Μια πρόταση διδασκαλίας για την ανταλλαγή κλειδιού Diffie – Hellman

Παναγιώτης Γροντάς

Καλλιτεχνικό Γυμνάσιο Γέρακα με Λυκειακές Τάξεις, pgrontas@gmail.com

Περίληψη

Η εργασία αυτή παρουσιάζει μια πρόταση διδασκαλίας για την ανταλλαγή κλειδιού Diffie – Hellman, μιας κρυπτογραφικής τεχνικής, με κομβική σημασία για την λειτουργία του Διαδικτύου και του Παγκόσμιου ιστού. Αν και για την πλήρη κατανόηση της απαιτούνται προχωρημένες μαθηματικές γνώσεις, υποστηρίζουμε πως στον πυρήνα της βρίσκονται διαδικασίες οι οποίες μπορούν να γίνουν κατανοητές από μαθητές Λυκείου. Για αυτές παρουσιάζουμε αναλογίες από την βιβλιογραφία και την καθημερινή ζωή και αναλύουμε πιθανά οφέλη και προβλήματα.

Λέξεις κλειδιά: Κρυπτογραφία, Ανταλλαγή Κλειδιού Diffie – Hellman, Ασυμμετρία, Υπολογιστή Σκέψη

1. Εισαγωγή

Το διδακτικό αντικείμενο της πληροφορικής στην δευτεροβάθμια εκπαίδευση χρήζει ποιοτικής βελτίωσης. Η πληροφορική δεν είναι πλέον μία νέα επιστήμη, αλλά έχει ωριμάσει σε τέτοιο βαθμό, ώστε γνώσεις που μέχρι πριν από μια εικοσαετία, ίσως θεωρούνταν εξεζητημένες, να κρίνονται απαραίτητες για την κατανόηση του σύγχρονου, αλλά πιο σημαντικά του μελλοντικού κόσμου, τον οποίον άλλωστε θα κληθούν να αντιμετωπίσουν οι μαθητές μας (Μπουκέας, Πουλάκης, & Τσοπόκης, 2012). Η κύρια πηγή μιας τέτοιας αναβάθμισης είναι συνήθως ο προγραμματισμός. Η ωρίμανση όμως της πληροφορικής, έχει αναδείξει και άλλες ενδιαφέρουσες και θεμελιώδεις έννοιες, οι οποίες μάλιστα δεν απαιτούν ιδιαίτερες πρότερες γνώσεις από τους μαθητές και μπορούν να εξηγηθούν με απτά παραδείγματα από την καθημερινότητα (Αλεξόπουλος & Ρόμπολα, 2012).

Ένα πεδίο, στο οποίο μπορούν να βρεθούν πολλές ιδέες για πρωτότυπες προτάσεις διδασκαλίας αποτελεί η Κρυπτογραφία, μία περιοχή με ιστορία χιλιάδων ετών, η οποία τα τελευταία 60 χρόνια έχει αποκτήσει αυτόνομη επιστημονική υπόσταση συνδυάζοντας τα Μαθηματικά και την Πληροφορική, με στενή σχέση με θεμελιώδη προβλήματα των δύο επιστημών. Εμπειρικά, έχουμε διαπιστώσει ότι έλκει το ενδιαφέρον των μαθητών, καθώς σχετικά θέματα στο μάθημα της «Ερευνητικής Εργασίας» συγκεντρώνουν συνεχώς παραπάνω δηλώσεις συμμετοχής από αυτές που θα

μπορούσαν να εξυπηρετηθούν. Επιπλέον σχετικές συζητήσεις στα πλαίσια παλαιότερων μαθημάτων επιλογής, έχουν προκαλέσει έντονη περιέργεια, όπως επιβεβαιώνεται και από προηγούμενες σχετικές εργασίες όπως οι (Καραγεώργος, 2010) και (Πέρδος, κ.ά., 2015).

Στην εργασία αυτή συνεχίζουμε την παραπάνω τάση, εστιάζοντας ίσως στο πιο σημαντικό αποτέλεσμα της σύγχρονης Κρυπτογραφίας. Συγκεκριμένα θα προτείνουμε ένα πλαίσιο διδασκαλίας για το πρωτόκολλο ανταλλαγής κλειδιού των Diffie και Hellman (και Merkle) - DHKE, (Diffie & Hellman, 1976), το οποίο έλυσε ένα πρόβλημα ηλικίας πάνω από 2000 ετών με έναν πολύ πρωτότυπο και απλό τρόπο, ανοίγοντας τον δρόμο στην διάδοση του Διαδικτύου και στην δημιουργία ηλεκτρονικών υπηρεσιών που χρησιμοποιούμε καθημερινά. Η σημασία του καταδεικνύεται από το ότι οι εμπνευστές του έλαβαν το βραβείο Turing για το έτος 2015 (ACM, 2016), την ανώτατη διάκριση που μπορεί να λάβει ένας επιστήμονας της Πληροφορικής.

Αφορμή για την επιλογή του, είναι η παρατήρηση ότι αν και το συγκεκριμένο πρωτόκολλο, απαιτεί προχωρημένα μαθηματικά στην πλήρη μορφή του, είναι στην ουσία , αρκετά απλό, απαιτεί λίγες πρότερες γνώσεις και η ουσία του εξηγείται χωρίς καμία αναφορά σε 'τεχνικές' έννοιες. Έτσι είναι εύκολα προσβάσιμο σε μαθητές Λυκείου. Επιπλέον, διαθέτει παραλλαγές, όπως αυτές που έχουν προταθεί σε βιβλία 'εκλαϊκευμένης' επιστήμης (Singh, 2001) και για τις οποίες έχει ήδη δημιουργηθεί εκπαιδευτικό υλικό (Khan Academy, 2016), προσβάσιμο και από μικρότερους μαθητές. Τέλος είναι μια πολύ καλή ευκαιρία για την παρουσίαση κεντρικών εννοιών της Πληροφορικής που δεν υπάρχουν στο παρόν πρόγραμμα σπουδών και που θέτουν τις βάσεις για την παρουσίαση με απλό τρόπο ακόμα πιο δύσκολων.

2. Η ανταλλαγή κλειδιού Diffie-Hellman

Αρχικά λοιπόν θα παρουσιάσουμε συνοπτικά τα κύρια σημεία του πρωτοκόλλου DHKE. Φυσικά δεν είναι στόχος μας το πρωτόκολλο αυτό καθ'αυτό. Απαιτείται όμως μία αναλυτική περιγραφή ώστε να γίνει φανερό το πώς μπορεί να απλοποιηθεί ώστε να δομηθεί η διδακτική μας προσέγγιση στη συνέχεια.

2.1 Το πρόβλημα

Η κλασική (συμμετρική) κρυπτογραφία επιτρέπει σε δύο οντότητες (*A* και *B*) να επικοινωνήσουν χωρίς να διατρέχουν τον κίνδυνο υποκλοπής των ανταλλασσόμενων μηνυμάτων. Βασίζεται στην ύπαρξη ενός κοινού κλειδιού, το οποίο ο *A* χρησιμοποιεί για να μετατρέψει το μήνυμα σε μία ακατανόητη μορφή, άχρηστη για οποιονδήποτε υποκλοπέα, την οποία αναιρεί ο *B*, πάλι με χρήση του ίδιου κλειδιού. Μέθοδοί της έχουν χρησιμοποιηθεί εδώ και χιλιάδες χρόνια σε ελεγχόμενα - κλειστά περιβάλλοντα, όπου ήταν εφικτό στον *A* και *B* να αποκτήσουν με το κοινό κλειδί, με αρκετά βέβαια προβλήματα διαχείρισης (Παγουρτζής & Ζάχος, 2016).

Δυστυχώς καμία από τις μεθόδους της κλασικής κρυπτογραφίας δεν ήταν κατάλληλη σε ένα ανοικτό περιβάλλον όπως το Διαδίκτυο, το οποίο είχε τις ίδιες ανάγκες μυστικότητας, χωρίς όμως να καθιστά δυνατή την εκ των προτέρων (και εκτός καναλιού) συνεννόηση για συμφωνία κλειδιού.

2.2 Η λύση

Το 1976 οι Whitfield Diffie και Martin Hellman (Diffie & Hellman, 1976) χρησιμοποιώντας δουλειά του Ralph Merkle, έδωσαν μία πρωτότυπη λύση στο πρόβλημα διανομής κλειδιού, δημιουργώντας την κρυπτογραφία δημοσίου κλειδιού και τις διάφορες εφαρμογές της (πχ. ψηφιακές υπογραφές). Το πρωτόκολλο που πρότειναν (με λεπτομέρειες που εισήχθησαν αργότερα) συνοψίζεται ως εξής:

1. Οι Α, Β συμφωνούν σε μία κυκλική ομάδα G με τάξη q, καθώς και σε έναν γεννήτορα της, g. Η συνομιλία αυτή μπορεί να είναι δημόσια. Μάλιστα δεν χρειάζεται καν να υπάρξει αλληλεπίδραση, καθώς μπορεί οποιαδήποτε από τις δύο οντότητες να επιλέξει τις παραμέτρους και να τις αποστείλει στην άλλη.
2. Κάθε ένας από τους Α και Β επιλέγει ιδιωτικά και διατηρεί μυστικό έναν αριθμό α και β αντίστοιχα, από το σύνολο $\mathbb{Z}_q = \{0,1,\dots,q-1\}$.
3. Ο Α υπολογίζει και δημοσιοποιεί την τιμή g^a και ο Β αντίστοιχα την τιμή g^b.
4. Ο κάθε ένας συνδυάζει την ιδιωτική του τιμή με τη δημόσια τιμή του άλλου, δημιουργώντας έτσι το κοινό κλειδί. Συγκεκριμένα:
    a. Ο Α υπολογίζει το $(g^b)^a = g^{ba}$
    b. Ο Β υπολογίζει το $(g^a)^b = g^{ab}$
5. Με το πέρας της επικοινωνίας οι Α, Β έχουν συμφωνήσει στο κοινό κλειδί $K = g^{ab}$, το οποίο είναι στοιχείο της ομάδας G.

Οι συνηθέστερες ομάδες στις οποίες μπορεί να εκτελεστεί το πρωτόκολλο είναι η πολλαπλασιαστική ομάδα $\mathbb{Z}_p^*$, όπου p ένας μεγάλος πρώτος αριθμός ή η προσθετική ομάδα των ελλειπτικών καμπυλών σε κάποιο κατάλληλο πεπερασμένο σώμα.

2.3 Ασφάλεια

Η ασφάλεια του πρωτοκόλλου DHKE εξαρτάται από τρία δύσκολα υπολογιστική προβλήματα τα οποία παραθέτουμε παρακάτω, με φθίνουσα σειρά δυσκολίας.

Το πρόβλημα του Διακριτού Λογαρίθμου

Δίνεται μια κυκλική ομάδα $G = \langle g \rangle$ τάξης q και ένα τυχαίο στοιχείο $y \in G$
Να υπολογιστεί $x \in \mathbb{Z}_q$ ώστε $g^x = y$ δηλ. το $log_g y \in \mathbb{Z}_q$. Το πρόβλημα αυτό αντιστοιχεί στην προσπάθεια ενός αντιπάλου να μαντέψει το κλειδί από το τελευταίο μήνυμα της επικοινωνίας.

Το υπολογιστικό πρόβλημα Diffie - Hellman
Δίνεται μια κυκλική ομάδα $G = \langle g \rangle$ τάξης q και δύο τυχαία στοιχεία $y_1, y_2 \in G$, με διακριτούς λογαρίθμους $x_1, x_2 \in \mathbb{Z}_q$. Να υπολογιστεί το $g^{x_1 x_2}$.

Το πρόβλημα απόφασης Diffie - Hellman
Δίνεται μια κυκλική ομάδα $G = \langle g \rangle$ τάξης q και τρία τυχαία στοιχεία $y, y_1, y_2 \in G$, με διακριτούς λογαρίθμους $x_1, x_2 \in \mathbb{Z}_q$. Να εξεταστεί αν $y = g^{x_1 x_2}$.

Τα δύο τελευταία προβλήματα αντιστοιχούν σε έναν αντίπαλο ο οποίος προσπαθεί να εκμεταλλευτεί και μηνύματα εκτός του τελευταίου για να βρει το κοινό κλειδί. Από την περιγραφή της ενότητας 2.2 είναι φανερό ότι αν είναι υπολογιστικά δύσκολο να εξετάσουμε αν ισχύει το πρόβλημα απόφασης Diffie – Hellman σε μια ομάδα G, τότε το πρωτόκολλο είναι ασφαλές απέναντι σε κάποιον παθητικό αντίπαλο. Αξίζει να σημειωθεί ότι το πρωτόκολλο δεν είναι καθόλου ασφαλές, αν ο αντίπαλος είναι ενεργητικός.

3. Διδακτική προσέγγιση

Έχοντας τώρα μία πλήρη κατανόηση της διαδικασίας ανταλλαγής κλειδιού, μπορούμε να κάνουμε τις απαραίτητες απλοποιήσεις ώστε να βρεθούμε πιο κοντά στις αναπαραστάσεις των μαθητών.

3.1 Αφαιρετικό Μοντέλο

Είναι φανερό ότι οι παραπάνω λεπτομέρειες της Θεωρίας Ομάδων δεν αφορούν τους μαθητές στην δευτεροβάθμια εκπαίδευση, με την παρούσα μορφή της, τουλάχιστον. Αν παρατηρήσουμε όμως, θα δούμε ότι ουσιαστικά το πρωτόκολλο αυτό αποτελείται από απλές ενέργειες:

1. **Συμφωνία στη δημόσια πληροφορία**. Όπως προαναφέραμε δεν χρειάζεται να υπάρξει κανενός είδους αλληλεπίδραση εδώ. Αρκεί ένας από τους δύο συμμετέχοντες να επιλέξει αυθαίρετα τις απαιτούμενες παραμέτρους.
2. **Επιλογή Μυστικού**. Ο κάθε συμμετέχων διαλέγει αυθαίρετα μία μυστική πληροφορία για τον εαυτό του.
3. **Πρώτη Μίξη και Αποστολή:** Η δημόσια πληροφορία του βήματος 1 συνδυάζεται με το μυστικό του βήματος 2 για κάθε παίκτη και το αποτέλεσμα αποστέλλεται (δημόσια) στον άλλο παίκτη. Η μίξη πρέπει να είναι τέτοια ώστε το μυστικό να μην μπορεί να εξαχθεί (εύκολα) από τη δημόσια πληροφορία.
4. **Δεύτερη Μίξη και Συμφωνία**: Τα αποτελέσματα της πρώτης μίξης που ελήφθησαν στο βήμα 3, συνδυάζονται ξανά με την μυστική πληροφορία σε κάθε πλευρά, παράγοντας έτσι το κοινό μυστικό, το οποίο χρησιμοποιείται

στο εξής. Και πάλι η μίξη πρέπει να αποτρέπει την εξαγωγή του μυστικού κλειδιού.

Οι διαδικασίες αυτές, είναι ανεξάρτητες της Θεωρίας Ομάδων και κατά συνέπεια μπορούν να παρουσιαστούν στους μαθητές, χωρίς καμία απαίτηση μαθηματικών γνώσεων. Στην συνέχεια λοιπόν θα καθοδηγήσουμε τους μαθητές σε αυτές, χρησιμοποιώντας απλά παραδείγματα και αναλογίες.

3.2 Προετοιμασία

Αρχικά, θα πρέπει να ξεκαθαριστεί ο στόχος του πρωτοκόλλου. Εμπειρικά έχουμε παρατηρήσει ότι οι μαθητές επικεντρώνονται στην ανταλλαγή των μηνυμάτων χωρίς να έχουν εμπεδώσει πλήρως ότι όλα γίνονται για να δημιουργηθεί ένα κοινό κλειδί. Για τον σκοπό, αυτό πρέπει να έχει δοθεί προηγουμένως μία ιστορική αναδρομή της έννοιας της κρυπτογραφίας όπου θα έχει τονιστεί ο ρόλος του κρυπτογραφικού κλειδιού, αλλά και τα το πρόβλημα της διανομής του. Στο τέλος, μπορεί να χρησιμοποιηθεί η προσέγγιση επίλυσης προβλήματος, όπου οι μαθητές, χωρισμένοι ίσως σε ομάδες, θα κληθούν να προτείνουν λύσεις για το πώς δύο οντότητες θα μπορέσουν να δημιουργήσουν ένα κοινό κλειδί χωρίς να διαθέτουν ένα ασφαλές κανάλι επικοινωνίας.

Για να γίνει αυτό θα πρέπει να αποσαφηνιστούν οι έννοιες της δημόσιας και ιδιωτικής πληροφορίας. Να τονιστεί δηλαδή ότι όλα τα μηνύματα που ανταλλάσσονται είναι προσβάσιμα, από οποιονδήποτε, ακόμα και από κάποια εχθρική οντότητα. Αυτό μπορεί να επιτευχθεί δίνοντας στους μαθητές μια εικόνα υψηλού επιπέδου για το τι ακριβώς συμβαίνει. Για τον σκοπό αυτό είναι χρήσιμο να παρουσιαστεί πώς φαίνεται το πρωτόκολλο σε κάποιον εξωτερικό παρατηρητή, ο οποίος το παρακολουθεί χωρίς να παρεμβαίνει (ωτακουστής). Γι' αυτό μπορεί να παρουσιαστεί ένα ανθρωπομορφικό ανάλογο του πραγματικού κόσμου (Κιαγιάς, 2011), ίσως και με ένα παιχνίδι ρόλων. Δύο μαθητές ξεκινούν μία συζήτηση μεταξύ τους στα ελληνικά. Όσοι παρακολουθούν την καταλαβαίνουν πλήρως. Στόχος της είναι να συμφωνήσουν σε μία ξένη γλώσσα που και οι δύο γνωρίζουν. Ξαφνικά όμως και ενώ όλοι έχουν παρακολουθήσει τις λέξεις που έχουν ειπωθεί, η γλώσσα της συζήτησης, θα αλλάξει χωρίς πλέον να καταλαβαίνει κανένας, εκτός από τους δύο ομιλούντες.

3.3 Χρήση αναλογιών

Οι αναλογίες είναι ένας μηχανισμός ο οποίος μπορεί να χρησιμοποιηθεί για να γίνουν κάποιες έννοιες πιο προσιτές στους μαθητές (Vosniadou & Brewer, 1987). Απαιτείται όμως προσοχή ώστε να μην χαθεί ο διδακτικός στόχος λόγω της προσήλωσης στην αναλογία, αλλά και να επισημανθούν τυχούσες διαφορές (Αδαμόπουλος, 2005). Μία πιο λεπτομερής μοντελοποίηση της συζήτησης λοιπόν, μπορεί να γίνει αντικαθιστώντας τους αριθμούς με χρώματα, όπως έχει προτείνει ο Singh στο (Singh, 2001) και

έχει υλοποιηθεί σε μορφή βίντεο στο (Khan Academy, 2016). Συγκεκριμένα, το κλειδί στο παράδειγμα αυτό είναι ένα κοινό χρώμα στο οποίο έχουν συμφωνήσει οι *A* και *B*. Η από κοινού δημιουργία του χρώματος προσαρμοσμένη στο πλαίσιο της ενότητας 2.2 έχει ως εξής:

1. **Συμφωνία:** Οι *A*, *B* συμφωνούν σε ένα κοινό δημόσιο χρώμα K και στις ποσότητες που θα χρησιμοποιηθούν για τη συνέχεια – όπως και πριν μπορεί απλά να το επιλέξει μία από τις δύο οντότητες.
2. **Επιλογή Μυστικού:** Οι *A* και *B* επιλέγουν από ένα μυστικό χρώμα ο καθένας.
3. **Μίξη 1:** Ο κάθε ένας συνδυάζει το ιδιωτικό του χρώμα με το δημόσιο, δημιουργώντας έτσι ένα μίγμα διαφορετικού χρώματος το οποίο αποστέλλει στον άλλο.
4. **Μίξη 2:** Τέλος ο κάθε ένας προσθέτει το δικό του ιδιωτικό χρώμα στο μίγμα των δύο χρωμάτων που έλαβε από το προηγούμενο βήμα.
5. Με το πέρας της επικοινωνίας οι *A*, *B* έχουν συμφωνήσει στο κοινό κλειδί - χρώμα, το οποίο έχει προκύψει από την ανάμιξη των τριών χρωμάτων – δημόσιο, ιδιωτικό *A* και ιδιωτικό *B* με διαφορετική σειρά βέβαια.

Εκτός από την προβολή του βίντεο στο (Khan Academy, 2016), οι μαθητές μπορούν να πειραματιστούν ανά δύο με διαθέσιμα διαδραστικά εργαλεία του παγκόσμιου ιστού όπως για παράδειγμα το (Online Color Mixing Tool, 2016), για να κατανοήσουν καλύτερα τη διαδικασία. Εναλλακτικά μπορούν να πειραματιστούν και με πραγματικά χρώματα, ίσως σε συνεργασία με το μάθημα των Καλλιτεχνικών.

Έχοντας τη διαδικασία στο μυαλό τους είναι ενδιαφέρον να προσπαθήσουν οι μαθητές μόνοι τους να ορίσουν τα προβλήματα της ενότητας 2.3 πάνω στα οποία βασίζεται η ασφάλεια του πρωτοκόλλου.

Το πρόβλημα της Ανάλυσης Χρώματος
Δίνεται ένα χρώμα *A* το οποίο αποτελείται από δύο χρώματα *K* και *α*. Να βρεθεί το *α*.

Το υπολογιστικό πρόβλημα Κοινού Χρώματος
Δίνεται ένα κοινό χρώμα *K* και δύο χρώματα *A* και *B* τα οποία αποτελούνται από το *K* και ένα μυστικό χρώμα *α* και *β,* αντίστοιχα.. Να βρεθεί το χρώμα που προκύπτει από την ανάμιξη των *K*, *α*, *β*.

Το πρόβλημα απόφασης Κοινού Χρώματος
Δίνεται ένα κοινό χρώμα *K* και δύο χρώματα *A* και *B* τα οποία αποτελούνται από το *K* και ένα μυστικό χρώμα *α* και *β*, καθώς και ένα τρίτο χρώμα Y. Να εξεταστεί αν το Y μπορεί να προκύψει από την ανάμιξη των *K*, *α*, *β*.

Στο σημείο αυτό η διαθεματική προσέγγιση μπορεί να χρησιμοποιηθεί για την επισήμανση της δυσκολίας των παραπάνω προβλημάτων. Επιπλέον οι μαθητές πρέπει να

ανακαλύψουν τη σχετική δυσκολίας τους. Για τον σκοπό αυτό μπορούν να καθοδηγηθούν με ερωτήσεις σχετικές με την ποσότητα πληροφορίας που διαθέτει ο κάθε αντίπαλος, αλλά και να αξιολογήσουν οι ίδιοι ποια μέθοδο θα επέλεγαν για να βρουν το κοινό χρώμα, βάζοντας τους στη θέση των κρυπταναλυτών. Τέλος, θα ήταν ενδιαφέρον να προσπαθήσουν οι μαθητές να 'σπάσουν' το σύστημα με οποιονδήποτε τρόπο επιθυμούν, ως ενεργητικοί αντίπαλοι.

3.4 Συμπλήρωση με απλά μαθηματικά

Αφού έχουμε παρουσιάσει μια υψηλού επιπέδου αναπαράσταση του πρωτοκόλλου μπορούμε να δώσουμε μία περιγραφή που είναι πιο κοντά στο βασικό πρωτόκολλο. Συγκεκριμένα θα παραλείψουμε τις λεπτομέρειες για την επιλογή ομάδας και θα δώσουμε ακριβώς τις βασικές λειτουργίες του πρωτοκόλλου, οι οποίες θα ευθυγραμμιστούν με την περιγραφή με τα χρώματα:

1. **Συμφωνία:** Οι *A, B* συμφωνούν σε έναν κοινό αριθμό g.
2. **Επιλογή Μυστικού:** Οι *A* και *B* επιλέγουν από ένα μυστικό αριθμό ο καθένας, α και β αντίστοιχα.
3. **Μίξη 1:** Ο κάθε ένας συνδυάζει το ιδιωτικό του αριθμό με τον δημόσιο, χρησιμοποιώντας την πράξη της ύψωσης σε δύναμη και υπολογίζοντας τα g^a και g^b και αποστέλλει το αποτέλεσμα στην άλλη οντότητα.
4. **Μίξη 2:** Οι *A* και *B* συνδυάζουν το $(g^b)^a$ και $(g^a)^b$ με την ύψωση σε δύναμη.
5. Με το πέρας της επικοινωνίας οι *A, B* έχουν συμφωνήσει στο κοινό κλειδί g^{ab}.

Σε αυτό το σημείο θα πρέπει να οριστούν ξανά τα δύσκολα προβλήματα στα οποία βασίζεται το πρωτόκολλο με παρόμοιο τρόπο με την ενότητα 2.3 χωρίς βέβαια τις λεπτομέρειες για τις ομάδες.

4. Διδακτικά οφέλη και δυσκολίες

4.1 Υπολογισμός και Ασυμμετρία

Όπως είδαμε στην ενότητα 2.3 η ασφάλεια του πρωτοκόλλου βασίζεται στην ασυμμετρία του προβλήματος της ύψωσης σε δύναμη. Η μία κατεύθυνση είναι εύκολη, ενώ η αντίστροφη είναι δύσκολη. Η διαδικασία μπορεί να παραλληλιστεί με την αντιστροφή συνάρτησης σε μαθητές που την έχουν διδαχθεί.

Εμπειρικά, έχουμε διαπιστώσει ότι κάτι τέτοιο είναι δύσκολο να κατανοηθεί καθώς έχουν συνηθίσει να θεωρούν ότι η ύψωση σε δύναμη, είναι απλά ένα σύμβολο, και όχι μια ενεργητική διαδικασία, η οποία χρειάζεται κάποια βήματα. Η ασυμμετρία δηλαδή μπορεί να επισημάνει την διαφορά του συμβολισμού ενός υπολογισμού από τα πραγματικά βήματα που χρειάζονται για την εκτέλεσή του.

Εδώ μπορεί να βοηθήσει η αναλογία με τη μίξη χρωμάτων, όπου φαίνεται με εύκολο τρόπο ότι δεν πρόκειται για μία αυτόματη διαδικασία. Δηλαδή για να αναμιχθούν δύο χρώματα, πρέπει να γίνουν κάποια βήματα. Το ίδιο ισχύει και για να αναλυθεί ένα χρώμα στα συστατικά του, μόνο που χρειάζονται περισσότερα βήματα.

4.2 Προηγούμενες αναπαραστάσεις

Μία δυσκολία που μπορεί να αντιμετωπίσουν οι μαθητές και η οποία έχει παρατηρηθεί σε ανεπίσημες συζητήσεις του πρωτοκόλλου, είναι ότι οι δυσκολία κατανόησης του ότι η εύρεση του λογαρίθμου είναι μία δύσκολη πράξη. Αυτό συμβαίνει ιδιαίτερα σε μαθητές μεγαλύτερων ηλικιών που έχουν γνωρίσει την αντίστοιχη έννοια στα μαθηματικά. Μία τέτοια δυσκολία είναι εύλογη καθώς τέτοιοι μαθητές μπορούν να υπολογίσουν από μόνοι τους μικρούς λογαρίθμους. Κάτι τέτοιο όμως μπορεί να αποτελέσει εκκίνηση για την αντιμετώπιση της, αφού αρκεί να 'προκληθεί' ο μαθητής να υπολογίσει τον λογάριθμο ενός αριθμού με μέγεθος χιλιάδων ψηφίων. Σε πιθανή αντίρρηση, σχετικά ότι η ταχύτητα μπορεί να βελτιωθεί με χρήση υπολογιστή, μπορούν να παρουσιαστούν πίνακες όπως ο (Wikipedia, 2016), που να παρέχουν μία απόδειξη της δυσκολίας του προβλήματος στην πράξη.

Επιπλέον, το πρόβλημα του Διακριτού Λογαρίθμου μπορεί να επισημάνει τη διαφορά που υπάρχει στον χειρισμό ακεραίων και πραγματικών αριθμών, καθώς στη δεύτερη περίπτωση, μπορεί να προσεγγιστεί σχετικά εύκολα. Αυτό θα δείξει στους μαθητές ότι κάποια υπολογιστικά προβλήματα της πληροφορικής είναι εύκολα στους πραγματικούς αλλά δύσκολα στους ακέραιους. Η διαφορά αυτή αξίζει ίσως να αποτελέσει ξεχωριστό άρθρο προσαρμοσμένο ίσως και στις ανάγκες της τριτοβάθμιας εκπαίδευσης.

Το πιο σημαντικό όμως που μπορεί να προκύψει από την όλη συζήτησης περί δυσκολίας προβλημάτων, αφορά την διάκριση των προβλημάτων η οποία έχει γίνει είναι ήδη γνωστή από την Γ' Γυμνασίου. Η διάκριση αυτή μπορεί να γίνει πιο εκλεπτυσμένη, καθώς θα εμπλουτιστεί με τα δυσεπίλυτα προβλήματα, τα οποία αν και είναι επιλύσιμα, έχουν συμπεριφορά πρακτικά παρόμοια με τα άλυτα. Γίνεται έτσι και μία σύντομη εισαγωγή στη Θεωρία Υπολογιστικής Πολυπλοκότητας.

5. Ένταξη στη διδασκαλία

Το δύσκολο στην διδακτική πρόταση της παρούσας εργασίας είναι η ένταξή της στο υπάρχον πρόγραμμα σπουδών. Υπολογίζουμε ότι για την παρουσίαση χρειάζονται 3 με 4 διδακτικές ώρες οι οποίες θα διατεθούν για μια ιστορική αναδρομή στην Κρυπτογραφία, τις δύο απλοποιημένες προσεγγίσεις αλλά και την σχετική συζήτηση και ανατροφοδότηση.

Σε παλαιότερα ωρολόγια προγράμματα υπήρχε χώρος να γίνει κάτι τέτοιο στα μαθήματα επιλογής «Εφαρμογές Πληροφορικής» και «Εφαρμογές Υπολογιστών». Τώρα

όμως τα μαθήματα αυτά έχουν καταργηθεί παντού εκτός από την Α' τάξη του Λυκείου, όπου είναι εφικτή μία τέτοια διδακτική πρόταση, ενταγμένη, ίσως, στο κεφάλαιο 10.

Μία εναλλακτική προσέγγιση είναι η διδασκαλία αυτής της μεθόδου στα πλαίσια της ερευνητικής εργασίας, σχετικά με την Κρυπτογραφία και την ιστορία της. Εκεί θα υπάρχει και χρόνος για αναλυτική συζήτηση και για τις εφαρμογές του. Σε κάθε περίπτωση αναγνωρίζουμε ότι η διδακτική πρόταση ταιριάζει καλύτερα σε ένα εμπλουτισμένο πρόγραμμα σπουδών, το οποίου την ανάγκη προσπαθεί να τονίσει.

6. Συμπεράσματα και μελλοντική δουλειά.

Στην εργασία αυτή παρουσιάσαμε μια διδακτική προσέγγιση για το πρωτόκολλο ανταλλαγής κλειδιού Diffie Hellman. Η προσέγγιση αυτή έχει προκύψει μετά από συνεχείς, αλλά ανεπίσημες, συζητήσεις με μαθητές που έχουν ενδιαφέρον για την πληροφορική, στα πλαίσια μαθημάτων επιλογής και ερευνητικών εργασιών καθώς και από αντίστοιχες προσπάθειες όπως αυτές που αναφέρθηκαν στην εργασία. Είναι σαφές ότι οι προτάσεις και οι προβληματισμοί που αναπτύχθηκαν χρειάζονται ένα πιο συστηματικό πλαίσιο για να επιβεβαιωθούν, να καταρριφθούν ή να εμπλουτιστούν, μέσω κάποιου ερωτηματολογίου ενδεχομένως, κάτι που αποτελεί μελλοντικό στόχο.

Πιο σημαντικά όμως η διδακτική πρόταση έχει ως στόχο να διερευνήσει πώς μπορεί να εμπλουτιστεί η διδασκαλία στη Δευτεροβάθμια εκπαίδευση με *βασικά αποτελέσματα* της επιστήμης της πληροφορικής, τα οποία είναι σημαντικά, θεμελιώδη και δεν εξαρτώνται από συγκεκριμένες υλοποιήσεις ή τεχνολογίες. Η απάντηση που δίνουμε στο ερώτημα αυτό είναι καταρχήν θετική, αρκεί να βρεθούν τα κατάλληλα προβλήματα αλλά και οι κατάλληλες αφαιρέσεις. Κατά τη γνώμη μας κάτι τέτοιο είναι απόλυτα εφικτό και μπορεί να εφαρμοστεί σε αρκετές περιπτώσεις τις οποίες θα παρουσιάσουμε σε μελλοντικές εργασίες. Επιπλέον αξίζει να εξεταστεί, αν εκτός από μεμονωμένα παραδείγματα, μπορεί να βρεθεί ένα γενικευμένο παράδειγμα που να ορίζει ποια είναι τα κατάλληλα αποτελέσματα της πληροφορικής τα οποία έχουν θέση στη δευτεροβάθμια εκπαίδευση.

Αναφορές

ACM. (2016, 07 01). Cryptography Pioneers Receive ACM A.M. Turing Award. Ανάκτηση από https://goo.gl/quphJ2

Diffie, W., & Hellman, M. (1976). New Directions In Cryptography. IEEE Transactions on Information Theory, 644–654.

Khan Academy. (2016, 07 01). Public key cryptography: What is it? Ανάκτηση από https://goo.gl/Fyo9GB

Online Color Mixing Tool. (2016, 07 01). Ανάκτηση από http://trycolors.com/

Singh, S. (2001). Κώδικες και μυστικά. Αθήνα: Τραυλός.

Vosniadou, S., & Brewer, W. (1987). Theories of knowledge restructuring in development. Review of Educational Research, 51-67.

Wikipedia. (2016, 07 01). Ανάκτηση από Discrete Logarithm Records: https://en.wikipedia.org/wiki/Discrete_logarithm_records

Αδαμόπουλος, Ν. (2005). Χρήση Αναλογιών και Μεταφορών στη Διδασκαλία του Μαθήματος 'Μετάδοση Δεδομένων & Δίκτυα Υπολογιστών': Μια μελέτη Περίπτωσης. 3ο Πανελλήνιο Συνέδριο "Διδακτική της Πληροφορικής". Κόρινθος.

Αλεξόπουλος, Κ., & Ρόμπολα, Ε. (2012). Μια πρόταση για τη διδασκαλία του αλγόριθμου βέλτιστης διαδρομής του Dijkstra στο Γενικό Λύκειο. 4th Conference on Informatics in Education (σσ. 110-122). Πειραιάς: ΕΠΥ.

Καραγεώργος, Π. (2010). Ένα Ηλεκτρονικό Μάθημα με Θέμα την Αυθεντικότητα και την Εμπιστευτικότητα στη Μετάδοση Πληροφοριών. Workshop on Informatics in Education (σσ. 29-38). Τρίπολη: ΕΠΥ.

Κιαγιάς, Ά. (2011). Προφορική συζήτηση στα πλαίσια διδασκαλίας.

Μπουκέας, Γ., Πουλάκης, Ε., & Τσοπόκης, Ι. (2012). Η Πληροφορική ως Μάθημα Γενικής Παιδείας. 6ο Πανελλήνιο Συνέδριο Καθηγητών Πληροφορικής. Πάτρα.

Παγουρτζής, Α., & Ζάχος, Ε. (2016). Υπολογιστική Κρυπτογραφία. Αθήνα: ΣΕΑΒ.

Πέρδος, Α., Δουκάκης, Σ., Γιαννοπούλου, Ν., & Σαράφης, Ι. (2015). Ανάπτυξη Διαδικτυακής Εφαρμογής Κρυπτογράφησης Αποκρυπτογράφησης Κειμένου με Βάση Αλγόριθμους Μετάθεσης. 7th Conference on Informatics in Education (σσ. 84-92). Πειραιάς: ΕΠΥ.

Abstract

We present a teaching proposal for the Diffie – Hellman Key Exchange, an important cryptographic technique that is crucial to the Internet and the World Wide. Despite the fact that it builds on advanced knowledge of mathematics, we support that, at its core it consists of processes that are easily understood by Senior High School students. To this end we cite analogies from the bibliography and everyday life and analyze potential benefits and problems.

Λέξεις κλειδιά: Cryptography, Diffie – Hellman Key Exchange, Asymmetry, Computational Thinking