Παραθέτω μερικά από τα σχόλια σας που αφορούν τον τρόπο διδασκαλίας και το επίπεδο δυσκολίας του μαθήματος... Μερικές από τις ιδέες για βελτιώσεις που επαναλαμβάνονται από πολλούς από σας αφορούν τα εξής:

- **Σχόλιο:** «Προσωπικά, θα ήθελα για εξάσκηση να κάναμε κάποιες ασκήσεις στο μάθημα και να μας δίνεται χρόνος να τις απαντάμε μόνοι μας»

  Απάντηση ΤΔ: Αυτό γίνεται σε ένα βαθμό και θα προσπαθήσω να γίνεται περισσότερο στο μέλλον. Αλλά δυστυχώς η έλλειψη βοηθών για το μάθημα καθιστά δύσκολη την ύπαρξη φροντιστηριακών ωρών...

- **Σχόλιο:** «Σαν ιδεες για βελτιωση, πιστευω οτι περισσοτερες πρακτικες εφαρμογες στις εργασιες θα ανεβαζαν το ενδιαφερον, ισως και διανομη ενος συγγραμματος στο μελλον για περισσοτερες πληροφοριες για το μαθημα ...»

  Απάντηση ΤΔ: Και εγώ θα ήθελα περισσότερες πρακτικές εφαρμογές, αλλά φοβάμαι ότι έτσι θα απέκλεια πολλούς συμφοιτητές σας που δεν αισθάνονται τόσο άνετα με τον προγραμματισμό (αν και οι ασκήσεις με το Vigenere, με τα DES/AES/κλπ, με το PGP έχουν αυτό τον χαρακτήρα). *Γι' αυτό λοιπόν θεώρησα ότι είναι καλό οι ασκήσεις να είναι μεν «θεωρητικές» αλλά να αφορούν real-life πρωτόκολλα και εφαρμογές (όπως με τα authentication πρωτόκολλα, τα cookies, κλπ.) ώστε να δείτε πως εφαρμόζεται η κρυπτογραφία στην πράξη. Υπόσχομαι όμως ότι σε λίγες εβδομάδες θα έχετε την ευκαιρία να κάνετε κάποιου είδους hacking…*☺

  Όσο για το σύγγραμα έχει ήδη παραγγελθεί αλλά όταν το παραλάβετε δεν νομίζω να σας είναι και ιδιαίτερα χρήσιμο...

- **Σχόλιο:** «Θα μπορούσαμε να εγκαταστήσουμε στον υπολογιστή της αίθουσας κάποια προγράμματα (εσείς γνωρίζετε ποια) ώστε να βλέπουμε την ώρα του μαθήματος πώς μπορούν να γίνουν στην πράξη οι επιθέσεις. Γενικά θα ήταν καλό να γίνει το μάθημα ακόμα πιο διαδραστικό.»

  Απάντηση ΤΔ: Αυτό σκόπευα να το κάνω σε επίπεδο ασκήσεων. Αλλά δυστυχώς ένας λόγος που δε μπορεί να γίνει αυτό σε ευρεία κλίμακα είναι γαιτί πολλές από αυτές τις τεχνολογίες είναι *dual use*. Αυτό σημαίνει ότι μπορεί να χρησιμοποιηθούν και για καλό και για κακό. Και η τάξη αυτή έχει πολλούς εν δυνάμει hackers... ☺

- **Σχόλιο:** «Για τις ασκήσεις θα μπορούσαμε να αφιερώνουμε ένα τέταρτο από το μάθημα, ώστε να τις συζητάμε στην τάξη, να μας εξηγείτε μερικά σημεία και γιατί όχι, να δίνετε και μερικά hints.»

  Απάντηση ΤΔ: Ναι αυτό μπορεί εύκολα να γίνει στο διάλειμμα ή στο τέλος του μαθήματος..

- **Σχόλιο:** «Μια σιγουρη βελτιωση θα ηταν οι διαφανειες του μαθηματος να μην ειναι στα αγγλικα και εφοσον σε καποια σημεια οι διαφανειες δεν ειναι παρα πολυ αναλυτικες καλο θα ηταν να υπηρχε και καποιο συγραμμα στο οποιο θα μπορουσαμε να ανατρεξουμε για λιγη πιο πολυ λεπτομερεια.»

  Απάντηση ΤΔ: Εδώ έχετε δίκιο και δεν μου αρέσει που οι διαφάνειες είναι στα Αγγλικά. Επιφυλάσσομαι λοιπόν για το μέλλον. Ελπίζω για την ώρα να μην αποτελούν εξαιρετικό πρόβλημα.

- **Σχόλιο:** «Οι προαιρετικές ασκήσεις ωστόσο είχαν πολύ μικρή βαθμολογική αξία, για την δουλειά που χρειαζόντουσαν...»

  Απάντηση ΤΔ: Το γνωρίζω αυτό. Δεν ήθελα όμως να είμαι άδικος με αυτούς που δε θα μπορούσαν να τις προσεγγίσουν. Ξέρω ότι «αδικώ» όσους τις λύνουν αλλά ελπίζω αυτή η αδικία να μειώνεται από το γεγονός ότι αν ποτέ ασχοληθείτε ενεργά με την ανάπτυξη κρυπτογραφικών εφαρμογών , θα ξέρετε πως να χρησιμοποιήσετε τους αλγόριθμους αυτούς στην πράξη...

- **Σχόλιο:** «Τέλος ελπίζω η συνέχεια του μαθήματος να είναι το ίδιο ενδιαφέρουσα, και η πρόοδος και η εξέταση να έχουν θέματα που να χρειάζονται κατανόηση της θεωρίας όπως και στις ασκήσεις, αλλά να λύνονται σε λογικά πλαίσια χρόνου.»

  Απάντηση ΤΔ: Ναι, ναι, και ναι! ☺

- **Σχόλιο:** «Οι εργασίες του είναι χρονοβόρες και ανήκουν στην κατηγορία "Η το βρίσκω σε 5 λεπτά, η βασανίζομαι 8 ώρες" και κατα τη γνώμη μου θα έπρεπε να μετράνε περισσότερο απο 30%.

  Απάντηση ΤΔ: Θα δούμε. Φροντίστε να τα πάτε καλά στις εξετάσεις και δε θα χρειαστούν αλλαγές... Πάντως περισσότερο από 30% για ομάδες των δύο ατόμων μάλλον δεν είναι σωστό...

- **Σχόλιο:** « Ίσως θα ήταν αποδοτικότερο να υπάρχει συνέχεια αυτού ως μάθημα επιλογής *Κρυπτογραφία 2*, ώστε να μη χρειάζεται να πιεστούμε χρονικά και ποσοτικά..»

  Απάντηση ΤΔ: Αυτό πρέπει να το [συ]ζητήσετε σε μια συνέλευση τμήματος. Για την ώρα υπάρχει μόνο Κρυπτογραφία 1. Ας δούμε λοιπόν τι μπορούμε να πετύχουμε στα πλαίσια αυτού του μαθήματος.

- **Σχόλιο:** «... καθώς και η εφαρμογή των attack game που κάνουμε στο μάθημα με κάποιο πιο πρακτικό/ηλεκτρονικό τρόπο (πχ να υπάρχει ένας server που να παίζει τον ρόλο του Oracle, και εμείς με κάποιο πρόγραμμα να κάνουμε τα attacks...?). Γενικά η μαγεία της Κρυπτογραφίας είναι στο να βλέπεις ζωντανά το να σπάει (πχ) ένα σύστημα!»

  Απάντηση ΤΔ: Όπως είπα πριν και εμένα θα μου άρεσε να γίνει το μάθημα έτσι. Αλλά αυτό θα απαιτούσε κάποιες γνώσεις Network Programming από όλους, που από όσο ξέρω δεν είναι δεδομένες στα μικρότερα έτη...

- **Σχόλιο:** «... και ελπίζω στο μέλλον να μην εστιάσουμε τόσο στη θεωρία αριθμών όπως ΝΟΜΙΖΑ ότι είναι η κρυπτογραφία.

  Απάντηση ΤΔ: Κανονικά έτσι έπρεπε να γίνει το μάθημα, αλλά σκέφτηκα να το ανοίξω σε περισσότερο κόσμο για να δείτε πως εφαρμόζεται η κρυπτογραφία στην πράξη. Πάντως η κρυπτογραφία ΕΙΝΑΙ θεωρία αριθμών ☺ …

- **Σχόλιο:** «Mexri stigmis eimai efxaristimenos apo to mathima, oson afora tis dialekseis kai to yliko pou mas dinetai. Apla pistevw oti oi apetiseis (3 set askisewn + Proodos + Teliki eksetasi) einai ypervolika psiles. Tha protina na ginontan 2 ta set askisewn h na mh ginotan h proodos.»

  Απάντηση ΤΔ: No can do ☺... *Πάντως για το υπόλοιπο μισό θα αναπροσαρμόσω λίγο τις απαιτήσεις του μαθήματος και θα λάβω υπόψη το φόρτο εργασίας των προπτυχιακών φοιτητών.*

  Η πρόοδος θα σας χρειαστεί για να ξέρετε τι θέματα περίπου θα υπάρχουν και στο τελικό διαγώνισμα...

- **Σχόλιο:** «Mia protasi veltiwsis toy mathimatos, tha itan na yparxei ksexoristo mathima gia tous metaptixiakous foitites. Me ayton ton tropo tha mporousame na emvathinoume perisotero se kapoia pio proxwrimena zitimata.»

  Απάντηση ΤΔ: Αυτό θα ήταν ιδανικό, αλλά για την ώρα δε μπορεί να γίνει, λυπάμαι. Στο μέλλον, πάντως, έτσι θα διδάσκεται το μάθημα.

- **Σχόλιο:** «Το μόνο που θα ήθελα είναι ορισμένες ασκήσεις να μην είναι σπαζοκεφαλιες και να μην σε εξετάζουν μόνο στο πόσο έξυπνος είσαι, άλλωστε κάποιοι παρακολουθούν το μάθημα απλά για να πάρουν βασικές γνώσεις για την ασφάλεια συστηματων. Γνωρίζω παιδιά τα οποία παράτησαν το μάθημα επειδή δύσκολα τα έβγαζαν πέρα με τις ασκήσεις.»

  Απάντηση ΤΔ: Οι ασκήσεις είναι «σπαζοκεφαλιές» επειδή δεν είστε εξοικιωμένοι με αυτού του είδους τις ασκήσεις. Πιστεύω όμως ότι σιγά-σιγά θα τις θεωρείτε δεδομένες. Όσο για τα παιδιά που έφυγαν, ίσως θα έπρεπε να επιμείνουν λίγο παραπάνω.

<u>Ακολουθούν αναλυτικά τα σχόλια που μου στείλατε κρυπτογραφημένα με το PGP και αφορούν παράπονα και ιδέες για βελτιώσεις</u>

Μέχρι τώρα, τα περιεχόμενα των μαθημάτων κατά τη γνώμη μου είναι αρκετά χρήσιμα και πιστεύω πως μέχρι το τέλος του εξαμήνου θα έχω μια καλή εικόνα για την κρυπτογραφία, το πως χρησιμοποιείται σήμερα, τους αλγόριθμους που υπάρχουν καθώς και κάποια βασικά πράγματα για τις επιθέσεις που μπορούν να γίνουν και πως να τις αποφεύγουμε.

...

Επίσης, οι διαλέξεις βοηθάνε πολύ αλλά ακόμα κι αν χάσεις κάποια υπάρχουν τα pdf του μαθήματος που είναι αρκετά κατατοπιστικά. Παρ' όλα αυτά, επειδή στις εργασίες μας ζητείται να σκεφτούμε κάποια πράγματα από μόνοι μας, πράγμα που μπορεί να μην τα καταφέρουμε πάντα, δεν το βρίσκω και εύκολο. Προσωπικά, θα ήθελα για εξάσκηση να κάναμε κάποιες ασκήσεις στο μάθημα και να μας δίνεται χρόνος να τις απαντάμε μόνοι μας (γίνεται με κάποιες ερωτήσεις, απλά θα προτιμούσα να κάναμε και μερικές ασκήσεις).

Το μάθημα της Κρυπτογραφίας, το επέλεξα αρχικά από "περιέργεια"...

Στη συνέχεια κατάλαβα πως είναι όντως ένας πολύ σημαντικός κλάδος της πληροφορικής, και αφού αποκτούσε ενδιαφέρον με τη δομή και το περιεχόμενο του, αποφάσισα να ασχοληθώ. Σημαντικό πιστεύω θα ήταν να γίνει μια μετάφραση των - πολύ καλών ομολογουμένως- διαφανειών στα ελληνικά. Αυτο θα βοηθούσε πολύ περισσότερο στην κατανόηση ορισμένων "λεπτών" εννοιών από όλους.

Στο τέλος ελπίζω να έχω καταφέρει να μπω στο κλίμα της Κρυπτογραφίας και να έχω αποκτήσει χρήσιμες γνώσεις σχετικά με αυτήν.

Το μάθημα είναι μέτριας δυσκολίας.Το δεύτερο σετ ασκήσεων ηταν εκθετικά δυσκολότερο του πρώτου. Το δεύτερο σετ ασκήσεων ηταν εκθετικά δυσκολότερο του πρώτου.

Θέλω όταν τελειώσει το μάθημα να μπορώ να στείλω κάτι στο Internet και να είμαι σίγουρος οτι δεν το διάβασε κανείς και αν πειράχτηκε το αρχικό μήνυμα να μπορώ να το καταλάβω. Δηλαδή να μπορώ να εφαρμόσω αυτά που λέμε στην τάξη πρακτικά.

...εκτός από τον επιστημονικό τομέα βρισκω ιδιαίτερα ενδιαφέρον την αναπτυξη της δημιουργικότητας στα πλαισια του μαθήματος. Επίσης βρίσκω ιδιαίτερα ενδιαφέρουσες τις ασκήσεις που ειναι περισσότερο πρόκληση πάρα μια καθιερομένη φοιτητική υποχρέωση.

...

Perimenw na exw mia kalh genikh eikona tou kladou ths kruptografias. Sto ma9hma de xreiazetai na alla3ei tipota, ginetai polu kalh douleia.

Το μάθημα είναι μέτριο προς το δύσκολο. Ειδικά το δεύτερο σετ ασκήσεων με δυσκόλεψαν αρκετά. Πιο συγκεκριμένα η τέταρτη άσκηση φαινόταν άλυτη, χωρίς να ξέρω ακόμη αν πλησίασα ή όχι την λύση. Σε γενικές γραμμές δεν είχα πρόβλημα, μέχρι το δεύτερο πακέτο ασκήσεων.

… η ύλη του μαθήματος: Καλύπτουμε ενδιαφέροντα θέματα για την ασφάλεια στις επικοινωνίες (χωρίς να μπαίνουμε σε λεπτομέριες μαθηματικών).

… Το μάθημα, είναι δύσκολο. Αυτό είναι σαφές. Όμως είναι και άκρως ενδιαφέρον για κάποιον που του αρέσει να αναλύει και να προσπαθεί να βρίσκει τις αδυναμίες ενός σχήματος. Σχετικά με τις ασκήσεις....το πρώτο σετ ήταν πραγματικά σε πολύ καλό επίπεδο δυσκολίας. Το δεύτερο όμως, με οδήγησε σε πλήρη απογοήτευση. Έμεινα στον υπολογιστή μου ώρες ολόκληρες χωρίς να μπορώ να βρω κάποια άκρη.

Ιδέες: Θα μπορούσαμε να εγκαταστήσουμε στον υπολογιστή της αίθουσας κάποια προγράμματα (εσείς γνωρίζετε ποια) ώστε να βλέπουμε την ώρα του μαθήματος πώς μπορούν να γίνουν στην πράξη οι επιθέσεις. Γενικά θα ήταν καλό να γίνει το μάθημα ακόμα πιο διαδραστικό.

Για τις ασκήσεις θα μπορούσαμε να αφιερώνουμε ένα τέταρτο από το μάθημα, ώστε να τις συζητάμε στην τάξη, να μας εξηγείτε μερικά σημεία και γιατί όχι, να δίνετε και μερικά hints. ...

Εξαιρετικά ενδιαφέρον μάθημα (το εννοώ αυτό!). Ιδιαίτερα καλή εντύπωση μου έχει κάνει το γεγονός ότι δε δίνετε "μασημένη τροφή". Οι ασκήσεις, στην πλειοψηφία τους, δεν είναι ούτε δύσκολες ούτε εύκολες, αλλά απαιτούν κατανόηση της ύλης, αρκετή ενασχόληση και σε κάποιο βαθμό ευρηματικότητα. Βελτιώσεις; Ίσως θα έπρεπε να γίνει καλύτερος συντονισμός με τα υπόλοιπα μαθήματα.

Epeleksa to mathima epeidh to vrisko poly endiaferon an kai to exo vrei kapos dyskolo. Exo dyskoleytei na katanohso tis epitheseis.Sto telos perimeno na exo mathei vasikes arxes ths Kryptografias. Tha voithouse arketa sto mathima an oi diafaneies htan sta ellhnika kai yphrxe kai ena syggrama pou anaferetai se osa didaskomaste.

....mas ma8ainei arketa xrhsima pragmata ta opoia omws efarmozontai akoma kai shmera kai den estiazei se palies xeperasmenes methodous kryptografias. Sto telos tou ma8hmatos pisteuw na exoun mpei kapoies baseis wste na mporoume na exetasoume pio polyploka systhmata asfaleias kai na sxediasoume systhmata asfaleias me oso to dynaton ligoteres "trypes".

To ma8hma to 8ewrw meshs dyskolias me askisis pou apaitoun kyriws autosxediasmo alla pisteuw oti mono etsi 8a ma8oume swsth kryptografia.

Pira to mathima apo endiaferon gia ton tomea kai logo tou didaskoda afou sto proto mathima mathame pos skopeuei na to diaxeiristei. To theoro arketa ipsilo to epipedo idietera sti deuteri askisi (i proti itan arketa vati aditheta me ti deuteri).

Pisteuo oti sto telos tou mathimatos tha exoume mathei arketa giro apo ton tomea tis asfaleias aditheta apo alles xronies pou to mathima itan sxedon ex oloklirou theoria arithmon. Poli kali douleia mono min anevasete kai allo to epipedo ton askiseon kai faneite elastikos se sxesi me tin teliki vathmologia! (Kanonikopoiisi pros ta pano!! :-))

Το μαθημα το επελεξα γιατι μου κινησε το ενδιαφερον και οντως επαληθευτηκα αν και ειναι αρκετα απαιτητικο.

...

Σαν ιδεες για βελτιωση , πιστευω οτι περισσοτερες πρακτικες εφαρμογες στις εργασιες θα ανεβαζαν το ενδιαφερον, ισως και διανομη ενος συγραμματος στο μελλον για περισσοτερες πληροφοριες για το μαθημα - περισσοτερες πηγες για να ανατρεχουμε για τις ασκησεις.

Το μαθημα αυτο το παρακολουθω γιατι πιστευω πως η κρυπτογραφια ειναι κατι το εξαιρετικα ενδιαφερον και μια μικρη εισαγωγη σε αλλο μαθημα μου αρεσε παρα πολυ.

...

Το μαθημα αυτο σιγουρα δεν ειναι καθολου ευκολο και απαιτει πολυ χρονο για την κατανοηση του και την ολοκληρωση των ασκησεων του. Μια σιγουρη βελτιωση θα ηταν οι διαφανειες του μαθηματος να μην ειναι στα αγγλικα και εφοσον σε καποια σημεια οι διαφανειες δεν ειναι παρα πολυ αναλυτικες καλο θα ηταν να υπηρχε και καποιο συγραμμα στο οποιο θα μπορουσαμε να ανατρεξουμε για λιγη πιο πολυ λεπτομερια.

Θα έλεγα ότι για μάθημα 6ου εξαμήνου η ύλη είναι αρκετή και οι ασκήσεις δύσκολες, αλλά με δουλειά και παρακολούθηση μπορούν να βγουν. Οι προαιρετικές ασκήσεις ωστόσο είχαν πολύ μικρή βαθμολογική αξία, για την δουλειά που χρειαζόντουσαν...

...

Πιστεύω ότι το μάθημα είναι πολύ καλό ως τώρα, θα έπρεπε να μην γίνεται σε 3ωρα γιατί παρόλο που είναι ενδιαφέρον χρειάζεται την συνεχή προσοχή όσων παρακολουθούν και αυτό είναι δύσκολο να επιτευχθεί σε ένα 3ωρο. Ίσως να βοήθαγε η ανακοίνωση των ασκήσεων λίγο νωρίτερα.

Τέλος ελπίζω η συνέχεια του μαθήματος να είναι το ίδιο ενδιαφέρον, και η πρόοδος και η εξέταση να έχουν θέματα που να χρειάζονται κατανόηση της θεωρίας όπως και στις ασκήσεις, αλλά να λύνονται σε λογικά πλαίσια χρόνου.

...

Θεωρώ ότι το μάθημα είναι μέτριας δυσκολίας αλλά απαιτητικό. Οι εργασίες του είναι χρονοβόρες και ανήκουν στην κατηγορία "Η το βρίσκω σε 5 λεπτά, η βασανίζομαι 8 ώρες" και κατα τη γνώμη μου θα έπρεπε να μετράνε περισσότερο απο 30%. Επίσης, θα βοήθαγε αν είχαμε ένα e-book με τη θεωρία αναλυτικά και όχι τα συμπικνωμένα slides η ακόμα καλύτερα να είχαμε το βιβλίο του μαθήματος...

Dialeksa to mathima giati endiaferomai na mathw perissotera gia thn asfaleia sto internet kai sta systhmata ypologistwn genikotera, kai h kryptografia einai shmantiko kommati tou tomea aytou. Oi askhseis tou mathimatos ws twra mou fainontai metrias dyskolias alla mou aresei pou apaitoun oxi toso gnwseis (mathimatikwn ktl) alla pollh skepsh kai psaksimo se diafores phges. Thewrw oti to mathima den xrhzei veltiwsewn kai oti prepei na synexistei me ayton ton tropo.

...

Par'ola ayta kai to periexomeno alla kai o tropos didaskalias moy kentrise to endiaferon . Pistevw pws san tomeas einai arketa periplokos. Oi ergasies wstoso einai bates kathws me tis sigkekrimenes gnwseis poy parexei to iliko sas alla kai me arketo psaksimo sto internet se sindiasmo me paaaaara poli skepsi linontai(ektos apo tin 4i askisi :P:P)

...

Θεωρώ ότι είναι ένα αρκετά απαιτητικό μάθημα, το αντικείμενο του οποίου δε μπορεί να καλυφθεί μέσα σε ένα 6/μηνο. Ίσως θα ήταν αποδοτικότερο να υπάρχει συνέχεια αυτού ως μάθημα επιλογής *Κρυπτογραφία 2*, ώστε να μη χρειάζεται να πιεστούμε χρονικά και ποσοτικά (από άποψη ύλης) αλλά να δωθεί ή δυνατότητα να μάθουμε αρκετά θέματα πιο άνετα και έχοντας στη διάθεση μας περισσότερο χρόνο.

...

Ενδιαφέρομαι ιδιαίτερα για το μάθημα κυρίως λόγω της πρόκλησης που περιέχει η ίδια η έννοια της ασφάλειας και της προστασίας της πληροφορίας.

Η σκέψη, η αναλυτική στρατηγική και ο πολυσύνθετος σχεδιασμός της αποτροπής ή ακόμα και του σχεδιασμού μιας επίθεσης, καθιστούν το μάθημα ιδιαίτερα ελκυστικό. Θεωρώ πως το μάθημα, από τη φύση του εμπεριέχει δύσκολες έννοιες και πολύπλοκες διαδικασίες, αυτό όμως που αναμένω είναι να αποκτήσω μια καλή εικόνα για το θέμα της ασφάλειας και της προστασίας των υπολογιστικών συστημάτω ώστε να μπορώ να ασχοληθώ αναλυτικότερα με το αντικείμενο.

...

Το μάθημα το επέλεξα γιατί μου φάνηκε ενδιαφέρον ο τομέας που ασχολείται καθώς και ο τρόπος που το προσεγγίζει αντί να μένει προσκολλημένο στα μαθηματικά και την θεωρία αριθμών.

...

Το μάθημα είναι σχετικά δύσκολο, αλλά θα φανεί και από το πως θα είναι οι ερωτήσεις στις εξετάσεις, που θα το κάνουνε ή απλά σχετικά δύσκολο ή πάρα πολύ δύσκολο αν είναι στο ίδιο στυλ με τις ερωτήσεις των ασκήσεων. Είναι αλήθεια ότι αν ξέρεις τις λύσεις είναι πάρα πολύ εύκολες αλλά το αντίθετο είναι πολύ δύσκολο και μπορεί να σκέφτεσαι την λύση για ώρες και να μην την βρεις ενώ είναι πολύ απλή!

...

Ακόμη πιστεύω πως 30% για τις ασκήσεις είναι πολύ λίγο αν σκεφτούμε πόσες ώρες θέλει μία διμελής ομάδα να τις λύσει (η και να αποτύχει να τις λύσει παρόλη την προσπάθεια).

Το αντικείμενο του μαθήματος είναι πολύ ενδιαφέρον, καθώς οι απαιτήσεις για ασφάλεια ολοένα και αυξάνουν. Περιμένω να γνωρίζω τουλάχιστον βασικά στοιχεία για νεότερα αλλά και παλαιά συστήματα ή πρωτόκολλα ασφαλείας, καθώς και αδυναμίες τους. Θα το χαρακτήριζα δύσκολο γιατί απαιτεί κάποιο βαθμό φαντασίας και αυτοσχεδιασμού, καθώς οι επιθέσεις που πρέπει να βρίσκουμε δεν βασίζονται πάντα σε κάτι που έχουμε ήδη συναντήσει.

...

Μια ιδέα για βελτίωση θα ήταν σίγουρα η μετάφραση των σημειώσεων στα Ελληνικά καθώς και η εφαρμογή των attack game που κάνουμε στο μάθημα με κάποιο πιο πρακτικό/ηλεκτροικό τρόπο (πχ να υπάρχει ένας server που να παίζει τον ρόλο του Oracle, και εμείς με κάποιο πρόγραμμα να κάνουμε τα attacks...?).

Γενικά η μαγέια της Κρυπτογραφίας είναι στο να βλέπεις ζωντανά το να σπάει (πχ) ένα σύστημα!

...

Το ωραίο με το μάθημα είναι ότι δεν χρειάζεται να μαθαίνουμε απέξω κατεβατά αλλά πιο πολύ χρειάζεται να σκεφτόμαστε λογικά. Για βελτίωση ίσως κάποιες πρακτικές εφαρμογές των παραδειγμάτων που συζητάμε. Και παραδείγματα απο την πραγματικότητα. (πχ η eve θα βρει έτσι πρόσβαση στο ταδε)

To mathima to thewrw idiaitera endiaferon an kai parallila arketa dyskolo. Pisteuw pantws pws sto telos tha exoume kataferei na gnwrizoume vasika themata tis kryptografias alla kai tha exoume mpei se mia kateuthinsi gia na psaxoume peraiterw pragmata. Me dyskoleuoun λigo oi diafaneies pou einai oles sta agglika, isws liges dieukriniseis sta ellinika (se merika paradeigmata) na voithousan perissotero.

To mathima einai dyskolo alla arketa endiaferon, opos eixate episimanei kai eseis o idios alloste stin proti dialeksi sas. Oi askiseis einai poly endiaferoyses epeidi afinoyn perithorio gia skepsi kai aytosxediasmo pano sto pos tha prospathiseis na "spaseis" i na prostatepseis" ena systima.Oi diafaneies merikes fores dyskolevoyn stin anagnosi kai katanoisi logo toy oti einai grammenes sta agglika.

Είναι πολύ ενδιαφέρον μάθημα η Κρυπτογραφία και μάλλον θα μου χρειαστεί το PGP από εδώ και πέρα κι ας μην κάνω BUY SELL

Ως τώρα τα πάω καλά και ελπίζω στο μέλλον να μην εστιάσουμε τόσο στη θεωρία αριθμών όπως NOMIZA ότι έιναι η κρυπτογραφία.

Οι σημειώσεις σας είναι πραγματικά πολύ χρήσιμες, αξίζει να μεταφραστούν.
Έχω πρόβλημα με τις προθεσμίες των ασκήσεων...

...
Mexri stigmis eimai efxaristimenos apo to mathima, oson afora tis dialekseis kai to yliko pou mas dinetai. Apla pistevw oti oi apetiseis (3 set askisewn + Proodos + Teliki eksetasi) einai ypervolika psiles. Tha protina na ginontan 2 ta set askisewn h na mh ginotan h proodos.

Σχετικά με το μάθημα είμαι αρκετά ευχαριστημένος με την όλη του λειτουργία.

...

Το μάθημα είναι αρκετά απαιτητικό και Θέλει αρκετό χρονο ασχολίας με αυτό καθώς και οι εργασίες είναι αρκετά δύσκολες.

...
Perimenw na mathw mesa apo to mathima vasikes arxes tis kriptografias kai enan kainoyrgio tropo skepsis epilisis Provlimatwn. Mia protasi veltiwsis toy mathimatos, tha itan na yparxei ksexoristo mathima gia tous metaptixiakous foitites. Me ayton ton tropo tha mporousame na emvathinoume perisotero se kapoia pio proxwrimena zitimata.

...
mou aresei o tropos me ton opoio ginetai to mathima kai eidika oi ergasies tou kathws pisteuw oti me vazei na skeftw enallaktika vazontas ti fantasia mou na doulepsei... Se oti afora ti diskolia tha to elega apaititiko.

Merikes protaseis veltiwseis tha itan:

-Pio elastikes imerominies paradosis ergasiwn

-Antistoixo mathima apokleistika gia to metaptixiako

-Parousiasi perisoterwn pragmatikwn paradeigmatwn paraviasis sistimatwn

---

Το μάθημα αυτό το πήρα από ενδιαφέρον για την κρυπτογραφία. Βέβαια αρχικά δεν ήμουν σίγουρη ότι θα το κρατήσω,όμως μετά τις πρώτες διαλέξεις το αποφάσισα.

Μερικά από τα πιο σημαντικά κίνητρα ήταν:

....

....

η ύλη του μαθήματος: Καλύπτουμε ενδιαφέροντα θέματα για την ασφάλεια στις επικοινωνίες (χωρίς να μπαίνουμε σε λεπτομέριες μαθηματικών).

To mathima to pairnw epeidi me endiaferei i kryptografia, alla kai genikotera i asfaleia twn ypologistwn. Einai arketa kalo, alla tha mporouse na einai ligo pio praktiko, me to na exei perissoteres programmatistikes askiseis, i toulaxiston aftes pou mpainoun na exoun megalyteri vathmologiki syneisfora. Px stin defteri ergasia i programmatistiki askisi, enw itan i pio xronovora, alla kai i pio endiaferousa, epiane mono 10 pontous, poly ligotero apo tis thewritikes. To idio kai stn prwti ergasia...

... To mathima to theoro arketa diskolo,eidika an skeftoume oti den einai basiko mathima,alla einai logiko logo tou oti apaitei opos eipate kai eseis kapoiou eidous autosxediasmo pou einai diskolo na didaktei.

... To mathima to theoro apo thn fysh tou dyskolo mias kai asxolite kai me theoria arithmon, mathimatika disbato klado, alla einai poly dhmiourgiko!

Η κρυπτογραφία θεωρώ οτι είναι ενα μάθημα ιδαίτερα ευχάριστο. Το μόνο που θα ήθελα είναι ορισμένες ασκήσεις να μην είναι σπαζοκεφαλιες και να μην σε εξετάζουν μόνο στο πόσο έξυπνος είσαι, άλλωστε κάποιοι παρακολουθούν το μάθημα απλά για να πάρουν βασικές γνώσεις για την ασφάλεια συστηματων. Γνωρίζω παιδιά τα οποία παράτησαν το μάθημα επειδή δύσκολα τα έβγαζαν πέρα με τις ασκήσεις. Εμένα προσωπικά με ενδιαφέρει ο τομέας της ασφάλειας των συστημάτων και μου αρέσει που μαθαίνω πράγματα πάνω σε αυτό.

Παίρνω το μάθημα γιατί η ασφάλεια των υπολογιστικών συστημάτων μου φαίνεται πολύ ενδιαφέρον και επίκαιρος ως τομέας. Παράλληλα είχα "επιστημονική" περιέργεια για το τι τελικά είναι η κρυπτογραφία.

Δυστυχώς λόγω δουλειάς δεν μπορώ να παρακολουθώ τις διαλέξεις του μαθήματος, και γι' αυτό βασίζομαι κυρίως στις διαφάνειες και σε εξωτερικές πηγές για τη μελέτη του. Υπο αυτή την έννοια, συναντάω δυσκολία στην κατανόηση κάποιων πραγμάτων, την οποία πιθανότατα να μην συναντούσα αν μπορούσα να παρακολουθώ τις διαλέξεις.

Πήρα το μάθημα γιατί είναι ενδιαφέρον. Στο τέλος μάλλον θα έχω μάθει κάποια πράγματα σχετικά με κρυπτογραφία, που πριν τα έβλεπα σε διάφορα μέρη και δε καταλάβαινα τι είναι. Μάλλον θα βοηθούσε πολύ αν οι διαφάνειες ήταν στα ελληνικά. Ίσως θα μπορούσε το μάθημα να έιναι λιγότερο απαιτητικό.

Πήρα το μάθημα επειδή βρίσκω ενδιαφέρουσα την κρυπτογραφία, αλλά είχα ασχοληθεί ελάχιστα με αυτή. Μου αρέσουν ιδιαίτερα τα σημεία εστίασης του μαθήματος, τα οποία αντίθετα με προηγούμενα έτη

δεν αφορούν ούτε μαθηματικά ούτε σκέτη θεωρία. Οι ασκήσεις είναι ενδιαφέρουσες αλλά και απαιτητικές. Τέλος, ενώ οι διαφάνειες και τα μαθήματα είναι αρκετά, θα ήταν χρήσιμο να είχαμε και κάποιο βιβλίο κρυπτογραφίας.

Το μάθημα έχει πολύ εντυπωσιακό όνομα. Εξίσου εντυπωσιακό είναι και το περιεχόμενό του. Βέβαια θεωρώ ότι το μάθημα είναι δύσκολο. Η δυσκολία δεν είναι στους αλγορίθμους ή στην ύλη γενικά, αλλά στην εφευρετικότητα που πρέπει να έχουμε για να μπορέσουμε να λύσουμε τις εργασίες, τις προόδους και το τελικό διαγώνισμα. Δυστυχώς η εφευρετικότητα αυτή δεν διδάσκεται πουθενά, με αποτέλεσμα να αυξάνεται ο συντελεστής δυσκολίας. Στο τέλος αυτού του μαθήματος περιμένω να μην είμαι τόσο naive χρήστης, αλλά περισσότερο ενημερωμένος και για τη δική μου αλλά και για την ασφάλεια των άλλων.

...

Για ένα εισαγωγικό μάθημα ο τωρινός τρόπος διδασκαλίας είναι προτιμότερος καθώς δίνει την ευκαιρία στους φοιτητές να καταλάβουν τι είναι η κρυπτογραφία, τα προβλήματα που έχει και πως λειτουργεί. Έτσι κάποιος μπορεί πιο εύκολα να αποφασίσει αν πραγματικά τον ενδιαφέρει.

Το μάθημα όπως παρουσιάζεται τώρα είναι αρκετα απαιτητικό αλλά οι εργασίες μέχρι τώρα έχουν πραγματικό ενδιαφέρον και μας βοηθούν να καταλάβουμε και στη πράξη πως λειτουργούν οι διάφορες μεθοδολογίες της κρυπτογραφίας.