταν, μαζί με τα διγράμματα 61, 65, 69, 6E, 6F, 72, 74 που αντιστοιχούν στα γράμματα a, e, i, n, o, r, t. Επίσης, τα διγράμματα 41 έως και 5A εμφανίζουν πολύ χαμηλότερη συχνότητα, αντιστοιχώντας στα κεφαλαία γράμματα, που εμφανίζονται πιο σπάνια από τα αντίστοιχα πεζά, όπως φαίνεται και στο ιστόγραμμα στη μεσαία και στη δεξία περιοχή αντίστοιχα.

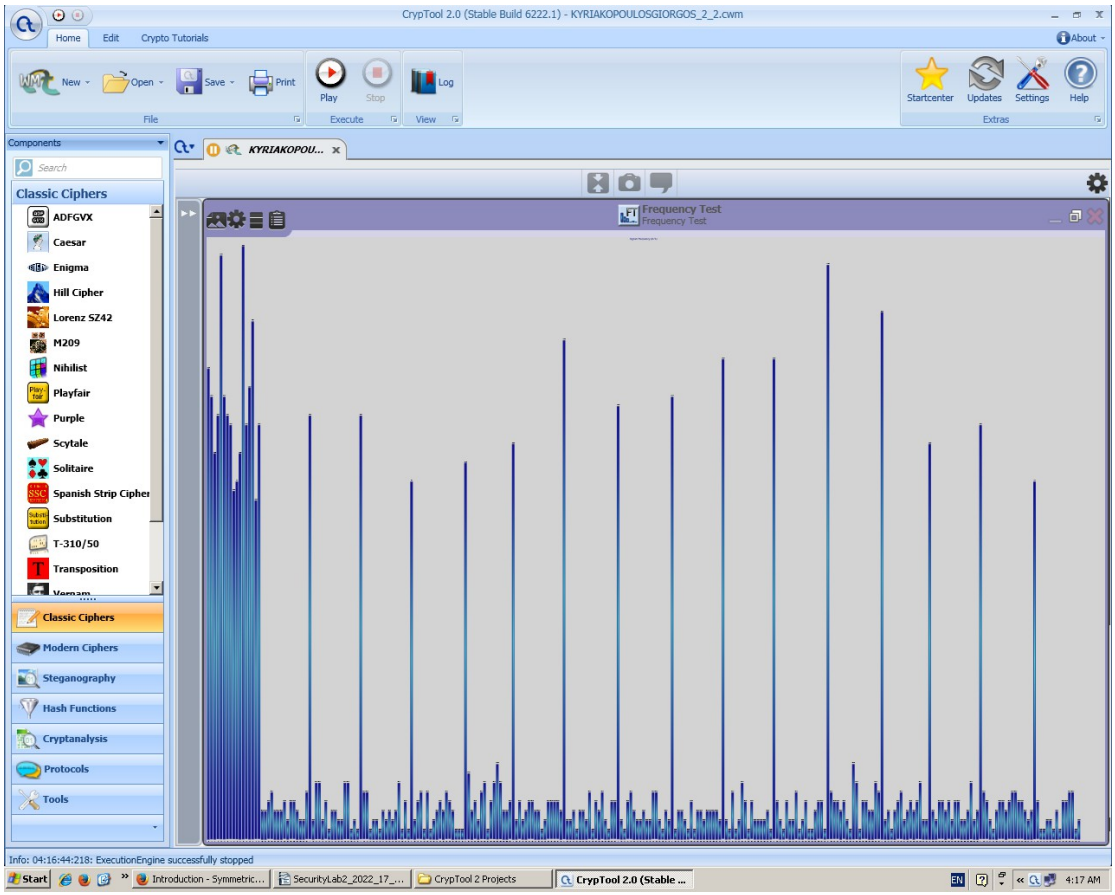
Το κλειδί που χρησιμοποίησα είναι KYRIAKOP, με μήκος 8 χαρακτήρες ή 64 bit, που είναι το επιθυμητό μήκος για τον DES, ώστε να δημιουργήσει τα διάφορα permutations των 56 bit.

Το κρυπτοκείμενο δεν έχει το ίδιο μήκος με το αρχικό κείμενο, αλλά περίπου τριπλάσιο του. Αυτό οφείλεται στη μετατροπή του ASCII κειμένου εισόδου σε HEX στην έξοδο, αφού κάθε ένας χαρακτήρας της εισόδου αντιστοιχεί σε δύο χαρακτήρες του διγράμματος HEX συν ένα κενό για το διαχωρισμό τους.



“E2 44 1B 78 D9 4B 6B 02 FE 0B 11 54 EA 96 38 82 24 E0 53 AD 4A D5 74 DC 2C 90 55 07 D8 42 B7 19 46 C7 4A DD F8 E9 5F 61 E6 76 B0 6E 4D C5 52 0B 3B E9 A1 BB A3 EB 08 DC 52 D8 64 45 7E 5B C9 3A 55 A6 F3 F6 3E 46 A8 1B 10 39 D0 BE 92 F0 B5 1C 32 C7 FC 5D 31 B7 B0 5E 42 62 EB EF BE CA CE DE B8 13 3D 92 15 D0 FB 6A 26 1C 88 DD 78 56 B7 33 31 74 21 B2 A7 B7 5D 46 2F 91 3C 34 0A 43 02 A3 B9 67 43 F8 8D 1C 7B 24 C6 96 0F D8 EA B1 38 11 58 27 0A 1C 48 30 41 64 99 89 89 B0 AE 11 80 4F E2 ED 59 C5 E9 41 77 D3 42 E7 6F 4A 34 CE C3 C1 1B E8 9C 4D 96 BC 11 4F A9 F2 70 A5 B1 32 D7 7A 96 82 F9 FB CA 8F 12 92 B7 45 AD E8 C0 03 5B CD D5 D4 A0 49 CD 49 36 0F CF 54 8B 08 D0 27 3A 38 17 66 55 CD 57 FD C5 36 11 F1 21 8E 10 B4 7C 5D 49 AE 7E E5 D6 2C 28 23 5D 25 C9 9E 18 9D 58 45 E4 7C 27 37 E0 BF 6E D4 7A 3A 8A 95 46 0D 65 25 F7 84 50 6C DB 20 D9 D3 02 53 73 D1 17 DF 6F 0B 90 B3 F5 2B 41 F9 F8 B3 0C 7F 64 E1 81 E9 A6 34 C9 34 E1 AB 37 52 F4 A9 9E 73 0E F3 C1 05 86 AC 8D F6 74 6E 4A 67 06 5E 67 BF 32 5C E4 1A 4B 6F 8A 8C B5 86 C5 4F 45 97 D7 1B FC 73 55 0F 9E BA A9 BF A0 56 4A ED 2A DD 9A 5E 20 68 00 A0 B2 39 6E 97 E7 17 86 5C 9F 93 61 B0 99 EB 2C 79 04 1C BB 20 76 EF 12 2B 06 77 06 09 CC A3 3C A1 8C 1C 4B 7B 5A 12 8B AC EC B8 6A 4D 4C DA 6D 6F 4C DD B3 B2 E4 CD 43 18 11 C0 E0 FC 2E DD 0C EE BE E5 00 E8 1B 62 C1 85 CC 5B 8B 95 A6 71 88 FE 81 32 87 CD 08 CA 57 0B 1E 04 28 A3 43 BD AA A6 84 6B 6C 86 49 0D 6B 54 C6 09 31 BD 92 E7 BE B4 DF 9C B8 ED 5B 70 7D 79 69 CB 9B D4 69 FB AC 20 E0 E3 EF 1F D8 46 B4 7B CF C6 DF DB C2 E1 49 DE 29 20 BE D9 E8 66 6B B7 BB 18 07 77 C6 EA 3A 5E 03 72 CD A9 03 13 57 12 37 F4 A0 21 2E 3B 9B 3B E6 E1 5A 2C EC 3A 4A 2C 34 7B 30 C6 8E E5 8C D5 47 F0 41 7A 08 56 49 4C 19 A4 4B 04 D6 5F 4B 60 67 0A D3 BC BD 75 B1 99 41 12 5C E6 EA D3 A2 2E D1 1E 1A 81 A4 B8 5C 7B 04 C3 AE 04 D6 31 29 B1 2D CC 4A 05 B2 0E 2E 89 AE 1B B8 45 B0 60 A8 BC 3C EC DA 38 44 9D B7 BA 0C 72 FC 63 CB 21 FC EA 8E 58 CB 05 3F 41 50 96 15 15 5F DC F9 9A 4B 46 65 EC B6 03 16 BA 7E 88 72 F0 BF 2B 3B 69 6B 48 32 97 35 99 F8 75 AD 62 8D AF 98 E9 67 39 F0 73 48 29 96 82 F9 FB CA 8F 12 92 7F BA 00 48 A6 72 E6

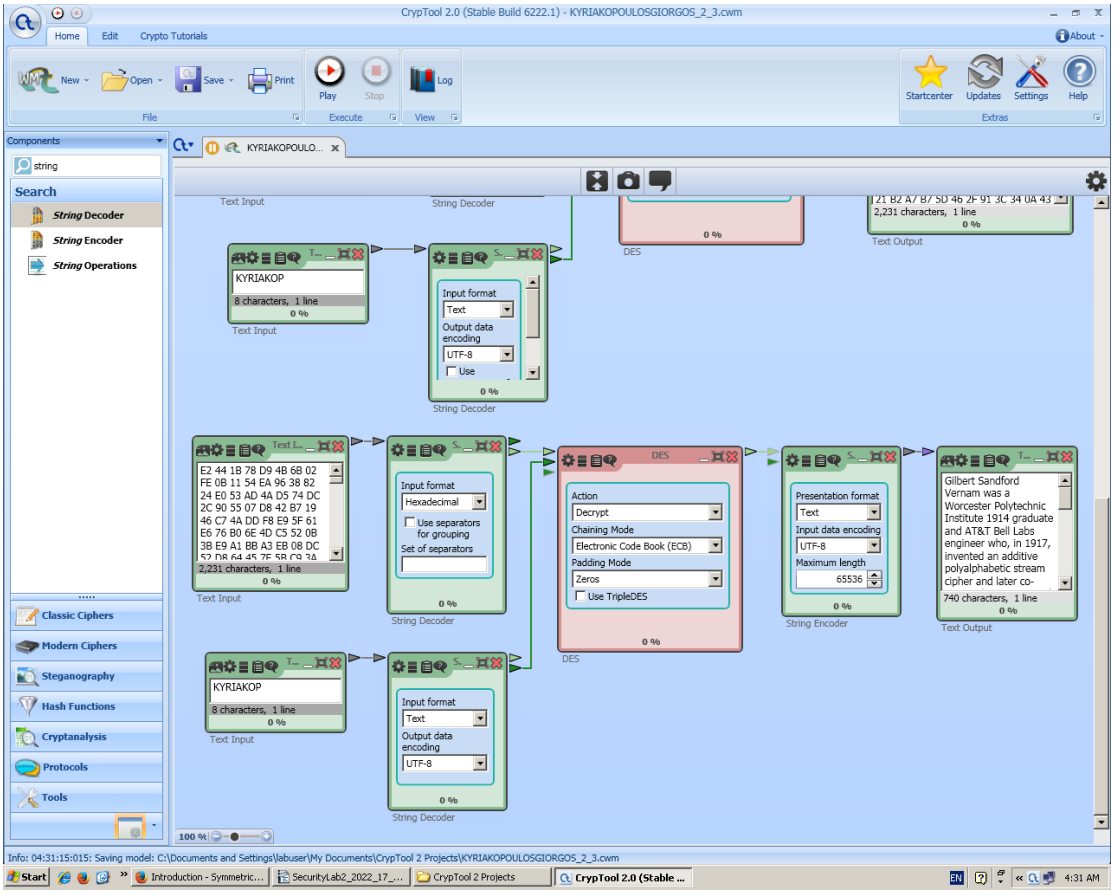
C3 BF E5 21 BE BB 4A 15 B4 EE AD D4 97 D9 4F 0F EB B7 F6 0F 41 69 FB E0 CC 7A 7A 56 D6 1D 2C 73 6A A5 0A 52 07 2A DD B8 65”



Παρατηρώ ότι με εξαίρεση τις υψηλές συχνότητες που εμφανίζονται σε μονά γράμματα ή αριθμούς και δεν μας ενδιαφέρουν, οι υπόλοιπες συχνότητες είναι σχετικά ομοιόμορφα κατανεμημένες, κάτι που είναι επιθυμητό από έναν αλγόριθμο κρυπτογράφησης.

Ερώτηση 2.3

Για την αποκρυπτογράφηση χρησιμοποίησα το ίδιο κλειδί που χρησιμοποίησα και για την κρυπτογράφηση, δηλαδή το KYRIAKOP. Επίσης, διάλεξα το ίδιο mode of operation που είχα και κατά την κρυπτογράφηση, δηλαδή το Electronic Code Block (ECB).

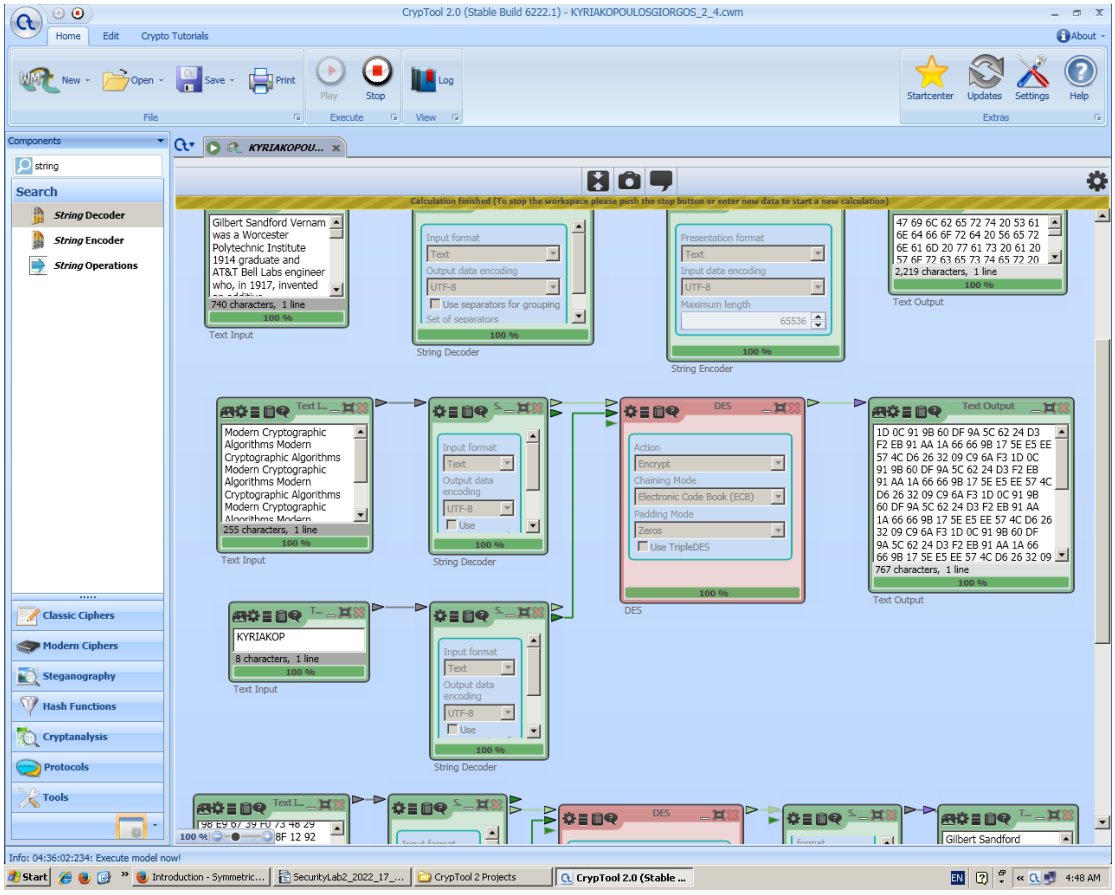


Ερώτηση 2.4

"***Modern Cryptographic Algorithms Modern Cryptographic Algorithms Modern Cryptographic Algorithms Modern Cryptographic Algorithms Modern Cryptographic Algorithms Modern Cryptographic Algorithms Modern Cryptographic Algorithms***"

Παρατηρώ ότι το μη κρυπτογραφημένο κείμενο που επαναλαμβάνεται κάθε 32 χαρακτηρές οδηγεί σε επανάληψη 32 διγραμμάτων HEX στο κρυπτογραφημένο κείμενο. Αυτό οφείλεται προφανώς στο γεγονός ότι χρησιμοποίειται ECB operation mode, το οποίο παίρνει block των 64 bit και τα κρυπτογραφεί ανεξάρτητα από τα υπόλοιπα, όλα όμως με το ίδιο κλειδί, όπως φαίνεται και από το διάγραμμα στο φύλλο. Επομένως, κάποιο επαναλαμβανόμενο κείμενο θα εμφανίζεται και στην έξοδο ως επαναλαμβανόμενα κομμάτια κρυπτοκειμένου.

Αυτή η επανάληψη είναι μία αδυναμία του αλγορίθμου, σε θέματα ασφάλειας. Για να ξεπεραστεί πρέπει να υπάρχει κάποιος τρόπος να παράγεται διαφορετικό μπλοκ σε περίπτωση επαναλάψης ενός ήδη παραγμένου μπλοκ. Ένας τέτοιος τρόπος εφαρμόζεται και στο operation mode CBC (Cipher Block Chaining), όπου κάθε block πριν κρυπτογραφηθεί περνάει από μία XOR μαζί με το τελευταίο κρυπτογραφημένο block, ώστε να αποφευχθεί η επανάληψη του σε περίπτωση που θα είχαν ίδιο παραγώμενο κρυπτοκείμενο.



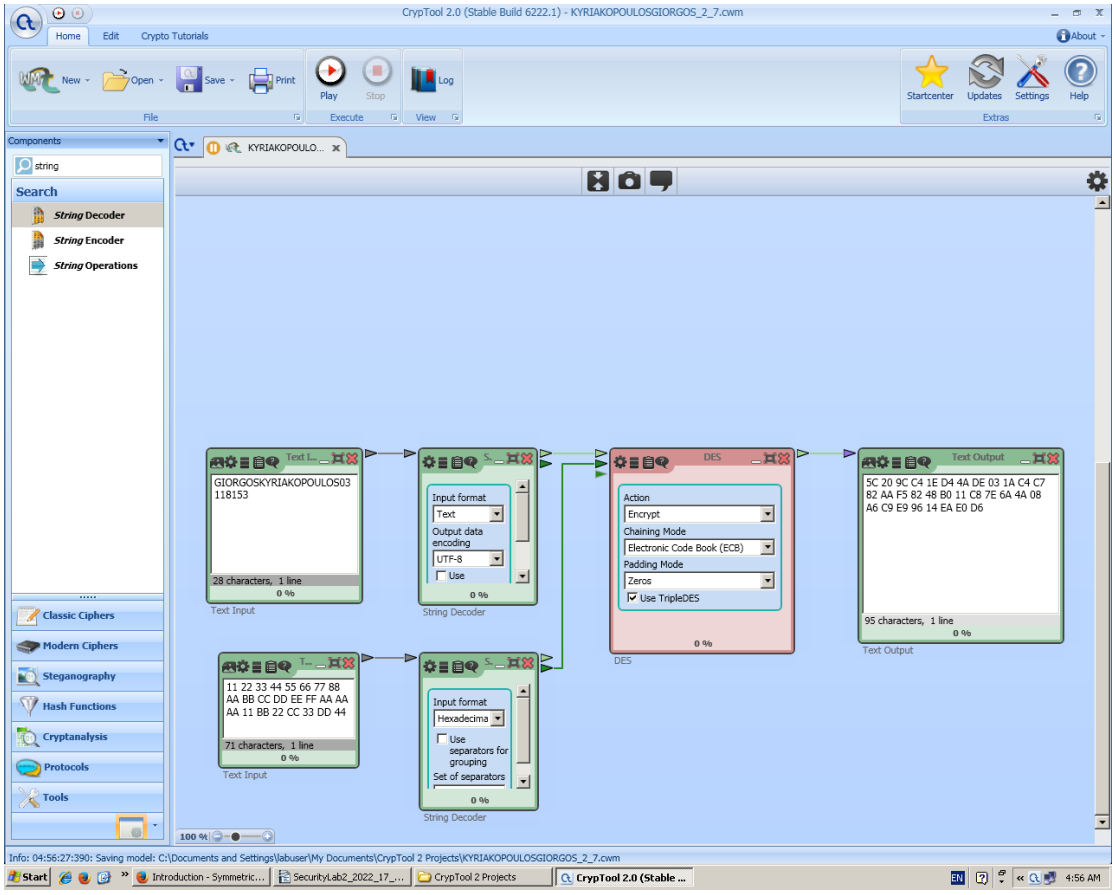
Ερώτηση 2.5

Ο χαρακτήρας του αρχικού κειμένου που μεταβάλατε και η θέση του στο κείμενο	Τρόπος λειτουργίας αλγορίθμου	Αριθμός χαρακτήρων που μεταβλήθηκαν στο κρυπτοκείμενο
Θέση ??, Χαρακτήρας ??	ECB	
Θέση ??, Χαρακτήρας ??	CBC	
Θέση ??, Χαρακτήρας ??	CFB	
Θέση ??, Χαρακτήρας ??	OFB	
Θέση ??, Χαρακτήρας ??	CTR	

Ερώτηση 2.6

Άγνωστα bits του κλειδιού	8	16	24	32	40	48	56	64
Χρόνος								

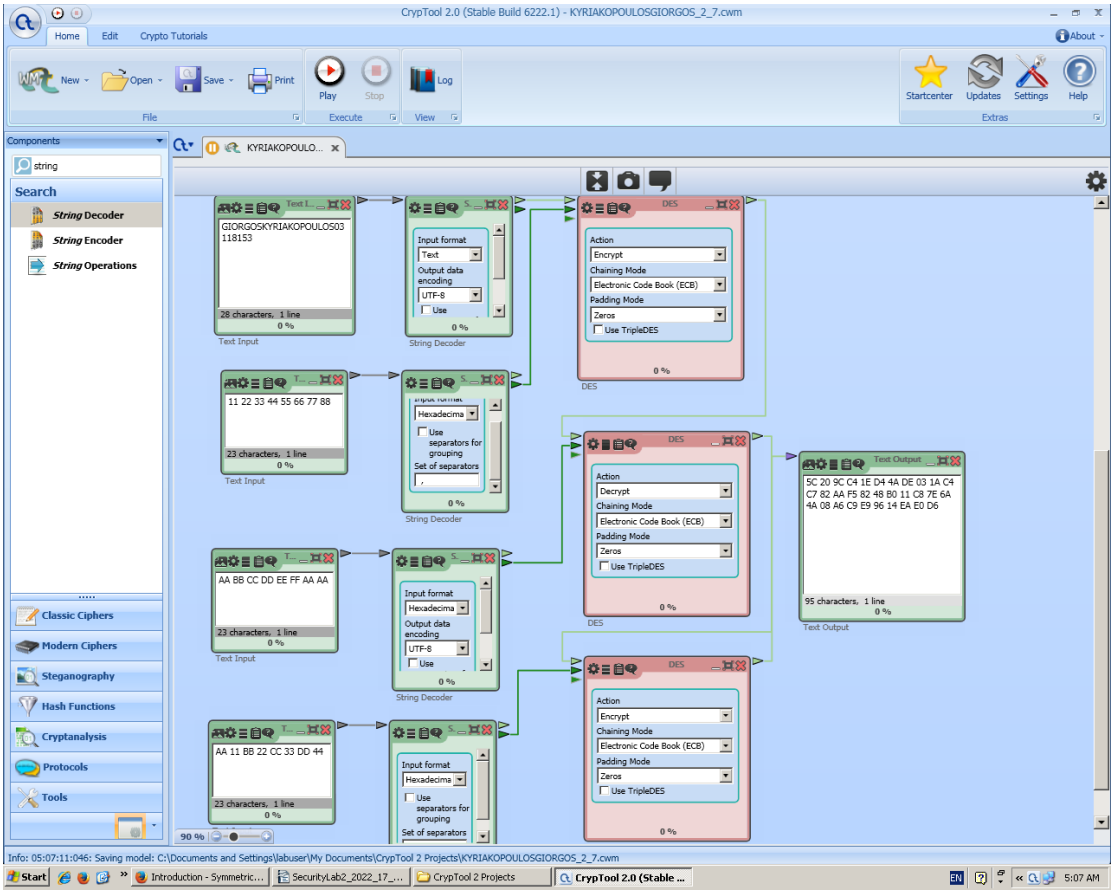
Ερώτηση 2.7



“5C 20 9C C4 1E D4 4A DE 03 1A C4 C7 82 AA F5 82 48 B0 11 C8 7E 6A 4A 08 A6 C9 E9 96 14 EA E0 D6”

Ερώτηση 2.8

Για να πάρω το ίδιο αποτέλεσμα με τον 3DES, μέσω της χρήσης του απλού DES, θα βάλω 3 DES στη σειρά σε Encrypt, Decrypt και Encrypt action, με αντίστοιχα κλειδιά K1 = 11 22 33 44 55 66 77 88, K2 = AA BB CC DD EE FF AA AA, K3 = AA 11 BB 22 CC 33 DD 44, που είναι αντίστοιχα το σπάσιμο του 192 bit κλειδιού του 3DES σε τρία κλειδιά των 64 bit.



Ερώτηση 2.9

Ερώτηση 2.10

"***He thought of Balducci. He had hurt him, for he had sent him off in a way as if he didn't want to be associated with him. He could still hear the gendarme's farewell and, without knowing why, he felt strangely empty and vulnerable. At that moment, from the other side of the schoolhouse, the prisoner coughed. Daru listened to him almost despite himself and then furious, threw a pebble that whistled through the air before sinking into the snow. That man's stupid crime revolted him, but to hand him over was contrary to honor. Merely thinking of it made him smart with humiliation. Dary got up, walked in a circle on the terrace, waited motionless, and then went back into the schoolhouse.***"

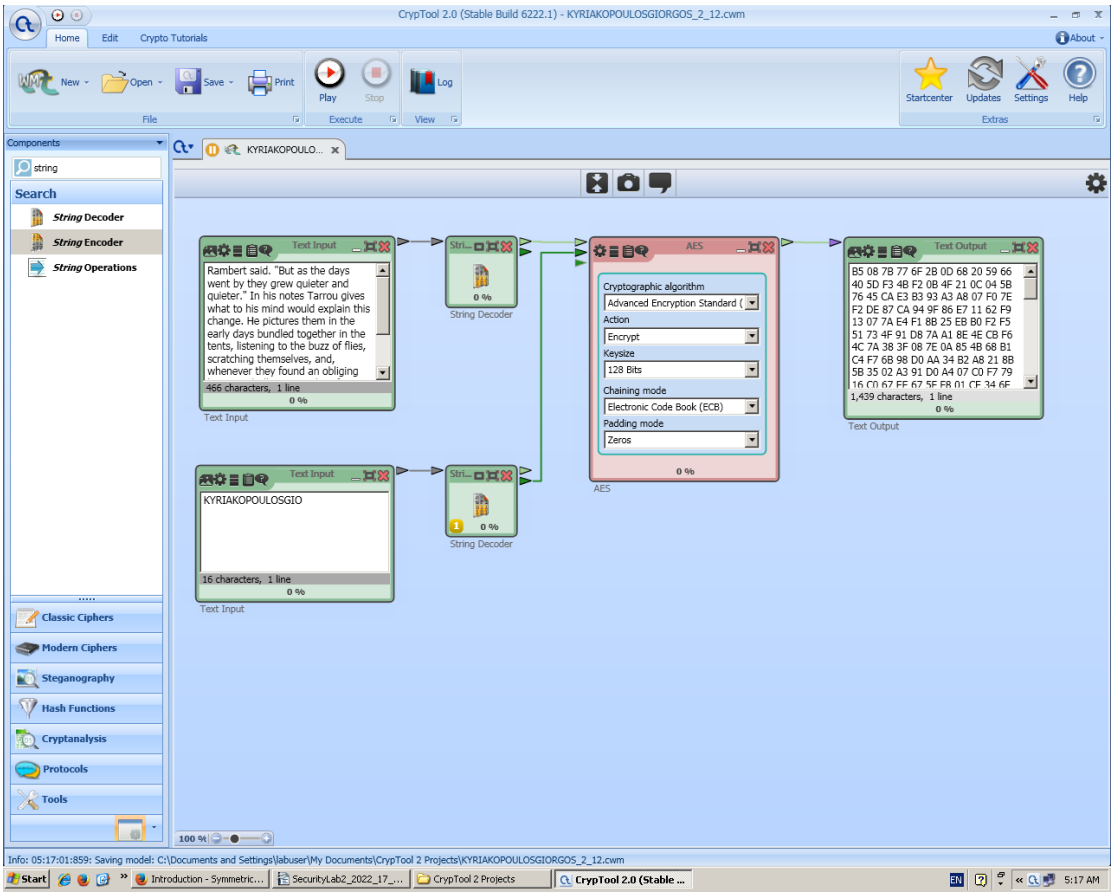
Ερώτηση 2.11

Ερώτηση 2.12

"***Rambert said. "But as the days went by they grew quieter and quieter." In his notes Tarrou gives what to his mind would explain this change. He pictures them in the early days bundled together in the tents, listening to the buzz of flies, scratching themselves, and, whenever they found an obliging listener,***

shrilly voicing their fear or indignation. But when the camp grew overcrowded, fewer and fewer people were inclined to play the part of sympathetic listener."

Χρησιμοποίησα κλειδί 16 χαρακτήρων (KYRIAKOPOULOSGIO), δηλαδή μήκους 128 bit, σύμφωνα και με το πως έχει ρυθμιστεί ο AES.



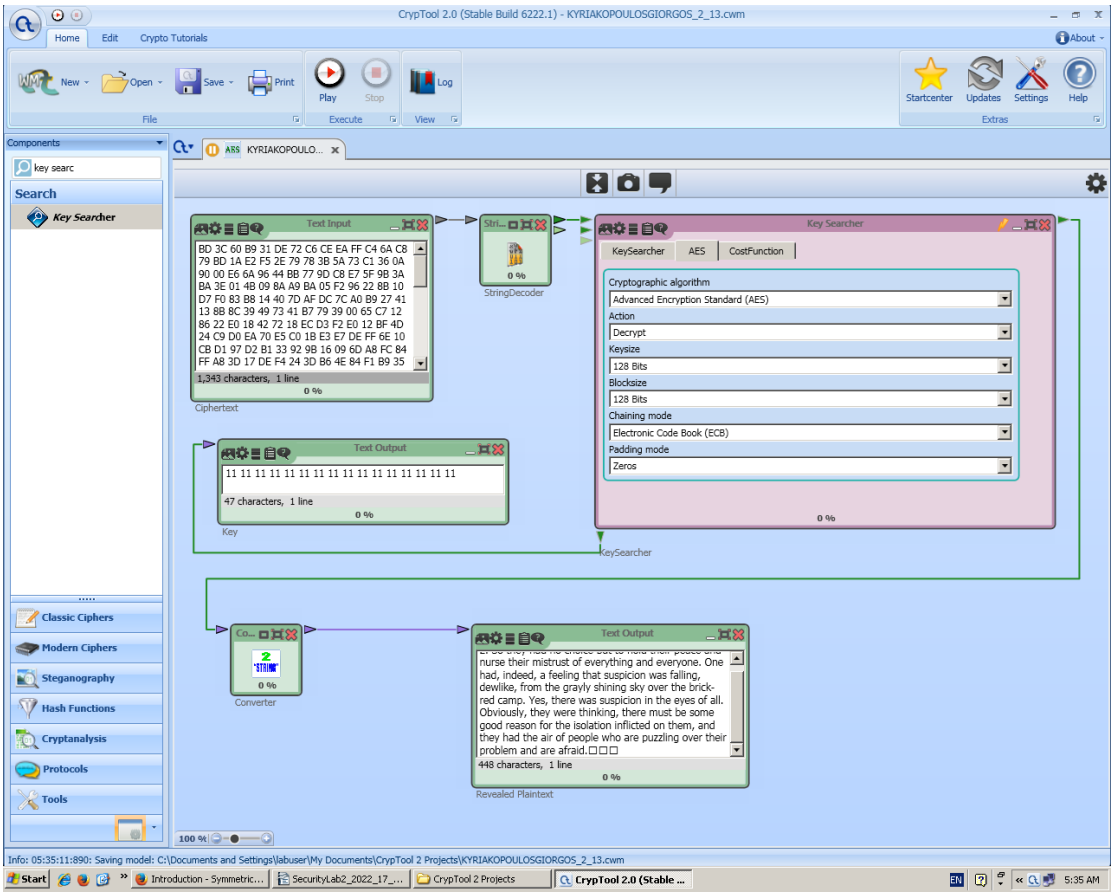
Ερώτηση 2.13

"***BD 3C 60 B9 31 DE 72 C6 CE EA FF C4 6A C8 79 BD 1A E2 F5 2E 79 78 3B 5A 73 C1 36 0A 90 00 E6 6A 96 44 BB 77 9D C8 E7 5F 9B 3A BA 3E 01 4B 09 8A A9 BA 05 F2 96 22 8B 10 D7 F0 83 B8 14 40 7D AF DC 7C A0 B9 27 41 13 8B 8C 39 49 73 41 B7 79 39 00 65 C7 12 86 22 E0 18 42 72 18 EC D3 F2 E0 12 BF 4D 24 C9 D0 EA 70 E5 C0 1B E3 E7 DE FF 6E 10 CB D1 97 D2 B1 33 92 9B 16 09 6D A8 FC 84 FF A8 3D 17 DE F4 24 3D B6 4E 84 F1 B9 35 9E 90 3F 4D A6 19 B9 FD 7B E0 19 60 79 33 78 44 B1 19 39 51 2F 5B F7 F7 29 D6 39 E5 DD EF C8 41 79 A3 B8 58 5B 9A 35 76 16 CE 8E D3 0F 2C 39 05 29 4E 83 EC AE A2 02 1B 2A FB 76 E4 EE 6B 1B 42 DB B9 B3 C9 58 A3 08 A4 07 18 72 C5 C0 FA 57 D0 C7 20 13 02 10 D0 04 BB 3E 1C 8D FE 2F 5F F3 F3 DA 67 9C 8D D0 52 FE E2 BC 69 FB 20 32 DB E8 31 D7 EF 07 EE A3 43 4A E3 96 B4 F9 7B 16 F4 7E 2A 9E AD 36 3F ED CB 49 BF A2 1D 5F 2A 5E 03 73 E1 89 CF 99 62 7F 7A 85 1C C9 02 D8 FE 7A EC 72 CD 27 05 C5 1F D3 68 95 11 75 61 75 0D D4 45 61 D6 10 16 2D 2D 04 86 13 56 F9 48 8B AD F1 6D 70 39 6D 90 A4 C5 3D B8 AF 25 4F 8B 44 CF 46 36 90 9E 5C CA ED B0 BB AE 93 20 7C 4B 14 9C CC FE 23 89 A8 BF 42 8F 4E FF F8 39 F3 C0 67 E1 49 38 2F 23 46 D9 2C AF 41 4E 4E AA CF D0 9C 8F 80 2A A8 54 8D 46 F5 B8 41***

34 41 A6 FC 5A 62 B8 39 51 BC 76 3D B5 58 B4 3F 13 6C 33 23 A2 DB D0 EE C0 D4 FD 5D 5E 25 D7 B0 36 48 61 94 EF DA EE 7B DA BD 69 7F FC 11 98"

Bytes γνωστού μέρους κλειδιού	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Χρόνος κρυπτανάλυσης	*	*	*	*	*	*	*	*	*	68 y	97 d	9 h	2 m	2 s	2 s

* incalculable



Ουσιαστικά, παρατηρούμε ότι, παρότι για μερικά missing byte του κλειδιού μπορεί η επίθεση να πετύχει σε λογικά χρονικά πλαίσια (2 second μέχρι 9 ώρες), μετά από μερικά ακόμα ο χρόνος ξεφεύγει εκθετικά σε αρκετά χρόνια και έπειτα σε μη υπολογίσιμο χρόνο (δηλαδή εξαιρετικά μεγάλο). Βλέπουμε, επομένως, ότι ο αλγόριθμος AES είναι ένας αλγόριθμος που είναι απίθανο να σπάσει με μία τέτοια επίθεση κρυπτανάλυσης.

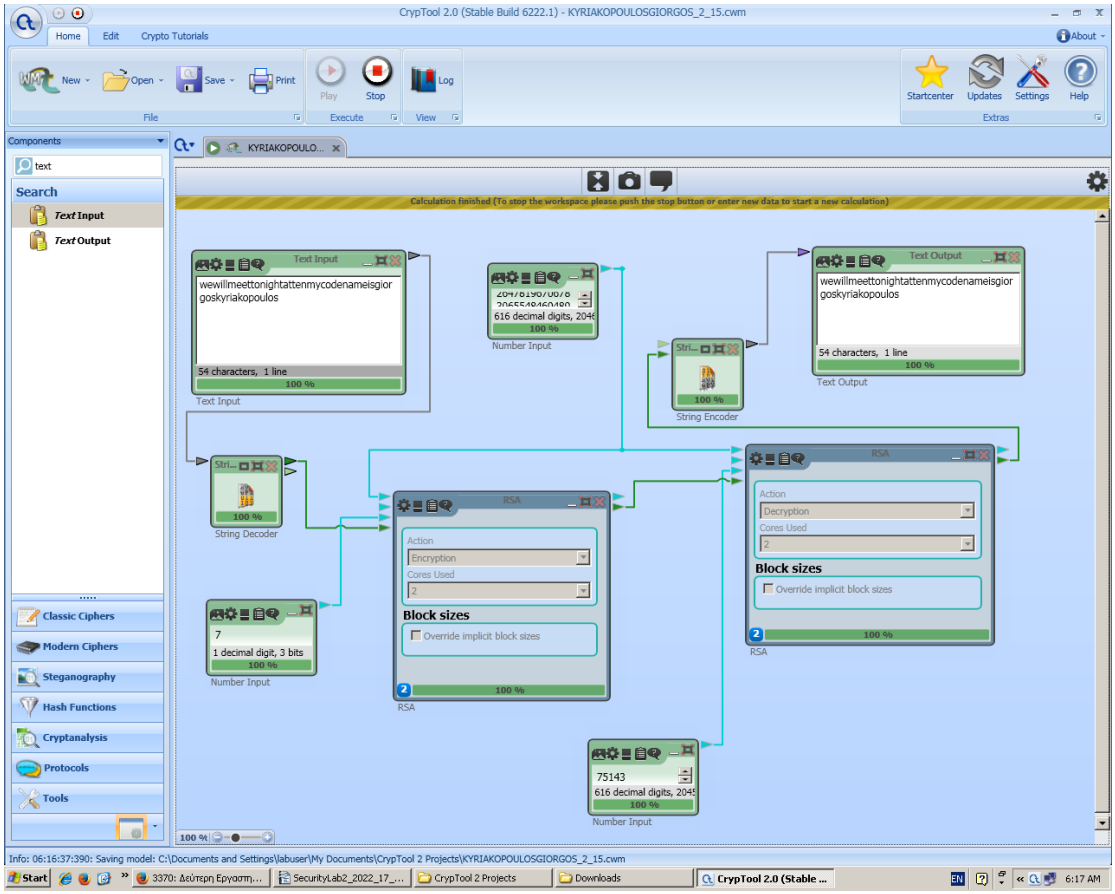
Ερώτηση 2.14

PUa =	{5,

{e,N}	119361875329472531278498727133101188999714916176452316569 479843955660580776725513678274899939181438589993985600646 606889183546282445130391181621325620928021388181090290049 446967093046189860610747563439947482122414853776168319529 703616347310912264434175410420019375300147787568086641095 974622683624946354650922452356316053010886355069297518261 349460179272891518828394798217169297966232617257288272462 565505278392947650039739020075212818682590503021230488795 295335844703525516534823346518970547757969432987122222958 329061536367741153687977428755266690705071780035372090870 084323098074155552340617149107872933756489993 07}
PRa = {d,N}	{954895002635780250227989817064809511997719329411618532555 8387516452846462138041094261991995134515087199518848051728 5511346837025956104312945297060496742417110544872232039557 5736744369518884885980507519579856979318830209346556237628 9307784872981154734032833601550024011823005446931287677969 8146899957083720736069081631182935221164147835393503126505 5917049900416965040434564619774606585074411472944773384634 1028022241016320680454162946062393482127772113550217237497 0124909643769619774394409157874654147306452796285147886696 3364925075034707743657021968598516453189326957273748888234 74442947388189219390874532299018430 1, 119361875329472531278498727133101188999714916176452316569 4798439556605807767255136782748999391814385899939856006466 0688918354628244513039118162132562092802138818109029004944 6967093046189860610747563439947482122414853776168319529703 6163473109122644341754104200193753001477875680866410959746 2268362494635465092245235631605301088635506929751826134946 0179272891518828394798217169297966232617257288272462565505 2783929476500397390200752128186825905030212304887952953358 4470352551653482334651897054775796943298712222295832906153 6367741153687977428755266690705071780035372090870084323098 074155552340617149107872933756489993 07}
Pub = {e,N}	{7, 416565098768820887282920493429604736319121884595877326733 4516371145624270181275748263755457091354924490440345019566 9824078685044921815526955624473261539308884490333585180281 5257723964586580085648700115031007203608826238719223040835 7011983482943045457614149331455349350514725783392337814505 7409122121530972961234795570122548654072584029547505106689 6614254776922829549116566270211687527279291618683119104001 2412653341734916307013368806202068788731033293199713506794 6489243483130777755205681584655156538803029714749001487072 7079806711916202836296092647819670678306554846948991829850 2490439411630717664580702388405111 91}
PRb = {d,N}	{357055798944703617671074708653946916844961615367894851485 8156889553392231583950641368933248935447078134663152873914 5563496015752790127594533392405652747979043848857358725955 5935191969645640073413171527169434745950422490330762606430 6010271556808324677954985141247442300441193528622003841004 9207818961312262536494962040735452230889989099061254931824 6970167505986102607419385572071437262658448843071311875952 5967809932346073889768845559634062170215614206465388230814 4677435595064894169350573871209533131470883121238965869947 9

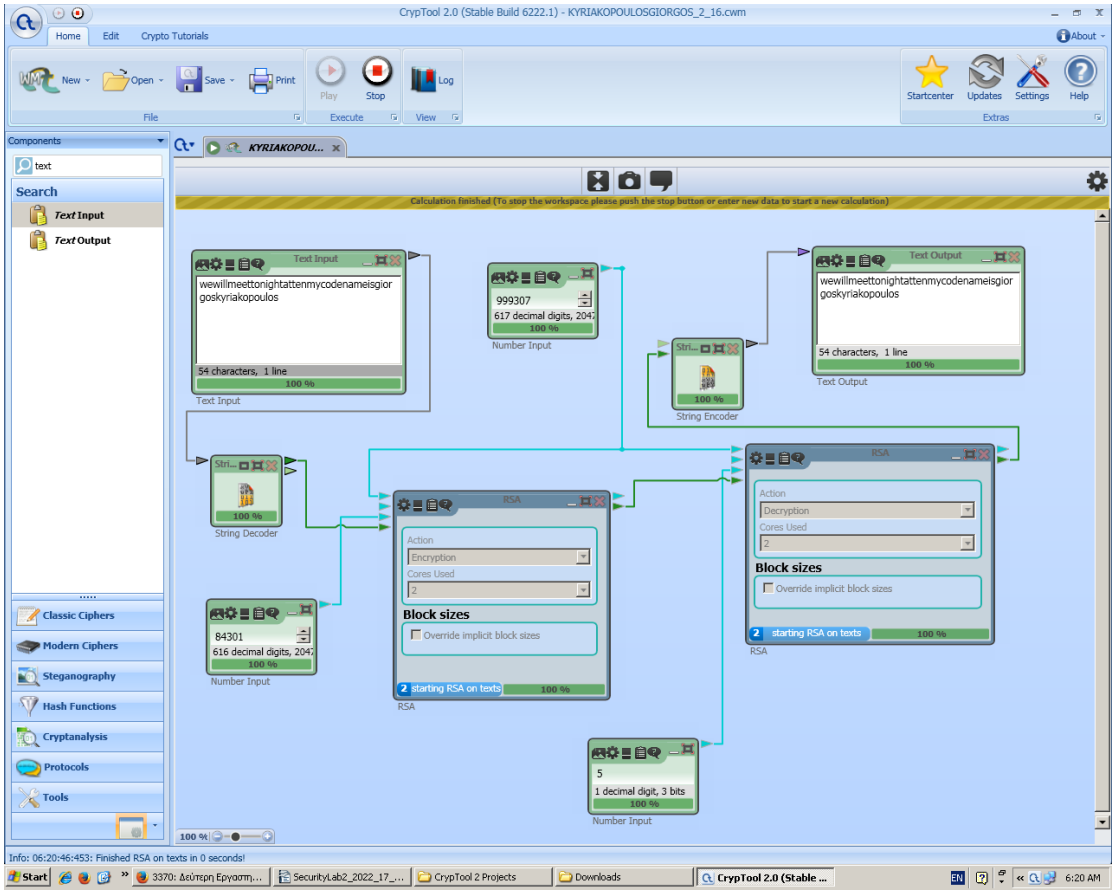
	553946509437104691936799910861831434699839093044732472479876489034189578146157350653592767514 3, 4165650987688208872829204934296047363191218845958773267334516371145624270181275748263755457091354924490440345019566982407868504492181552695562447326153930888449033358518028152577239645865800856487001150310072036088262387192230408357011983482943045457614149331455349350514725783392337814505740912212153097296123479557012254865407258402954750510668966142547769228295491165662702116875272792916186831191040012412653341734916307013368806202068788731033293199713506794648924354831307777552056815846551565388030297147490014870727079806711916202836296092647819670678306554846948991829850249043941163071766458070238840511191}

Ερώτηση 2.15



Τα κλειδιά είναι κατάλληλα, το αποκρυπτογραφημένο κείμενο στο στόχο Β είναι ίδιο με το αρχικό, ενώ έχει προηγηθεί η διαδικασία της κρυπτογράφησης με το public key του Β και της αποκρυπτογράφησης με το private key του Β. Επομένως, η προστασία της εμπιστευτικότητας έχει πετύχει.

Ερώτηση 2.16



Τα κλειδιά είναι κατάλληλα, το αποκρυπτογραφημένο κείμενο στο στόχο Β είναι ίδιο με το αρχικό, ενώ έχει προηγηθεί η διαδικασία της κρυπτογράφησης με το private key του Α και της αποκρυπτογράφησης με το public key του Α. Επομένως, η πιστοποίηση της ταυτότητας έχει πετύχει.

Ερώτηση 2.17