Ανάπτυξη Διαδικτυακής Εφαρμογής Κρυπτογράφησης - Αποκρυπτογράφησης Κειμένου με Βάση Αλγόριθμους Μετάθεσης

Πέρδος Αθανάσιος[1], Δουκάκης Σπύρος[2], Γιαννοπούλου Νάγια[3], Σαράφης Ιωάννης[4]

[1]Ελληνογαλλική Σχολή Καλαμαρί, perdos@kalamari.gr
[2]PIERCE-Αμερικανικό Κολλέγιο Ελλάδος, sdoukakis@acg.edu
[3]Λεόντειο Λύκειο Πατησίων, gianagia@gmail.com
[4]Ελληνογαλλική Σχολή Καλαμαρί, sarafis@kalamari.gr

Περίληψη

Στην παρούσα εργασία, περιγράφεται η υλοποίηση μιας δράσης με θέμα την κρυπτογραφία στο πλαίσιο ομίλου για μαθητές της Α΄ Λυκείου. Οι μαθητές της Α΄ Λυκείου έχουν αποκτήσει εμπειρία σε βασικές έννοιες προγραμματισμού με τη χρήση της γλώσσας LOGO, στο μάθημα της Πληροφορικής της Γ΄ Γυμνασίου. Η δράση είχε ως κύριο στόχο να περιγράφουν οι μαθητές τι είναι η κρυπτογραφία, να δίνουν παραδείγματα εφαρμογών της και να υλοποιούν τεχνικές κρυπτογραφίας με τη χρήση υπολογιστών. Με τον τρόπο αυτό οι μαθητές ήρθαν σε επαφή με τα εφαρμοσμένα μαθηματικά αφού κλήθηκαν να επιλύσουν ένα πρακτικό πρόβλημα και να διαμορφώσουν και να μελετήσουν ένα μαθηματικό μοντέλο. Ενίσχυσε επίσης στους μαθητές την αλγοριθμική τους σκέψη και τους βοήθησε να αποκτήσουν νέες προγραμματιστικές τεχνικές, ενώ παράλληλα καλλιεργήθηκε και η κουλτούρα του ελεύθερου λογισμικού.

Λέξεις κλειδιά: κρυπτογραφία, Αλγόριθμος του Καίσαρα, ομαδοσυνεργατικότητα, STEM

1. Εισαγωγή

Ο κύριος σκοπός της συμμετοχής των μαθητών σε ομίλους δημιουργικότητας, είναι η ανάδειξη και η αξιοποίηση των ιδιαίτερων κλίσεων και ενδιαφερόντων των μαθητών. Στο πλαίσιο αυτών των ομίλων και των δημιουργικών εργασιών που υλοποιούνται, οι βασικές γνώσεις των μαθητών που έχουν αναπτυχθεί μέσα στη σχολική τάξη, αναδομούνται, αναπλαισιώνονται, αξιοποιούνται και αναπτύσσονται περαιτέρω.

Ο όμιλος «CryptoClub» με θέμα την ανάπτυξη λογισμικού κρυπτογράφησης – αποκρυπτογράφησης ελληνικού και αγγλικού κειμένου με βάση αλγόριθμους μετάθεσης, είχε ως στόχο την ενεργό συμμετοχή των μαθητών σε δράσεις στο πεδίο STEM (Science, Technology, Engineering and Mathematics).

Μέσα λοιπόν σε ένα πλαίσιο προσέγγισης στο πεδίο STEM, τα θέματα που διαπραγματεύτηκαν οι μαθητές στον όμιλο περιελάμβαναν α) τη συζήτηση του ιστορικού

ISBN: 978-960-578-010-4.

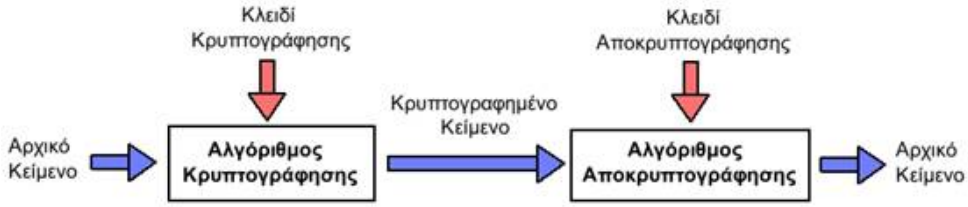
πλαισίου των συστημάτων κρυπτογράφησης, β) τη μελέτη του ζητήματος κρυπτογράφησης – αποκρυπτογράφησης ελληνικού και αγγλικού κειμένου με βάση τον Αλγόριθμο του Καίσαρα, γ) τη δημιουργία του κατάλληλου μαθηματικού μοντέλου, δ) την ανάπτυξη των κατάλληλων αλγορίθμων, ε) την υλοποίηση των αλγορίθμων σε πρόγραμμα με τη χρήση του MicroWorlds Pro και στ) τη δημιουργία ιστοσελίδας για την παρουσίαση της εφαρμογής.

Όπως αναφέρθηκε λοιπόν κύριο έργο του ομίλου, ήταν η ανάπτυξη μίας εφαρμογής κρυπτογράφησης – αποκρυπτογράφησης ελληνικού και αγγλικού κειμένου με βάση τον αλγόριθμο του Καίσαρα (Beissinger & Pless, 2006). Η εφαρμογή αναπτύχθηκε με τη χρήση του MicroWorlds Pro και μπορεί να κρυπτογραφεί κείμενο που έχει γραφεί με ελληνικούς και αγγλικούς κεφαλαίους και πεζούς χαρακτήρες, ενώ παρέχει δυνατότητα και για αποκρυπτογράφηση.

2. Ανάπτυξη της εφαρμογής

2.1 Πλαίσιο εφαρμογής

Αρχικά, οι μαθητές του ομίλου, συζήτησαν τις έννοιες της κρυπτογράφησης – αποκρυπτογράφησης καθώς και ιστορικά ζητήματα που σχετίζονται με τις έννοιες αυτές. Επιπλέον, επιχειρήθηκε να εμπλακούν οι μαθητές σε αλγόριθμους κρυπτογράφησης και αποκρυπτογράφησης μέσω των εννοιών του αρχικού κειμένου, του κλειδιού και του κρυπτογραφημένου κειμένου (Εικόνα 1).



Εικόνα 1. *Τα βήματα που ακολουθούνται σε μία διαδικασία κρυπτογράφησης – αποκρυπτογράφησης ενός μηνύματος.*

Στη συνέχεια οι μαθητές εστίασαν στο ζήτημα της ανάπτυξης του σχετικού αλγορίθμου. Ο αλγόριθμος του Καίσαρα –που αναπτύχθηκε στο πλαίσιο του ομίλου– αποτελεί μία από τις απλούστερες και πιο γνωστές τεχνικές κωδικοποίησης στην κρυπτογραφία. Είναι κώδικας αντικατάστασης στον οποίο κάθε γράμμα του κειμένου αντικαθίσταται από κάποιο άλλο γράμμα με σταθερή απόσταση κάθε φορά στο αλφάβητο. Για παράδειγμα στην περίπτωση των Ελληνικών Κεφαλαίων Χαρακτήρων, με μετατόπιση 3, το Α θα αντικατασταθεί από το Δ, το Β από το Ε, και ούτω καθεξής. Η μέθοδος πήρε το όνομά της από τον Ιούλιο Καίσαρα, ο οποίος την χρησιμοποιούσε στην προσωπική του αλληλογραφία.

ISBN: 978-960-578-010-4.

2.2 Ο αλγόριθμος

Η ανάπτυξη του σχετικού αλγορίθμου παρουσιάζεται στη συνέχεια. Η υλοποίηση της εφαρμογής σε προγραμματιστικό περιβάλλον έγινε με τη χρήση του MicroWorlds Pro. Σε ότι αφορά τους ελληνικούς κεφαλαίους χαρακτήρες ο αλγόριθμος είναι ο εξής:

1. Διάβασε έναν - έναν τους χαρακτήρες προς κρυπτογράφηση και μετάτρεψέ τους σε κώδικα ASCII.
2. Αν ο κωδικοποιημένος χαρακτήρας είναι 32 (κενός χαρακτήρας) μην κάνεις τίποτα.
3. Αν ο κωδικοποιημένος χαρακτήρας είναι από το 193 (που είναι το Α) μέχρι το 217 (που είναι το Ω) μετάτρεψέ το σε αριθμό μεταξύ των 1 και 24.
4. Κρυπτογράφησε τον αριθμό με βάση το κλειδί χρησιμοποιώντας την συνάρτηση: $y = (x + k) \bmod 24$ όπου:
   y: κρυπτογραφημένος αριθμός
   x: αριθμός 1 - 24
   k: κλειδί
5. Άλλαξε τον αριθμό ώστε να γίνει μεταξύ του 193 και 217.
6. Μετάτρεψε τον αριθμό σε χαρακτήρα.
7. Βάλε τον κρυπτογραφημένο χαρακτήρα στο πλαίσιο κειμένου.

Παραπλήσιοι είναι και αλγόριθμοι για την κρυπτογράφηση των υπόλοιπων χαρακτήρων ελληνικών και αγγλικών, πεζών και κεφαλαίων. Επιπλέον, παρόμοιος είναι και ο αλγόριθμος της αποκρυπτογράφησης. Η μόνη διαφορά είναι στη χρήση της συνάρτησης η οποία αλλάζει ως εξής: $x = (y - k) \bmod 24$ όπου:

y: κρυπτογραφημένος αριθμός
x: αριθμός 1 - 24
k: κλειδί

Σε περίπτωση που προκύπτει αρνητικός αριθμός στην πράξη (y - k) τότε αλλάζει η συνάρτηση σε: $x = (24 - (y - k)) \bmod 24$.

Εφόσον επεξεργάζονται αγγλικοί χαρακτήρες ο αριθμός 24 αντικαθίσταται με τον αριθμό 26 το πλήθος δηλαδή των αγγλικών χαρακτήρων.

Όπως φαίνεται για να είναι σε θέση οι μαθητές να υλοποιήσουν τους αλγορίθμους γνώρισαν έννοιες της Θεωρίας Αριθμών, όπως η έννοια του υπόλοιπου (modulo) της διαίρεσης ακέραιων αριθμών.

2.3 Κωδικοποίηση

Στη συνέχεια παρατίθεται ενδεικτικά ο κώδικας κρυπτογράφησης και αποκρυπτογράφησης αγγλικών κεφαλαίων χαρακτήρων:

κρυπτογραφημένο, τύπωσε [Κρυπτογράφηση Αγγλικών Κεφαλαίων Χαρακτήρων]

ISBN: 978-960-578-010-4.

```
        κάνε "κ 1
        κάνε "φορές μέτρησε αρχικό
        επαναλαβε :φορές [
                κάνε "χ ascii στοιχείο :κ αρχικό
                ανδιαφορετικά :χ = 32
                        [κάνε "καβ ΒάλεΤ χαρ :χ :καβ]
                        [
                                ανδιαφορετικά ή (:χ < 65) (:χ > 90)
                                []
                                [
                                        κανε "αρ26 (:χ - 64)
                                        κάνε "καρ26 υπόλοιπο (:αρ26 + κλειδί) 26
                                        αν :καρ26 = 0 [κάνε "καρ26 26]
                                        κάνε "καρ :καρ26 + 64
                                        κάνε "κχ χαρ :καρ
                                        κάνε "καβ ΒάλεΤ χαρ :καρ :καβ
                                ]
                        ]
                                κάνε "κ :κ + 1
        ]
```

Αντίστοιχα για την αποκρυπτογράφηση έχουμε:

```
αρχικό, τύπωσε [Αποκρυπτογράφηση Αγγλικών Κεφαλαίων Χαρακτήρων]
        κάνε "κ 1
        κάνε "φορές μέτρησε κρυπτογραφημένο
        επαναλαβε :φορές
        [
                κάνε "χ ascii στοιχείο :κ κρυπτογραφημένο
                ανδιαφορετικά :χ = 32
                [κάνε "καβ ΒάλεΤ χαρ :χ :καβ]
```

ISBN: 978-960-578-010-4.

```
        [
            ανδιαφορετικά ή (:χ < 65) (:χ > 90)
            []
            [
                κάνε "αρ26 (:χ - 64)
                κάνε "καρ26 υπόλοιπο (:αρ26 - κλειδί) 26
                αν :καρ26 < 0 [ κάνε "καρ26 υπόλοιπο (26 + :καρ26)
26]

                αν :καρ26 = 0 [κάνε "καρ26 26]
                κάνε "καρ :καρ26 + 64
                κάνε "καβ ΒάλεΤ χαρ :καρ :καβ
            ]
        ]
        κάνε "κ :κ + 1
    ]
```

Όπως φαίνεται από τον κώδικα οι μαθητές χρειάστηκε να ανακαλέσουν τις γνώσεις τους σχετικά τόσο με τη δομή επανάληψης όσο και με τη δομή επιλογής ώστε να υλοποιήσουν τους αλγόριθμους κρυπτογράφησης και αποκρυπτογράφησης. Επίσης ήρθαν σε επαφή με την έννοια της δομής δεδομένων αφού κλήθηκαν να χειριστούν λίστες που περιείχαν το κείμενο προς επεξεργασία. Σε ότι αφορά τη διαχείριση των λιστών που χρησιμοποιεί η γλώσσα LOGO, οι μαθητές αρχικά παρακολούθησαν μία εισαγωγή από τον καθηγητή τους και στη συνέχεια με τη χρήση του εγχειριδίου του MicroWorlds, πειραματίστηκαν, συνεργάστηκαν και τελικά ανέπτυξαν τον κώδικα.

Πέρα όμως από την κρυπτογράφηση – αποκρυπτογράφηση οι μαθητές του ομίλου σχεδίασαν και υλοποίησαν τους λεγόμενους κύκλους αντιστοίχησης κρυπτογραφημένων και αποκρυπτογραφημένων χαρακτήρων με στόχο να αναδείξουν την διαδικασία όσο απλούστερα γίνεται στους συμμαθητές τους. Για να το πετύχουν αυτό οι μαθητές του ομίλου ανακάλεσαν γνώσεις από το μάθημα των Μαθηματικών της Β΄ Γυμνασίου και συγκεκριμένα της Γεωμετρίας (Βλάμος κ.α., 2007) τις οποίες τις συνδύασαν με γνώσεις από το μάθημα της Πληροφορικής της Γ΄ Γυμνασίου (Αράπογλου κ.α., 2006).

Ενδεικτικά παρατίθεται ο κώδικας σχεδιασμού των κύκλων:

ISBN: 978-960-578-010-4.

```
για κυκλος :α
στα

θέσεχ -360 * :α / (2 * 3.14 ) + 180
θέσεψ 0

στκ
επαναλαβε 360[μπ :α δε 1]

τέλος

για σχ_γρ

επαναλαβε 24[
δε 90
μπ 360 * 1 / (2 * 3.14 )
πι 360 * 1 / (2 * 3.14 )
αρ 90
στα
επαναλαβε 15[μπ 3 δε 1]
στκ
]
τέλος
```

2.4 Η εφαρμογή

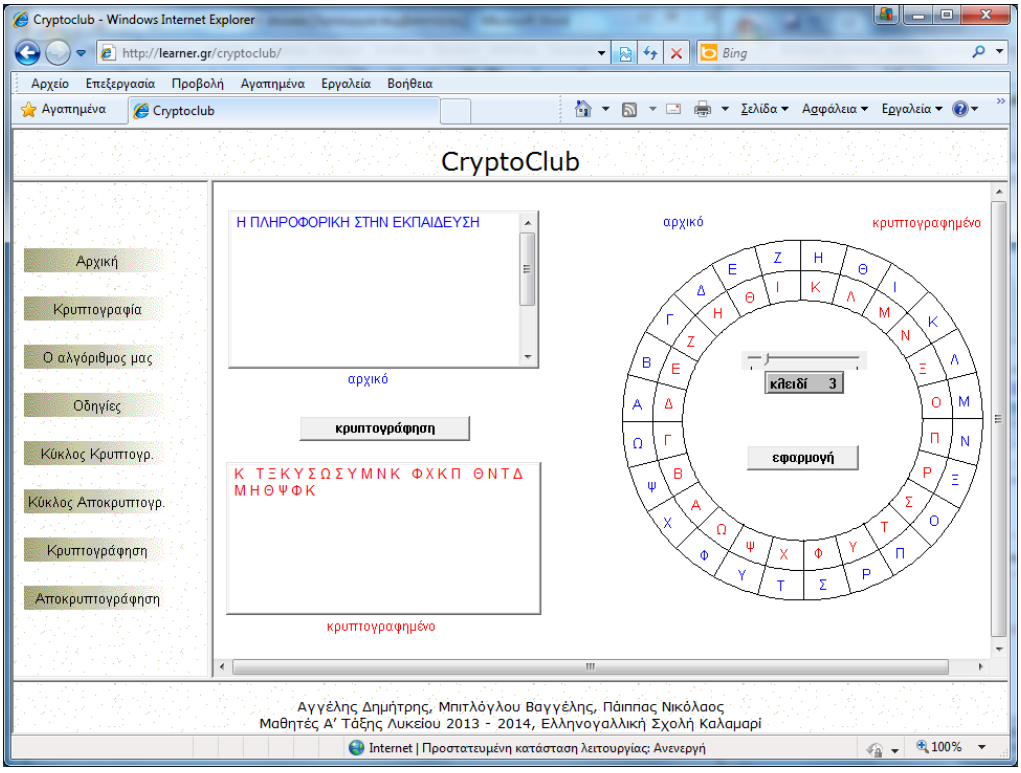
Η ανάπτυξη του αλγορίθμου και η υλοποίησή του σε προγραμματιστικό περιβάλλον, οδήγησε στο επόμενο στάδιο, όπου, οι μαθητές ήρθαν σε επαφή και με το ζήτημα του σχεδιασμού και ανάπτυξης ιστοσελίδων, ώστε να είναι διαθέσιμη η εφαρμογή μέσω διαδικτύου.

Η ιστοσελίδα που ανέπτυξαν οι μαθητές περιέχει εκτός από την εφαρμογή κρυπτο-γράφησης – αποκρυπτογράφησης και σχετικές αναφορές τόσο στην κρυπτογραφία

ISBN: 978-960-578-010-4.

όσο και στον αλγόριθμο που χρησιμοποιήθηκε. Επίσης υπάρχουν οδηγίες για τη χρήση της εφαρμογής.

Στις ακόλουθες εικόνες, φαίνεται το τμήμα κρυπτογράφησης ελληνικού κειμένου που αποτελείται από κεφαλαίους χαρακτήρες καθώς και ο κύκλος κρυπτογράφησης, με κλειδί 3 και κλειδί 11. Η εφαρμογή βρίσκεται πλήρης στο δικτυακό τόπο: http://learner.gr/cryptoclub/ ενώ υπάρχει και η κατάλληλη διεύθυνση επικοινωνίας με την οποία μπορεί να επικοινωνήσει κάποιος για να αποκτήσει τα αρχεία της εφαρμογής.



Εικόνα 2. *Κρυπτογράφηση ελληνικού κειμένου με κλειδί 3.*

3. Μαθησιακά οφέλη

Η υλοποίηση του συνόλου των δράσεων της εφαρμογής είχε ετήσια διάρκεια. Μέσα λοιπόν από ένα ενδιαφέρον πρόβλημα στο πεδίο STEM, οι μαθητές που συμμετείχαν στον όμιλο, ήρθαν σε επαφή με τα ζητήματα κρυπτογράφησης – αποκρυπτογράφησης ελληνικού κειμένου με βάση τον Αλγόριθμο του Καίσαρα, ανέπτυξαν την αντίστοιχη εφαρμογή με τη χρήση του MicroWorlds Pro και κατασκεύασαν κατάλληλη ιστοσελίδα. Επιπλέον, συζήτησαν το ιστορικό πλαίσιο των συστημάτων κρυπτογράφησης,

ISBN: 978-960-578-010-4.

πειραματίστηκαν με την ισχύ των προσωπικών κωδικών και ευαισθητοποιήθηκαν σε σχέση με την κρυπτογραφία.

Ένα σημαντικό όφελος επίσης για τους μαθητές που συμμετείχαν στον όμιλο ήταν και το πλαίσιο συνεργασίας μέσα στο οποίο κλήθηκαν να δημιουργήσουν. Ανατέθηκαν ρόλοι, μοιράστηκαν εργασίες οι οποίες υλοποιήθηκαν παράλληλα, τηρήθηκαν προθεσμίες και τέλος όλοι μαζί κλήθηκαν να συνθέσουν τις ατομικές τους εργασίες ώστε να ολοκληρώσουν το έργο. Επίσης λειτούργησαν και ως πολλαπλασιαστές για τους συμμαθητές τους αφού οργάνωσαν και ένα παιχνίδι θησαυρού στο οποίο έπρεπε να κρυπτογραφηθούν και να αποκρυπτογραφηθούν μηνύματα με τη χρήση της ιστοσελίδας. Έτσι ευαισθητοποίησαν τους συμμαθητές τους σε θέματα που αφορούν την κρυπτογραφία, ενώ παράλληλα ανέδειξαν και τις δυνατότητες επίλυσης πρακτικών προβλημάτων με τον προγραμματισμό. Επίσης οι ίδιοι οι μαθητές παρουσίασαν την εργασία τους στο 7ο Μαθητικό Συνέδριο Πληροφορικής στη Θεσσαλονίκη.

Με όλα τα παραπάνω, καλλιεργήθηκαν γνωστικές, συναισθηματικές, κοινωνικές και μεταγνωστικές δεξιότητες στους μαθητές μέσα από τη δημιουργία και εφαρμογή της συγκεκριμένης δραστηριότητας (Κασιμάτη, 2008). Το πλαίσιο λειτουργίας του ομίλου στηρίχθηκε στη διερευνητική και ομαδοσυνεργατική μέθοδο διδασκαλίας.

Στο πλαίσιο της διερευνητικής προσέγγισης οι μαθητές συνέλεξαν με επιστημονικές μεθόδους τις πηγές τους, απόκτησαν επιστημονικό λόγο μέσω του οποίου τεκμηρίωναν τις απόψεις και τις θέσεις τους. Επιπλέον, μέσα σε ένα πλαίσιο παρατήρησης, συλλογής και αρχειοθέτησης δεδομένων και πληροφοριών, έκαναν εικασίες, πραγματοποίησαν συγκρίσεις και σύνδεσαν την πρότερη γνώση τους με τις νέες έννοιες (κρυπτογράφηση και αποκρυπτογράφηση), οι οποίες είναι ιδιαίτερα χρήσιμες και στην ευρύτερη κοινωνία. Επιπρόσθετα, επιχείρησαν τις δικές τους ερμηνείες ώστε να διατυπώσουν τους σχετικούς αλγορίθμους, ενώ κατέληξαν στην ανάπτυξη της αντίστοιχης εφαρμογής με το MicroWorlds Pro και στην ανάπτυξη ιστοσελίδων με τη χρήση html. Στο πλαίσιο της εργασίας σε ομάδες, ανάμεσα στα μέλη της ομάδας υπήρξε η θετική αλληλεξάρτηση, ενώ ήταν ιδιαίτερα αναπτυγμένη η ατομική και η συλλογική ευθύνη των μελών.

4. Επίλογος

Θεωρούμε ότι η υλοποίηση σχετικών δράσεων συνεισφέρει στην ανανέωση της εκπαιδευτικής καθημερινότητας των μαθητών, αφού μέσα από πλαίσια ομαδοσυνεργατικότητας, διερεύνησης και βιωματικών δράσεων, οι μαθητές αντλούν ευχαρίστηση, κινητοποιούνται, παράγουν γνώσεις ή θεμελιώνουν αρτιότερα τις πρότερες γνώσεις τους.

Επίσης, μετά τις αλλαγές που αποφασίστηκαν από το Υπουργείο Παιδείας για το μάθημα πληροφορικής στη Γ΄ Γυμνασίου, σκοπεύουμε να αναδιαμορφώσουμε τη διδακτική μας προσέγγιση, να υιοθετήσουμε τη χρήση μιας Οπτικής Γλώσσας Προγραμ-

ISBN: 978-960-578-010-4.

ματισμού όπως η Scratch και να επιδιώξουμε την ανάπτυξη της εφαρμογής στη συγκεκριμένη γλώσσα. Η γλώσσα Scratch είναι πολύ πιο εύκολη για τους μαθητές τόσο στην εκμάθηση της λόγω της χρήσης των πλακιδίων, όσο και στην ανάπτυξη προγραμμάτων αφού δεν υπάρχουν συντακτικά λάθη.

Αναφορές

Beissinger, J., & Pless, V. (2006). *Cryptoclub: Using mathematics to make and break secret codes, workbook*, AK Peters Limited.

Psycharis, S., Botsari, E., & Chatzarakis, G. (2014). Examining the effects of learning styles, epistemic beliefs and the computational experiment methodology on learners' performance using the easy java. *Journal Educational Computing Research, 51(1), 91–118.*

Αράπογλου, Α., Μαβόγλου, Χ., Οικονομάκος, Η., & Φύτρος, Κ. (2006). *Πληροφορική Α΄ Β΄ Γ΄ Γυμνασίου*. Αθήνα, Οργανισμός Εκδόσεως Διδακτικών Βιβλίων.

Βλάμος, Π., Δρούτσας, Π., Πρέσβης, Γ., & Ρεκούμης, Κ. (2007). *Μαθηματικά Β΄ Γυμνασίου.* Αθήνα, Οργανισμός Εκδόσεως Διδακτικών Βιβλίων.

Κασιμάτη, Α. (2008). *Εισαγωγή στη Διδακτική Μεθοδολογία - Μεθοδολογία Εκπαιδευτικής Έρευνας*. Παιδαγωγική Επιμόρφωση Εκπαιδευτικών του Ο.Α.Ε.Δ.

Abstract

This paper presents how students of a greek Lyceum, who have basic programming skills using the language LOGO, were involved with an action on cryptography. The action mainly intended to make students able to describe what is cryptography, to give examples of implementations of cryptography, and to develop a computer application that encrypts and decrypts Greek and English text. In this way students negotiated issues related to the applied mathematics since they were asked to solve a practical problem and create a mathematical model. Also they developed algorithmic thinking and they learned new programming techniques. In addition they learned about free software since they created a web page that hosts both the application and the code.

Keywords: cryptography, STEM, Caesar Cipher

ISBN: 978-960-578-010-4.