Εργασία 1

Κωσταντίνος Σαΐτας - Ζαρκιάς - 2406
Οδυσσεύς Κρυσταλάκος - 2362

9 Απριλίου 2016

Θέμα 1

i) Η αρχή του Kerchoff υποστηρίζει ότι η ασφάλεια ενός κρυπτοσυστήματος δεν πρέπει να βασίζεται στη γνώση του κρυπτοσυστήματος αλλα στη γνώση του μυστικού κλειδιού. Αναλυτικότερα, σε μία κατάσταση(;;;) που η Αλίκη προσπαθεί να επικοινωνήσει με τον Μπομπ μέσω ενός μη ασφαλούς δίαυλου η Εύα έχει την δυνατότητα να υποκλέψει τα μηνύματα της Αλίκης αλλά να δεν μπορεί να τα διαβάσει καθώς δεν γνωρίζει το κλειδί με το οποίο έγινε η κρυπτογράφηση στο σύστημα που χρησιμοποίει η Αλίκη και ο Μπομπ.

ii) Ορισμός τέλειας ασφάλειας κατα Shannon: Αν κάποιος έχει ολόκληρο το κρυπτογραφημένο μήνυμα c, δεν μπορεί να αποκτήσει καμία πληροφορία για το αρχικό μήνυμα m.

Ορισμός τέλειας ασφάλειας: Ο ορισμός μπορεί να δωθεί και με ένα υποθετικό παράδειγμα στο οποίο η Αλίκη στέλνει ένα μήνυμα m0 με τέλεια κρυπτογράφηση στον Μπομπ και δίνει στην Εύα το κρυπτογραφημένο μήνυμα c, το αρχικό μήνυμα m0 και ένα άλλο διαφορετικό μήνυμα m1. Αν η Εύα δεν μπορεί να ξεχωρίσει το c αν προήλθε από το m0 ή το m1 και η επιλογή του σωστού βασίζεται σε πιθανότητα ακριβώς 50/50 τότε το κρυπτοσύστημα έχει τέλεια ασφάλεια.

iii) XKeyscore:

Το XKeyscore είναι ένα είδος μηχανής αναζήτησης για τους υπαλλήλους της NSA για την συλλογή πληροφοριών ενός στόχου από το ίντερνετ χωρίς την απαίτηση εντάλματος ή κάποιας υπογραφής ανώτερου πολιτειακού στελέχους. Το πρόγραμμα από μόνο του δεν παρεμβάλεται στις επικοινωνίες του στόχου που ορίζει ο χρήστης. Αντίθετα, μαζεύει τις πληροφορίες και υποκλέβει δεδομένα του στόχου από άλλες υπηρεσίες που αναφέρονται παρακάτω.

F6:
Συνεργασία CIA και NSA για αποστολές προς ξένους διπλωμάτες και πολιτικούς.

FORNSAT:
Υποκλοπή δεδομένων από ξένους δορυφόρους.

Overhead:
Συλλογή δεδομένων από κατασκοπικά αεροπλάνα, drones και δορυφόρους.

SSO (PRISM):
Συνεργασία NSA και ιδιωτικών εταιριών τηλεφωνιάς (π.χ Verizon) για την υποκλοπή δεδομένων και τηλεφωνικών συνομιλιών από οπτικες ίνες και κεραίες. Ένα πιο συγκεκριμένο παράδειγμα είναι η επιχείρηση MUSCULAR που έχει ως σκοπό την ελεύθερη πρόσβαση της NSA στους servers της google και της yahoo.

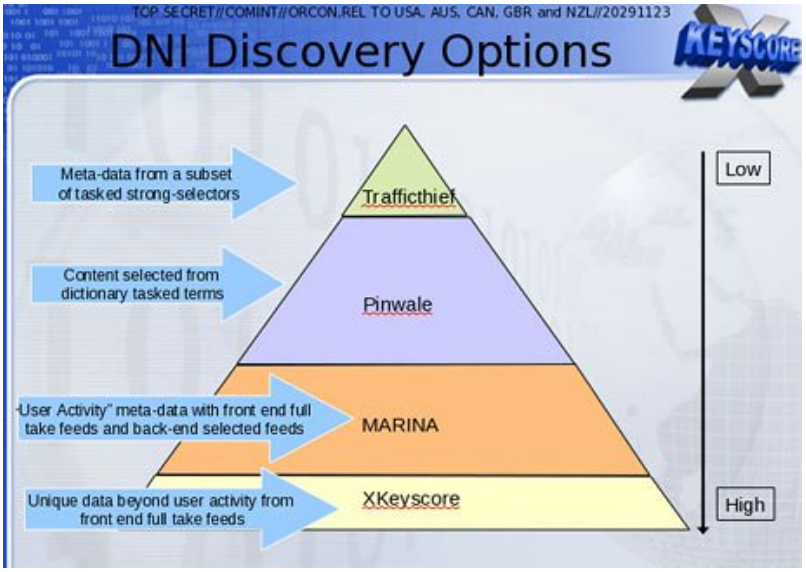
Επιθέσεις QUANTUM κινούμενες από το τμήμα TAO της NSA που ασχολείται κατα κόρον με cyberwarfare και hacking.

Από άλλες συνεργαζόμενες κυβερνήσεις όπως η Αυστραλία, ο Καναδάς, η Νέα Ζηλανδία και το Ηνωμένο Βασίλειο. Η συγκεκριμένη ομάδα αυτών των 5 χωρών μαζί με τις Η.Π.Α είναι γνωστή και ως Five Eyes ύστερα από την υπογραφή μυστικής συνθήκης στο τέλος του 2ου Παγκόσμιου Πόλεμου για την μεταξύ τους διάθεση πληροφοριών για κατασκοπία. Ο Snowden περιέγραψε την Five Eyes ως μια πολυεθνική οργάνωση πληροφοριών που δεν ακολουθεί τους νόμους των χωρών από τις οποίες αποτελείται.

Τεχνικές πληροφοριές:
Διαμοιρασμένο σε μεγάλα clusters σε διάφορα σημεία του κόσμου με πάνω από 700 servers και έλεγχο περίπου 150 sites.

Παραδείγματα δυνατοτήτων του προγράμματος:

- Πρόσβαση σε ιστορικό και mail οποιουδήποτε.
- Παρακολούθηση της 'κίνησης' (traffic) σε οποιουδήποτε site.
- Real-time γεωλογικός εντοπισμός φορητών συσκευών με πρόσβαση στο διαδίκτυο.
- Ακολουθώντας το διαδικτυακό μονοπάτι του στόχου και συλλέγοντας δεδομένα από φόρμες που συμπληρώνει μπορεί να συλλέξει usernames και passwords για site που επισκέπτεται, να βρει την διεύθυνση του στόχου, τους φίλους του και τα ενδιαφέροντά του που τελικώς δημιουργούν ένα ολοκληρωμένο προφίλ (fingerprint) μοναδικό για τον κάθε στόχο.



Σχήμα 1: Miscellaneous D.N.I (Digital Network Intelligence - intelligence collected by Internet traffic) Software used be NSA and Five Eyes

iv) Ασφάλεια OTP

Το OTP δεν παραμένει ασφαλές αν χρησιμοποιηθεί το ίδιο κλειδί περισσότερες από μία φορές. Αυτό ισχύει για τους παρακάτω λόγους.

Αρχικά, σε περίπτωση που ο επιτηθέμενος, με κάποιον τρόπο, αποκτήσει ένα από τα δύο plaintext, μπορεί να αποκρυπτογραφίσει και το άλλο χρησιμοποιώντας το ίδιο κλειδί.

Ακόμη, αν ο επιτιθέμενος αποκτήσει πολλά μηνύματα που έχουν κρυπτογραφηθεί με το ίδιο κλειδί, μπορεί να επιχειρήσει την επίθεση που χρησιμοποιείται και στο κρυπτοσύστημα μετατόπισης. Δηλαδή, μπορεί να βρεί τις συχνότητες εμφάνισης χαρακτήρων και να επιχειρήσει να βρεί το κλειδί. Αυτό ισχύει διότι, χρησιμοποιώντας το ίδιο κλειδί, οι χαρακτήρες των δύο μηνυμάτων που βρίσκονται στις ίδιες θέσεις, έχουν υποστεί την ίδια μετατόπιση.

Τέλος, ο OTP είναι ασφαλής ακόμα και ενάντια σε brute force attacks καθώς, όλες οι πιθανές περιπτώσεις κλειδιού θα οδηγήσουν σε όλα τα πιθανά μηνύματα. Έτσι, ο attacker δεν μπορεί να γνωρίζει το πραγματικό περιεχόμενο. Αν όμως χρησιμοποιηθεί το ίδιο κλειδί, μπορεί να διαπιστωθεί αν ένα πιθανό κλειδί οδηγεί σε πραγματικό κείμενο και για τα δύο κρυπτομηνύματα. Αυτό, αν και δεν δίνει μεγάλο προβάδισμα στον

επιτιθέμενο, αυξάνει, έστω και λίγο, τις πιθανότητες να βρεί το αρχικό μήνυμα.

v) GCM

Το GCM (Galois Counter Mode) είναι μία ιδιαίτερα δημοφιλής κατάσταση λειτουργίας για συμμετρικά κρυπτοσυστήματα τμήματος. Σημαντικό χαρακτηριστικό του είναι πως, εκτός από κρυπτογράφηση, προσφέρει και αυθεντικοποίηση.

Περιγραφή αλγορίθμου

Η λειτουργία κρυπτογράφησης του GCM βασίσεται στο κλασσικό counter mode το οποίο σημαίνει:

- Το αρχικό κείμενο σπάει σε blocks των 128 bits
- Δημιουργείται ένας counter που παίρνει τιμές μέχρι το πλήθος των block του αρχικού κειμένου
- Ένα τυχαίο IV συνενώνεται με έναν counter και κρυπτογραφείται με έναν συμμετρικό αλγόριθμο κρυπτογράφησης τμήματος (π.χ. AES DES)
- Το αποτέλεσμα γίνεται XOR με το αντίστοιχο block του αρχικού κειμένου

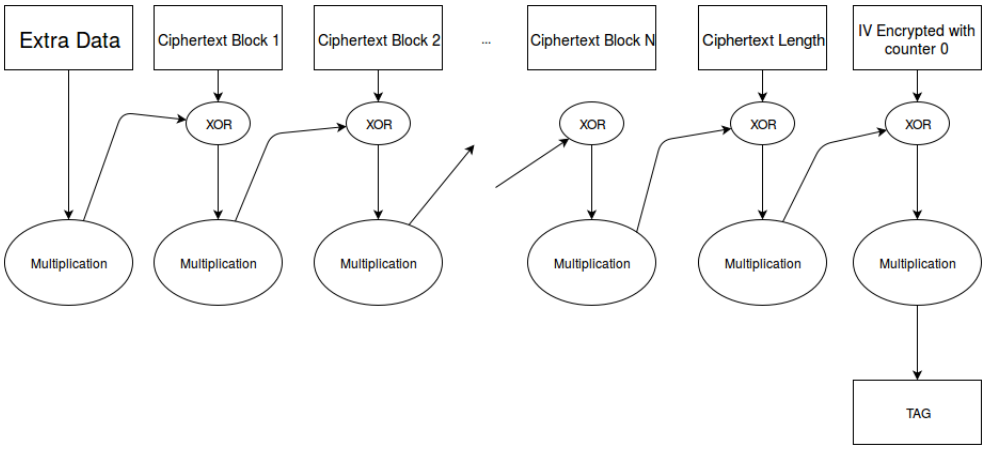
Αυτή η κατάσταση λειτουργίας είναι ευπαθής σε περιπτώσεις όπου κάποιος τρίτος μπορεί να προκαλέσει αλλαγές στο κρυπτογραφημένο κείμενο κατά την ανταλλαγή του. Για να εξασφαλίσουμε ακεραιότητα και αυθεντικοποίηση, πρέπει να χρησιμοποιηθεί μία MAC επί του κρυπτογραφημένου κειμένου και του IV.

Για να επιτευχθεί αυτό χρησιμοποιείται η GMAC, δηλαδή μία MAC που χρησιμοποιεί πολλαπλασιασμό στο $GF(2^{128})$. Αναλυτικότερα:

- Το αποτέλεσμα κρυπτογράφησης από του πρώτου block περνά από πολλαπλασιασμό σε $GF(2^{128})$
- Το αποτέλεσμα κρυπτογράφησης από το επόμενο block γίνεται XOR με το αποτέλεσμα του προηγούμενου βήματος και περνά από πολλαπλασιασμό σε $GF(2^{128})$
- Όταν γίνουν πολλαπλασιασμοί και XOR σε όλα τα block, το αποτέλεσμα, γίνεται XOR με το μήκος του κειμένου και περνά από έναν πολλαπλασιασμό
- Το τυχαίο IV συνενωμένο με τον counter 0 περνά από πολλαπλασιασμό σε $GF(2^{128})$ και γίνεται XOR με το προηγούμενο βήμα.

Το αποτέλεσμα είναι ένα TAG που συνενώνεται με το κρυπτογραφημένο κείμενο.

Το GCM έχει μία ακόμα πολύ σημαντική δυνατότητα. Μπορεί να εξασφαλίσει την ακεραιότητα παραπάνω δεδομένων. Για παράδειγμα, δεδομένα που έχουν σχέση με τα πακέτα που ανταλλάσσονται, αν πρόκειται για επικοινωνία μέσω διαδικτύου. Αυτά τα στοιχεία περνούν από πολλαπλασιασμό σε $GF(2^{128})$ και στη συνέχεια γίνονται XOR με το πρώτο block κρυπτογραφημένου κειμένου. Η διαδικασία συνεχίζεται όπως περιγράφεται παραπάνω.



Σχήμα 2: Αλυσίδα GMAC

Πολλαπλασιασμός σε $GF(2^{128})$

Η διαδικασία που αναφέρθηκε ως πολλαπλασιασμός σε $GF(2^{128})$ αναλύεται σε μεγαλύτερη λεπτομέρεια παρακάτω. Ουσιαστικά πρόκειται για πολλαπλασιασμό πολυωνύμων.

Αρχικά επιλέγεται ένα δεύτερο κλειδί των 128 bits. Το κλειδί αυτό, καθώς και τα 128 bits που δίνονται σε κάθε βήμα του GMAC αναπαριστούν πολυώνυμα που ανήκουν στο $GF(2^{128})$, δηλαδή πολυώνυμα μέχρι και 127ου βαθμού. Αυτά τα δύο πολυώνυμα πολλαπλασιάζονται μεταξύ τους και το αποτέλεσμα που προκύπτει, επιστρέφεται ως ακολουθία των 128 bits.

Επομένως, όπως βλεπουμε, για την χρήση της κατάστασης λειτουργίας GCM, απαιτούνται 2 κλειδιά των 128 bit:

- Ένα για την κρυπτογράφηση με συμμετρικό αλγόριθμο τμήματος
- Ένα για τον πολλαπλασιασμό σε $GF(2^{128})$

Θέμα 2

Η άσκηση αυτή είχε ως στόχο την δημιουργία του αλγορίθμου κρυπτογράφησης RC4 και την κρυπτογράφηση ενός μηνύματος. °°°°°°° ΗΕΑΔ Επίσης, δημιουργήθηκε μια συνάρτηση αποκρυπτογράφησης για τον έλεγχο της επιτυχής κρυπτογράφησης. Το κρυπτογραφημένο μήνυμα είναι (qomqcgepirhks!two.n(oaifam.evg και το αποκρυπτογραφημένο neversendahumantodoamachinesjob ======= Επίσης, δημιουργήθηκε μια συνάρτηση αποκρυπτογράφησης για τον έλεγχο της επιτυχής κρυπτογράφησης. °°°°°°° 0833δε97ςαεα4α5ε8αδφα8ς8ε80ε2βα4φ51φ8δ10

Θέμα 3

Αρχικά έγινε προσπάθεια εύρεσης του μήκους του κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση. Χρησιμοποιώντας τον δείκτη σύμπτωσης (Index of Coincidence) που υλοποιήθηκε σε Python και έτσι βρέθηκε με μεγάλη βεβαιότητα ότι το μήκος του κλειδιού είναι 7 χαρακτήρες (IC = 0.06722).
Έτσι το κείμενο διασπάστηκε σε 7 στήλες έτσι ώστε να ισχύει η ίδια μετατόπιση σε κάθε στήλη. Κάνοντας ανάλυση συχνοτήτων των χαρακτήρων κάθε στήλης, βρέθηκαν οι πιο συχνοί χαρακτήρες κάθε στήλης. Αυτοί είναι:

- I
- Q
- T
- I
- V
- S
- V

Αν θεωρηθεί ότι αυτοί οι χαρακτήρες αντιστοιχούν στο E (που είναι το γράμμα με την υψηλότερη συχνότητα εμφάνισης), τα κλειδιά που προκύπτουν σε κάθε στήλη είναι:

- Μετατόπιση 4 άρα κλειδί E
- Μετατόπιση 12 άρα κλειδί M
- Μετατόπιση 15 άρα κλειδί P
- Μετατόπιση 4 άρα κλειδί E
- Μετατόπιση 17 άρα κλειδί R
- Μετατόπιση 14 άρα κλειδί O
- Μετατόπιση 17 άρα κλειδί R

Παρατηρείται ότι σχηματίζουν τη λέξη EMPEROR και έτσι φαίνεται πως βρέθηκε το σωστό κλειδί. Με αποκρυπτογράφηση του μηνύματος με αυτό το κλειδί, προκύπτει το σωστό κείμενο

Αν το κλειδί που προέκυπτε από την παραπάνω ανάλυση ήταν λάθος, θα δοκιμάζονταν άλλοι συνδιασμοί βρίσκοντας τα δεύτερα πιο συχνά εμφανιζόμενα γράμματα κλπ.

Θέμα 4

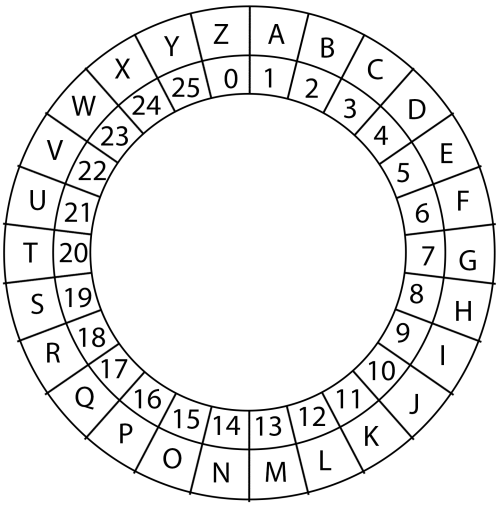
Εφόσον χρησιμοποιείται το σύστημα μετατόπισης, τα πιθανά κλειδιά είναι μόλις 23. Επομένως, με επίθεση ωμής βίας μπορούν να δοκιμαστούν όλα τα πιθανά κλειδιά. Βλέποντας τα αποτελέσματα, παρατηρείται ότι το κείμενο που προκύπτει χρησιμοποιώντας το κλειδί 3 είναι:
ΜΗΔΕΙΣΑΓΕΩΜΕΤΡΗΤΟΣΕΙΣΙΤΩΜΟΥΤΗΝΣΤΕΓΗΝ.
Αντίθετως, το κείμενα που προκύπτουν από τα υπόλοιπα κλειδιά δεν έχουν κάποιο νόημα. Έτσι έχουμε βρεθεί ότι το κλειδί είναι 3 και το κείμενο ΜΗΔΕΙΣ ΑΓΕΩΜΕΤΡΗΤΟΣ ΕΙΣΙΤΩ ΜΟΥ ΤΗΝ ΣΤΕΓΗΝ.

Θέμα 5

Στο θέμα αυτό εξετάστηκε το ποσοστό του avalanche effect στον AES μεταξύ διαφόρων ζευγαριών μηνυμάτων που διέφεραν μεταξύ τους σε ένα bit. Συγκεκριμένα, 32 λέξεις/φράσεις μήκους 16 χαρακτήρων(16 bytes με 5-bit κωδικοποίηση μετράπηκαν σε δεκαεξαδικό και ύστερα σε δυαδικά ψηφία και τροποιήθηκε ένα bit από την σειρά αυτή δημιουργώντας ένα παρόμοιο μήνυμα. Στην συνέχεια, τα αρχικα και τα τροποποιημένα μηνύματα κρυπτογραφήθηκαν με τον AES σε ECB mode και CBC mode για να εξαταστούν οι διαφορές σε επίπεδο bit του κρυπτογραφημένου αρχικού μηνύματος με το κρυπτογραφημένο τροποποιημένο μήνυμα. Η διαδικασία αυτή επαναλήφθηκε για 32 λέξεις/φράσεις και βρέθηκε οτι το ποσοστό μεταλλαγμένων βιτς και σε ECB mode και σε CBC mode ήταν μεταξύ 49-51

Θέμα 6

Η μέθοδος που ακολούθησα για την αποκρυπτογράφηση του μηνύματος με οδήγησε στην δημιουργία τριών διαφορετικών μηνυμάτων που προέκυψαν αποκρυπτογραφόντας κάθε φόρα το μήνυμα με ένα από τα γράμματα K, E και Y. Αναλυτικότερα, τα μηνύματα αυτά μπορούν να προκύψουν είτε από συνεχείς αλγεβρικές πράξεις με βάση τον τύπο $XMod26 - S_i$ όπου $S_i : i = K, E, Y$ είτε με την χρήση του παρακάτω δίσκου σε μια κίνηση.



Ο δίσκος αυτός αναπαριστά το αλφάβητο σε κυκλική μορφή για την διευκόλυνση της εύρεσης του αποτελσματος του mod26. Για παράδειγμα, θέλουμε να αποκρυπτογραφήσουμε το γράμμα A με βάση το γράμμα K. Αρχικά, σημειώνουμε την θέση του γράμματος A, δηλαδή το 1, και γυρνάμε τον εξωτερικό δαχτύλιο του αλφάβητου ως ότου το γράμμα με το οποίο αποκρυπτογραφούμε (σε αυτήν την περίπτωση το K να έρθει πάνω από τον αριθμό 1. Ύστερα, παρατηρούμε σε ποιόν αριθμό τώρα αντιστοιχεί το γράμμα A, δηλαδή το 16, και συμβολευόμαστε τον αρχικό δίσκο ποιό γράμμα βρίσκεται σε αυτόν τον αριθμό, δηλαδή το P.

Θέμα 7

Χρησιμοποιήθηκε επίθεση ωμής βίας, δηλαδή δοκιμάστηκαν ως κλειδιά όλες οι λέξεις που βρίσκονται στο english.txt. Μετά απο αρκετές προσπάθειες βρέθηκε το κλειδί: secret.

Θέμα 8

Χρησιμοποιήθηκε επίθεση ωμής βίας, δηλαδή δοκιμάστηκαν ως κλειδιά όλοι οι εξαψήφιοι ακέραιοι. Για να βρεθεί ποιός από τους αριθμούς είναι ο κωδικός, χρησιμοποιήθηκε η εξής μεθοδολογία:

Αρχικά, ο κωδικός αποθηκεύεται μετά από hashing με sha512 (6) και salt kHnyu3Ni όπως δίνονται στο το /etc/shadow. Αν το αποτέλεσμα του αλγορίθμου είναι ίδιο με το hash που μας δίνεται, τότε ο κωδικός έχει βρεθεί.

Έτσι βρέθηκε ότι το password είναι: 676767

Θέμα 9

(i)

Έστω K το keystream που χρησιμοποιήθηκε για την κρυπτογράφηση.
Έστω C το κρυπτογραφημένο κείμενο.
Για να βρεθεί το αρχικό κείμενο ακολουθήθηκε η παρακάτω διαδικασία:

Πρώτα, χρησιμοποιώντας το known plaintext ab για το κρυπτογραφημένο sq, μπορούν να βρεθούν τα bits 10-19 του K. Αυτό γίνεται κάνοντας XOR μεταξύ των 5-bit κωδικοποιήσεων των ab και sq.

Γνωρίζουμε πως τα bits $K[10:20]$ που βρέθηκαν, είναι μία ανεστραμμένη κατάσταση του LFSR (λόγω της ιδιότητας του LFSR να βγάζει αντίστροφα τα bits των καταστάσεων μέσα στο K). Συγκεκριμένα γνωρίζουμε ότι τα bits $K[10:20]$ μας δίνουν την 10 κατάσταση του LFSR.

Έστω S η αντεστραμμένη ακολουθία των bits 10-19

Για να βρούμε το πλήρες keystream μπορούν να ακολουθηθούν δύο μεθοδολογίες:

- Αντίστροφο LFSR ξεκινώντας από την κατάσταση 10 μέχρι να βρεθεί το seed (κατάσταση 0)
- Εκτέλεση του LFSR με κλειδί το S και χρησιμοποίηση μόνο ενός τμήματος του stream

Για λόγους ευκολίας υλοποίησης, χρησιμοποιήθηκε η δεύτερη μεθοδολογία. Αναλυτικότερα, το K είναι το τμήμα του stream που έχει:

- Έναρξη: 1023 - 10 = 1013
  (Περίοδος του LFSR - μετατόπιση επειδή δόθηκε ως κλειδί η 10η κατάσταση)

- Μήκος: len(Ciphertext) * 5
  (Αριθμός χαρακτήρων του κρυπτογραφημένου * 5 bit ανά χαρακτήρα)

Έτσι προκύπτει το K. Κάνοντας XOR μεταξύ του K και του C, γίνεται γνωστό το αρχικό μήνυμα

(ii)

Έστω $K1$ το stream που προκύπτει από το LFSR-10.
Έστω $K2$ το stream που προκύπτει από το LFSR-16.
Έστω $K3$ το keystream που προκύπτει από το XOR των $K1$ και $K2$.

Αρχικά, δίνονται τα bits 10-29 με παρόμοιο τρόπο όπως στο προηγούμενο υποερώτημα. Επίσης, με brute force στο seed του LFSR-10, μπορούν να βρεθούν όλα τα πιθανά $K1$.

Κάνοντας XOR μεταξύ του γνωστού τμήματος του $K3$ και κάθε πιθανού $K1$, είναι δυνατό να βρεθούν 20 bits του $K2$. Αυτά, κάνοντας αντίστροφο LFSR, μπορούν να χρησιμοποιηθούν για την εύρεση του seed.

Επομένως έχουν προκύψει 1024 ζεύγη seed για τα δύο LFSR. Άρα μπορούν να βρεθούν 1024 πιθανά κείμενα τα οποία αποτελούν το αρχικό κείμενο.

Για τον περιορισμό των πιθανών αποτελεσμάτων, χρησιμοποιήθηκε η παρακάτω τεχνική:

- Τα γνωστά bits 10-25 του $K2$ χρησιμοποιούνται για την εύρεση του 2ου seed.
- Μετά την εύρεση του πιθανών seed και $K2$, γίνεται έλεγχος εάν τα bits 26-29 του $K2$ είναι ίδια με τα γνωστά bits. Αν ναι, τότε αυτό το stream θεωρείται έγκυρο.

Τελικά, μετά την εκτέλεση του αλγορίθμου, προέκυψαν περίπου 60 πιθανές προτάσεις από τις οποίες αναγνωρίστηκε η παρακάτω:
alwaysforgiveyourenemies.nothingannoysthemsomuch