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.***"

	Ciphertext/K1	**Ciphertext/K2**	**Ciphertext/K3**	**Ciphertext/K4**	**Ciphertext/K5**
Key ☾ char					
Key ☾ Hex					
Key ☾ Bits					
Συχνότερο δίγραμμα					
Πλήθος εμφανίσεών του					

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."

Ερώτηση 2.3

Ερώτηση 2.4

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

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

Ερώτηση 2.8

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.*"

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															

Ερώτηση 2.14

PUa = {e,N}	
PRa = {d,N}	
Pub = {e,N}	
PRb = {d,N}	

Ερώτηση 2.15

Ερώτηση 2.16

Ερώτηση 2.17