ePublishing

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΤΕΚΜΗΡΙΩΣΗΣ
EKT
NATIONAL DOCUMENTATION CENTRE

Open Schools Journal for Open Science

Vol 3, No 6 (2020)

Λύνοντας Κρυπτογράμματα στο Scratch

Αντώνης Παπαδόπουλος, Ανατολή Μανωλίδου, Δημήτρη Λάμπρου, Ιλιάνα Ρήγα, Βασιλική Τσώνη, Μαριάννα Πέϊου, Νεφέλη Κασαμπαλίδου, Δήμητρα Ποτούλη, Απόστολος Θεοφυλίδης, Ιωάννης Λιαρής

doi: 10.12681/osj.24305

Copyright © 2020, Αντώνης Παπαδόπουλος, Ανατολή Μανωλίδου, Δημήτρη Λάμπρου, Ιλιάνα Ρήγα, Βασιλική Τσώνη, Μαριάννα Πέϊου, Νεφέλη Κασαμπαλίδου, Δήμητρα Ποτούλη, Απόστολος Θεοφυλίδης, Ιωάννης Λιαρής

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0.

To cite this article:

Παπαδόπουλος Α., Μανωλίδου Α., Λάμπρου Δ., Ρήγα Ι., Τσώνη Β., Πέϊου Μ., Κασαμπαλίδου Ν., Ποτούλη Δ., Θεοφυλίδης Α., & Λιαρής Ι. (2020). Λύνοντας Κρυπτογράμματα στο Scratch. *Open Schools Journal for Open Science*, *3*(6). https://doi.org/10.12681/osj.24305

https://epublishing.ekt.gr | **e-Publisher:** EKT | **Downloaded at:** 18/06/2025 04:04:53

Open Schools Journal for Open Science

Λύνοντας Κρυπτογράμματα στο Scratch

Αντώνης Παπαδόπουλος[1], Μανωλίδου Ανατολή[1] , Λάμπρου Δημήτρη[1], Ρήγα Ιλιάνα[1], Τσώνη Βασιλική[1], Πέϊου Μαριάννα [1], Κασαμπαλίδου Νεφέλη [1], Ποτούλη Δήμητρα [1], Θεοφυλίδης Απόστολος[1], Ιωάννης Λιαρής[2]

[1] Ελληνικό Κολλέγιο Θεσσαλονίκης, Θεσσαλονίκη, Ελλάδα

[2]Εκπαιδευτικος, Ελληνικό Κολλέγιο Θεσσαλονίκης, Θεσσαλονίκη, Ελλάδα

ΠΕΡΙΛΗΨΗ

Μαθητές της Γ' Γυμνασίου του Ελληνικού Κολλεγίου Θεσσαλονίκης επέλεξαν να ερευνήσουν και να κατανοήσουν σημαντικά κρυπτογράμματα για την εξέλιξη της κρυπτογραφίας. Έθεσαν ως στόχο να υλοποιήσουν μία εφαρμογή – παιχνίδι που θα υλοποιεί την κρυπτογράφηση απλού κειμένου χρησιμοποιώντας διαδεδομένες τεχνικές κρυπτογραφίας, όπως για παράδειγμα το κρυπτόγραμμα του Καίσαρα, τον κώδικα Μορς και τον κώδικα ASCII. Στόχος συνάμα ήταν η υλοποίηση αυτής της εφαρμογής με τη βοήθεια του οπτικού περιβάλλοντος προγραμματισμού Scratch, το οποίο εισάγει μαθητές σε αυτήν την ηλικία με επιτυχία στο δομημένο προγραμματισμό. Οι μαθητές θέλησαν να κατανοήσουν τις φάσεις δημιουργίας ενός τέτοιου είδους λογισμικού μετά από βιβλιογραφική έρευνα. Μπόρεσαν να κατανοήσουν εις βάθος τις μεθόδους κρυπτογράφησης μέσα από τη χαρά δημιουργίας μίας καινοτόμου εφαρμογής, διότι μπόρεσαν μέσα από δικά τους παραδείγματα να κατανοήσουν στην πράξη τους παραπάνω αλγορίθμους κρυπτογράφησης.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ:

κρυπτογραφία, οπτικός προγραμματισμός, Scratch

Open Schools Journal
for Open Science

1. ΕΙΣΑΓΩΓΗ

Στο σύγχρονο κόσμο, τα πάντα γύρω μας είναι κρυπτογραφημένα. Για κάθε κλήση στο κινητό τηλέφωνο, για κάθε καλωδιακό τηλεοπτικό κανάλι που παρακολουθούμε, βασιζόμαστε σε εκλεπτυσμένη ηλεκτρονική κρυπτογράφηση για να αποκλείσουμε την πρόσβαση σε αδιάκριτα μάτια και αυτιά. Όμως, η ανάγκη για κρυπτογράμματα δεν είναι τωρινό φαινόμενο, αλλά εδώ και περισσότερα από 2.000 χρόνια, οι κώδικες και τα κρυπτογράμματα παίζουν καθοριστικό ρόλο σε κάθε τομέα της οποιαδήποτε κοινωνίας. Μυστικά μηνύματα καθόριζαν την έκβαση πολέμων, διασώζαν και καταδίκαζαν ανθρώπους και καταστάσεις. Με τόσα να διακυβεύονται, δεν προκαλεί έκπληξη ότι υπάρχει μια διαρκής μάχη μεταξύ των κρυπτογράφων – αυτών που παλεύουν να κρύψουν το περιεχόμενο ενός μηνύματος με τη βοήθεια ενός κώδικα – και των κρυπταναλυτών, δηλαδή αυτών που προσπαθούν να δουν ότι λέει το κρυπτογραφημένο μήνυμα.

Είναι κατανοητό ότι με αυτόν τον τρόπο γεννήθηκε ο κλάδος της Κρυπτογραφίας, ο οποίος καθόρισε τον ρου της ιστορίας. Οι κώδικες που «πλάστηκαν» και ύστερα «σπάστηκαν» αιχμαλωτίζουν τη φαντασία και τονίζουν τη σημαντικότητα της ύπαρξης τους. Η κρυπτογραφία τις τελευταίες δεκαετίες της εξέλιξης της και με την εξάπλωση του Διαδικτύου και των Νέων Τεχνολογιών Διάδοσης Πληροφορίας, συνεργάζεται με τον κλάδο της Πληροφορικής, αφού οι κώδικες και τα κρυπτογράμματα πλέον ψηφιοποιούνται. Και οι δυο κλάδοι έχουν μία κοινή αφετηρία, τον αλγόριθμο. Ο τρόπος, με τον οποίο μπορούμε να επιλύσουμε μεθοδικά και με συγκεκριμένα βήματα και χαρακτηριστικά ένα πρόβλημα. Κοινός στόχος για τον κλάδο της Κρυπτογραφίας, όσο και για τον κλάδο της Πληροφορικής.

Η σημαντικότητα και η χρησιμότητα των δυο κλάδων αποτελεί κίνητρο για έναν μαθητή Γυμνασίου, για να μάθει, να ερευνήσει και να προγραμματίσει για κώδικες και κρυπτογράμματα. Η κατανόηση των «μυστικών» αυτών μπορεί να προέρθει μέσα από τον προγραμματισμό και τον πειραματισμό. Ο προγραμματισμός υλοποιείται πιο εύκολα μέσα από ψηφιακά παιχνίδια που προσφέρει στον εμπλεκόμενο διασκέδαση, ψυχαγωγία, αλλά με τον σωστό τρόπο κα μάθηση.

2. ΨΗΦΙΑΚΑ ΠΑΙΧΝΙΔΙΑ

Το παιχνίδι μπορεί να περιγραφεί ως μια δομημένη ή ημιδομημένη δραστηριότητα ανταγωνιστικού χαρακτήρα, ατομική ή ομαδική που γίνεται για ψυχαγωγικούς σκοπούς ακολουθώντας ορισμένους κανόνες για την επίτευξη κάποιου στόχου, ώστε να ανακηρυχθεί ένας ή περισσότεροι νικητές (Alessi & Trolip, 2001). Ο όρος «ψηφιακό παιχνίδι» χρησιμοποιείται στη διεθνή βιβλιογραφία για να περιγράψει προγράμματα που πρώτον, έχουν τα τυπικά χαρακτηριστικά παιχνιδιού και γεννούν στους χρήστες κίνητρο εμπλοκής, προσφέροντας άμεση διαδραστική εμπειρία που δημιουργεί το αίσθημα της ψυχαγωγίας (Salen & Zimmerman, 2003). Δεύτερον, παίζονται σε σύγχρονες ψηφιακές τεχνολογικές πλατφόρμες, π.χ.: υπολογιστή, Διαδίκτυο, κονσόλες παιχνιδιών. Γενικά, τα ψηφιακά παιχνίδια μπορούν να θεωρηθούν ως κάποιου είδους προσομοιώσεων, είτε κάποιου πραγματικού κόσμου (αθλητικά παιχνίδια, παιχνίδια ανάπτυξης πολιτισμών, αγωνιστικά παιχνίδια), είτε κάποιου φανταστικού (παιχνίδια φαντασίας και περιπέτειας), είτε ως υλοποίηση υπαρκτών παιχνιδιών (πάζλ, σταυρόλεξα). Οι προσομοιώσεις αυτές προσφέρουν στο χρήστη ψηφιακές αναπαραστάσεις γνωστών εργαλείων παιχνιδιού (όπως π.χ. κάρτες ή ζάρια) ή ακόμη δημιουργούν φανταστικούς κόσμους, όπου ο χρήστης – παίκτης καλείται να διαχειριστεί κάποια πραγματικά ή φανταστικά στοιχεία.

Η έννοια «gameplay» αποτελεί μια αφηρημένη έννοια που συχνά χρησιμοποιείται στο χώρο των ψηφιακών παιχνιδιών και σχετίζεται με τις εμπειρίες των χρηστών κατά τη διάδραση τους με το παιχνίδι. Στα ελληνικά μπορεί να μεταφραστεί ως «τρόπος παιχνιδιού» και επικεντρώνεται στις δυνατότητες αλλά και τους περιορισμούς που θέτει το παιχνίδι, όσο και τη συμπεριφορά του χρήστη. Παρά την αρχική της αποκλειστική σύνδεση με ψηφιακά παιχνίδι, η έννοια «gameplay» χρησιμοποιείται πλέον και για την περιγραφή παραδοσιακών μορφών παιχνιδιού. Το «gameplay» μπορεί να σημαίνει και η «καθαρή διάδραση του παιχνιδιού» που σχετίζεται με τους κανόνες του (Juul, 2005), ενώ ο Rouse (2005) τονίζει πως αυτή η έννοια τις περισσότερες φορές καθορίζεται από το «αποτέλεσμα της συσχέτισης εισόδου και εξόδου

μέσω επιλογών που κάνει ο χρήστης και αποκρίσεων του παιχνιδιού».

Εάν κάποιος θέλει να ασχοληθεί με το σχεδιασμό και την υλοποίηση ψηφιακών παιχνιδιών, καλό είναι να έχει υπόψη του και τη θεωρία που διέπει τα ψηφιακά παιχνίδια. Η χρήση της έννοιας «gameplay» έχει υποστεί κριτική λόγω της αφηρημένης υπόστασης της. Είναι συνηθισμένο, να περιγράφονται κάτω από τον ίδιο όρο τόσο η ευκολία ή δυσκολία χρήσης του παιχνιδιού, όσο και η γενικότερη ποιότητα του καθώς και η δυνατότητα του να προκαλέσει το ενδιαφέρον των χρηστών. Δεν υπάρχει γενικά αποδεκτός ορισμός της έννοιας αυτής, ενώ τα αίτια της δυσκολίας ενός τέτοιου ορισμού έγκειται στο γεγονός ότι ή έννοια αυτή δεν αφορά μια συγκεκριμένη οντότητα που μπορεί να προσδιοριστεί επαρκώς, αλλά αποτελεί τη συνισταμένη διαφόρων στοιχείων του παιχνιδιού που το καθένα συνεισφέρει με τον τρόπο του (Rollings & Adams, 2003).

3. ΤΟ ΜΟΝΤΕΛΟ PRENSKY ΓΙΑ ΤΗ ΜΑΘΗΣΗ ΜΕ ΨΗΦΙΑΚΑ ΠΑΙΧΝΙΔΙΑ

Ο Prensky (2001 ; 2002) παρουσιάζει ένα ολοκληρωμένο μοντέλο σχετικά με τις ευκαιρίες μάθησης που προσφέρει εγγενώς ένα παιχνίδι και θα εξηγηθούν παρακάτω, επειδή χρησιμοποιήθηκε στη δική μας μελέτη περίπτωσης. Πρώτα, ένα ψηφιακό παιχνίδι πρέπει να απαντάει στο ερώτημα ποιος είναι ο τρόπος παιχνιδιού (gameplay). Ο παίκτης πρέπει να κατανοήσει πως λειτουργούν τα διάφορα στοιχεία του παιχνιδιού, π.χ.: οι χαρακτήρες, τα αντικείμενα, τι μπορεί να πράξει ένας παίκτης με αυτά κ.α. Εδώ μπορούν να αναφερθούν αποτελέσματα ερευνών που δείχνουν, ότι τα παιχνίδια τα οποία απαιτούν από τους παίκτες να μάθουν πώς να διακρίνουν διαφορετικά σχεδιαστικά πρότυπα στο χώρο (π.χ.: Tetris), ενισχύουν τις νοητικές ικανότητες των παικτών, όσον αφορά την επεξεργασία οπτικοχωρικής πληροφορίας (Greenfield, 1998).

Δεύτερον, πρέπει να εξηγηθεί το τι μπορεί να κάνει κάθε παίκτης επακριβώς. Δηλαδή, ποιοι είναι οι κανόνες που διέπουν το παιχνίδι. Τι είναι επιτρεπτό να κάνει κάθε παίκτης και τι όχι. Τι θα γίνει, αν παραβιάσει κάποιον από τους κανόνες. Η Turkle (1995) διαπιστώνει ότι σε μεγάλο

βαθμό το παιχνίδι είναι ακριβώς η σε βάθος κατανόηση των κανόνων του μέσω διερεύνησης σεναρίων και στρατηγικών.

Ένα επόμενο στοιχείο που πρέπει να προσεχθεί είναι η απάντηση στο ερώτημα σε ποιο «κόσμο» και υπό ποιες συνθήκες εξελίσσεται το ψηφιακό παιχνίδι. Οι παίκτες πρέπει να μάθουν τους κανόνες του παιχνιδιού και τις αξίες σε αυτόν. Στο παιχνίδι δημιουργούνται κάποιες ειδικές συνθήκες, στις οποίες κάθε παίκτης χρειάζεται εξοικείωση, όπως περιβαλλοντικές, καιρικές συνθήκες, πολιτισμικές συνθήκες κ.α.

Ένα τελευταίο στοιχείο αποτελεί το επίπεδο λήψης αποφάσεων με βάση κυρίως κλίμακα ηθικών αξιών που είτε τονίζει το παιχνίδι και αναπτύσσει ο παίκτης παίζοντας, είτε είναι ήδη ανεπτυγμένες . Είναι το είδος των αποφάσεων που βασίζονται σε εκτιμήσεις για το αν μια στρατηγική- νόμιμη σύμφωνα με τους κανόνες του παιχνιδιού – θα ήταν αποδεκτό να εφαρμοστεί σύμφωνα με την ηθική ή γενικά με την κλίμακα αξιών του παίκτη.

Το παραπάνω μοντέλο μελετήθηκε και εφαρμόστηκε στο παρακάτω σενάριο, με σκοπό να συνδεθούν στοιχεία μάθησης που αναφύονται σε κάθε ένα άξονα συγκεκριμένα. Ένα επιτυχημένο ψηφιακό παιχνίδι καλλιεργεί στοιχεία μάθησης που αναδεικνύονται ενδογενώς, δηλαδή αναδεικνύονται από το σενάριο. Η ιδιαίτερη βοήθεια που δίνει αυτό το μοντέλο βασίζεται στο γεγονός ότι αναλύει την εμπειρία του ψηφιακού παιχνιδιού σε ειδικότερους άξονες για τους οποίους πρέπει να σχεδιαστούν και να προγραμματιστούν συγκεκριμένες λειτουργίες. Αυτό το γεγονός αποτελεί μία ευχάριστη πρόκληση για τους μαθητές.

4. Η ΕΠΙΛΟΓΗ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΣΤΟ ΣΕΝΑΡΙΟ ΜΑΣ

Οι μαθητές της συγκεκριμένης εργασίας καθοδηγήθηκαν από την ανάγκη για την επίτευξη δυο στόχων για την πραγματοποίηση της εργασίας. Ο πρώτος αφορά την βιβλιογραφική έρευνα, σπουδή, εφαρμογή, αλλά και την κατανόηση των πιο βασικών και διάσημων εννοιών και αλγορίθμων του κλάδου της Κρυπτογραφίας, ο οποίος παίζει καταλυτικό ρόλο στην καθημερινότητα μας. Αυτός ο στόχος θα μπορούσε να επιτευχθεί μέσα από την επίτευξη και

του δεύτερου στόχου που αφορά την υλοποίηση ενός ψηφιακού παιχνιδιού που προσφέρει μάθηση, τόσο στον προγραμματιστή, όσο και στο χρήστη μέσα από την έννοια του «gameplay». Ο κλάδος της Κρυπτογραφίας είναι αχανής με πολλούς αλγορίθμους και έπρεπε να γίνει μια προσεκτική επιλογή. Η επιλογή είχε ως κριτήριο, να κατανοηθούν οι πιο διαδεδομένοι αλγόριθμοι κρυπτογραμμάτων. Τι είναι όμως ένα κρυπτόγραμμα; Κρυπτόγραμμα είναι ένα συγκεκριμένο σύστημα που αντικαθιστά κάθε μεμονωμένο γράμμα του μηνύματος που θέλουμε να κωδικοποιήσουμε με κάποιο άγνωστο σύμβολο. Χαρακτηρίζεται από ευελιξία και ο τρόπος με τον οποίο κρυπτογραφείται μια λέξη στο μήνυμα μπορεί να εξαρτάται από τη θέση της στο μήνυμα και από πλήθος άλλων μεταβλητών, που καθορίζονται από τους κανόνες του συστήματος κρυπτογράφησης που ονομάζεται αλγόριθμος (Pincock, 2008). Ποια η διαφορά του κρυπτογράμματος με τον κώδικα; Ο κώδικας δίνει μεγαλύτερη έμφαση στα νοήματα παρά στους χαρακτήρες και αντικαθιστά ολόκληρες φράσεις ή λέξεις με αντίστοιχες κωδικές ομάδες που περιέχονται σε μια γνωστή λίστα. Επίσης, ένας κώδικας χαρακτηρίζεται από στατικότητα.

Οι μαθητές επέλεξαν τέσσερις μελέτες περίπτωσης κρυπτογραμματών και κωδικών, για να αναλύσουν και να μπορέσουν να μετατρέψουν σε ψηφιακό παιχνίδι. Αυτά είναι: το κρυπτόγραμμα του Καίσαρα, ο κώδικας Braille, ο κώδικας Morse και το κρυπτόγραμμα συμμετρικού κλειδιού.

Η χρήση μυστικής γραφής από τον Καίσαρα ήταν γνωστή στους αρχαίους. Ο ιστορικός Γάιος Σουτένιος, περιγράφοντας τη ζωή του Καίσαρα, περισσότερο από 100 χρόνια μετά, έγραψε ότι όποτε χρειαζόταν να πει κάτι εμπιστευτικό « το έγραφε με κρυπτόγραμμα». Όποιος ήθελε να αποκρυπτογραφήσει τα γράμματα του και να τα διαβάσει, θα έπρεπε να αντικαταστήσει το τέταρτο γράμμα του αλφαβήτου. Αυτός ο τύπος κρυπτογραφικής υποκατάστασης γραμμάτων είναι γνωστός ως μεταθετικό κρυπτόγραμμα του Καίσαρα. Ο Καίσαρας κρατούσε τα μυστικά του κρυμμένα μεταθέτοντας, απλώς, τα γράμματα κατά τρεις θέσεις προς τα αριστερά. Όμως η ίδια αρχή ισχύει οπουδήποτε κι αν μετακινήσουμε τα γράμματα, από μία μέχρι 24 θέσεις. Τέτοια κρυπτογράμματα, όπου τα γράμματα σε ένα μήνυμα αντικαθίστανται από μία άλλη ομάδα γραμμάτων, είναι γνωστά ως κρυπτογράμματα αντικατάστασης. Η άλλη μεγάλη

κατηγορία κρυπτογράφησης είναι τα κρυπτογράμματα μετάθεσης, όπου τα γράμματα ενός μηνύματος ανακατεύονται χρησιμοποιώντας έναν πίνακα.

Ο γνωστός σε όλους μας κώδικας ASCII (Αμερικανικός Πρότυπος Κώδικας για Ανταλλαγή Πληροφοριών, είναι ένα κωδικοποιημένο σύνολο χαρακτήρων του λατινικού αλφάβητου όπως αυτό χρησιμοποιείται σήμερα στην Αγγλική γλώσσα και σε άλλες δυτικοευρωπαϊκές γλώσσες. Χρησιμοποιείται για αναπαράσταση κειμένου στους υπολογιστές. Ιστορικά, ο ASCII αναπτύχθηκε από τηλεγραφικούς κώδικες. Η πρώτη εμπορική χρήση του ήταν ως κώδικας ενός τηλέτυπου 7 bit της Bell. Η δουλειά για τον ASCII ξεκίνησε επίσημα στις 6 Οκτωβρίου 1940, με την πρώτη συνάντηση της υποεπιτροπής X3.2 του Αμερικανικού Οργανισμού Τυποποίησης (American Standards Association, ASA). Η πρώτη έκδοση δημοσιεύτηκε το 1963, μία μείζων αναθεώρηση το 1967, και η πλέον πρόσφατη ενημέρωση το 1986. Σε σύγκριση με τους παλαιότερους τηλεγραφικούς κώδικες, ο προτεινόμενος κώδικας της Bell και ο ASCII ήταν διατεταγμένοι για πιο άνετη ταξινόμηση (π.χ. αλφαβητική σειρά) καταλόγων ενώ είχαν χαρακτηριστικά και για άλλες συσκευές εκτός από τηλέτυπα.

Οι μαθητές επέλεξαν να ερευνήσουν επίσης τον πολύ σημαντικό κώδικα Μορς, ο οποίος έφερε στην εποχή του τη δική του επανάσταση στην κρυπτογραφία. Το 1844 ο Αμερικανός εφευρέτης Σάμουελ Μορς κατασκεύασε την πρώτη τηλεγραφική γραμμή που κάλυπτε μια απόσταση περίπου 60 χιλιομέτρων, μεταξύ Βαλτιμόρης, Μέριλαντ και Ουάσιγκτον. Ο Μορς απέδειξε με το αλφάβητο του ότι η ηλεκτρική επικοινωνία μακράς αποστάσεως ήταν πλέον εφικτή και σηματοδότησε μια επανάσταση που θα είχε τεράστιο αντίκτυπο στην κοινωνία. Σε πολύ λίγο χρονικό διάστημα οι επιχειρήσεις άρχισαν να χρησιμοποιούν την τεχνολογία του και ειδικά στην ναυσιπλοΐα. Τα σύμβολά του αλφαβήτου του αποτελούνται από συνδυασμούς δύο μόνο στοιχείων. Αυτά τα στοιχεία είναι παλμοί μικρής και παλμοί μεγάλης διάρκειας. Οι παλμοί μεγάλης διάρκειας έχουν τριπλάσια διάρκεια από αυτήν των παλμών μικρής διάρκειας. Στο χαρτί και μόνο για τις ανάγκες της παράστασης του κώδικα συμβολίζουμε τους παλμούς μικρής διάρκειας με . (τελεία) και τους παλμούς μεγάλης διάρκειας με – (παύλα). Μέσα σε λίγες

δεκαετίες ένα πυκνό δίκτυο τηλεγραφικών καλωδίων διέσχιζε όλους τους ωκεανούς της υδρογείου, κάνοντας πραγματικότητα την ακαριαία παγκόσμια επικοινωνία.

5. ΥΛΟΠΟΙΗΣΗ ΨΗΦΙΑΚΟΥ ΠΑΙΧΝΙΔΙΟΥ

5.1. ΔΙΑΜΟΙΡΑΣΜΟΣ ΡΟΛΟΣ ΣΤΟ ΣΧΕΔΙΑΣΜΟ ΨΗΦΙΑΚΟΥ ΠΑΙΧΝΙΔΙΟΥ

Αυτό που προσπάθησαν να επιτύχουν οι μαθητές με την εργασία τους είναι να απαντήσουν στο ερώτημα, αν μπορούν μέσα από τον όρο «gameplay» στο οπτικό προγραμματιστικό περιβάλλον του Scratch, να φτιάξουν ένα ολοκληρωμένο λογισμικό που να επεξηγεί τους βασικούς αλγορίθμους κρυπτογράφησης.

Ένα ολοκληρωμένο ψηφιακό παιχνίδι περιλαμβάνει και αναπτύσσεται από μια ομάδα που έχει διακριτούς ρόλους. Διακρίνονται τρεις βασικοί ρόλοι. Κάθε ρόλο δε χρειάζεται να την έχει ένα άτομο, αλλά μπορεί να ανατεθεί και σε ολόκληρη ομάδα.

Ο πρώτος ρόλος είναι αυτός του σεναριογράφου. Ρόλος που έχει τις υπευθυνότητες της σύλληψης και της ανάπτυξης της κεντρικής ιδέας του σεναρίου του ψηφιακού παιχνιδιού και των διάφορων εκδοχών του. Αυτός ο ρόλος κατέχεται από τη συνεχόμενη διατήρηση του ενδιαφέροντος του παίκτη, αλλά και από τη δημιουργία ενός γενικά πρωτότυπου σεναρίου που διέπεται από ξεκάθαρους στόχους που πρέπει ο ή οι παίκτες να επιτύχουν.

Ο δεύτερος ρόλος είναι αυτός του αναλυτή – σχεδιαστή που μετασχηματίζει το σενάριο σε τρόπο παιχνιδιού (gameplay), για την ανάπτυξη των αντίστοιχων οθονών (storyboards) και συνολικά για την ανάλυση της πληθώρας των τεχνικών θεμάτων που μπορεί να αφορούν το παιχνίδι. Αποδεικνύεται εξίσου σημαντικός με τον πρώτο ρόλο.

Ο τρίτος ρόλος αναφέρεται στο ρόλο του προγραμματιστή, ο οποίος αναλαμβάνει τη συγγραφή κώδικα σύμφωνα με τις οδηγίες του αναλυτή – σχεδιαστή. Εδώ, μπορεί να χρησιμοποιηθεί ένα περιβάλλον προγραμματισμού που χαρακτηρίζεται εργαλείο συγγραφή παιχνιδιών (game authoring tools), τα οποία προσφέρουν στον προγραμματιστή τη δυνατότητα να χρησιμοποιεί ένα ενδιάμεσο, οπτικό επίπεδο προγραμματισμού με χρήση μιας εύχρηστης «μεταφοράς» στη διεπαφή. Ένα τέτοιο κατάλληλο περιβάλλον που θα αναλύσουμε παρακάτω και

χρησιμοποιήθηκε στη δική μας μελέτη περίπτωσης είναι το οπτικό προγραμματιστικό περιβάλλον Scratch. Σε ένα τέτοιο περιβάλλον μπορεί ο χρήστης γρήγορα και εύκολα να δημιουργεί εικονικούς κόσμους και να τους εμπλουτίζει με οντότητες – αντικείμενα. Στη συνέχεια χρησιμοποιώντας απλές σχετικά προγραμματιστικές τεχνικές, μπορεί να ρυθμίσει τη συμπεριφορά των οντοτήτων του, την αντίδραση τους στις ενέργειες του χρήστη, στους κανόνες του παιχνιδιού, το πώς αρχίζει και πότε τελειώνει κ.λ.π. Αυτός ο τρόπος εργασίας βοηθά το χρήστη – προγραμματιστή του εργαλείου συγγραφής να έρθει σε εξοικείωση με προγραμματιστικές έννοιες και δομές και να αναπτύξει δεξιότητες υπολογιστικής σκέψης.

5.2. ΥΛΟΠΟΙΗΣΗ ΣΕΝΑΡΙΟΥ ΣΤΟ SCRATCH

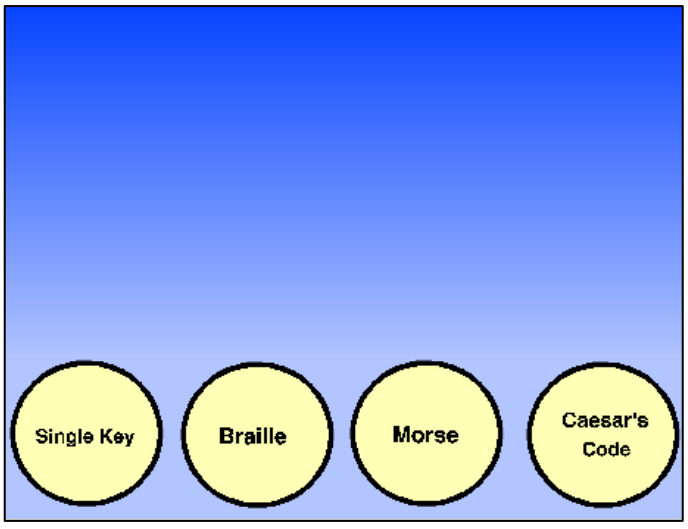
Στη δική μας μελέτη περίπτωση για μαθητές/τριες γ' Γυμνασίου επιλέξαμε την οπτική γλώσσα προγραμματισμού Scratch, όπως προαναφέραμε. Για να υλοποιήσουμε το δικό μας ψηφιακό παιχνίδι που είχε και στόχους μάθησης ακολουθήθηκαν οι παρακάτω φάσεις:

Στη φάση προετοιμασίας διδάχθηκε από τον εκπαιδευτικό με συγκεκριμένα φύλλα εργασίας το θεωρητικό υπόβαθρο για να μπορέσουν οι μαθητές να υλοποιήσουν ένα τέτοιο ψηφιακό παιχνίδι (δηλαδή το μοντέλο Prensky, ο όρος «gameplay», οι ρόλοι της ομάδας και οι κατάλληλες προγραμματιστικές δομές).

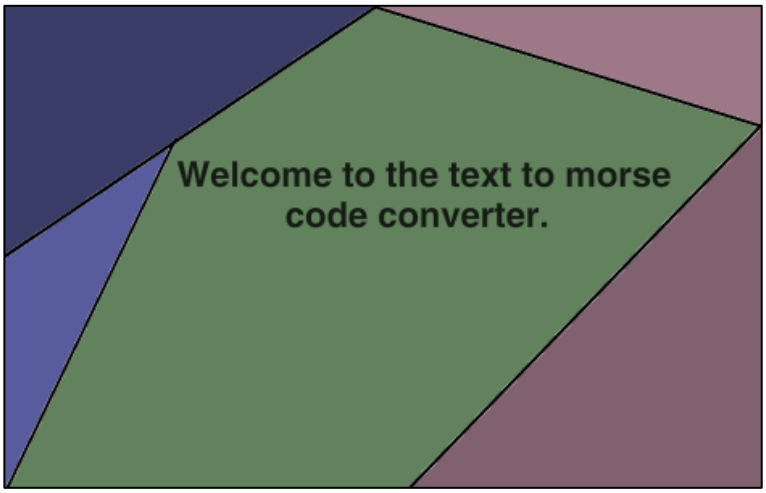
Ακολούθησε η φάση της σχεδίασης του ψηφιακού παιχνιδιού. Η ομάδα των μαθητών χρησιμοποίησαν την μέθοδο του καταιγισμού ιδεών (brainstorming), για να αποφασίσουν και να απαντήσουν σε ερωτήματα που αφορούσαν τους κανόνες και το πλαίσιο του ψηφιακού παιχνιδιού μάθησης. Σε αυτό το σημείο αποφασίστηκε και η κατανομή των διακριτών ρόλων των μαθητών σε ομάδες. Σε ένα παιχνίδι που παίζεται ελεύθερα ο μαθητής – παίκτης μπορεί να μην δοκιμάσει πότε μια στρατηγική που οδηγεί μεν σε αποτυχία αλλά μέσω της αποτυχίας προσφέρει ένα χρήσιμο μάθημα. Οι διακριτοί ρόλοι ενθάρρυναν τους μαθητές να εφαρμόσουν και να αναστοχαστούν πάνω σε στρατηγικές αποτυχίας. Το ψηφιακό τους παιχνίδι το ονόμασαν «Λύνοντας Κρυπτογράμματα στο Sratch». Τα γραφικά είναι αποκλειστικά δημιουργία των μαθητών.

Μετά από αυτήν τη φάση ακολούθησε η φάση της υλοποίησης του ψηφιακού παιχνιδιού στο οπτικό, προγραμματιστικό περιβάλλον του Scratch. Σε αυτήν τη φάση τα παιδιά υλοποίησαν φύλλα εργασίας που βασίζονται στο προγραμματιστικό πλαίσιο της θεωρίας, δηλαδή δομή ακολουθίας, δομή επιλογής και δομή επανάληψης που δόθηκαν από τον εκπαιδευτικό. Το αποτέλεσμα του παιχνιδιού που υλοποίησαν φαίνεται ενδεικτικά στα Σχήματα 1, 2 & 3, όπως και τμήματα του αλγορίθμου στα Σχήματα 4 και 5.

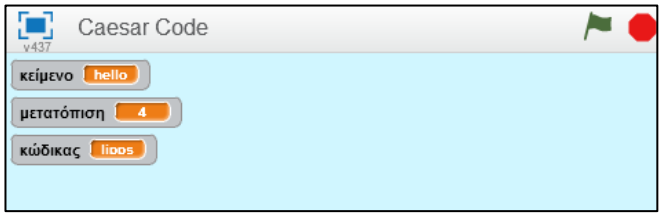
Είναι σίγουρο, ότι οι μαθητές αναλογίστηκαν, ότι είναι εφικτό να επεκτείνουν την εφαρμογή παιχνίδι που υλοποίησαν, αφού για να παίξει ένας χρήστης με κάθε παιχνίδι– κωδικοποίηση, πρέπει πρώτα να τελειώσει ένα ψηφιακό παιχνίδι. Αυτό θα μπορούσε στη δική μας περίπτωση να είναι ένας λαβύρινθος, στον οποίο ο χρήστης πρέπει να διαβεί και να βρει την έξοδο (ίσως σε συγκεκριμένο χρονικό διάστημα). Ακόμα, δεν πρέπει να ξεχνάμε, ότι η εφαρμογή έχει οθόνες με οδηγίες για τον τρόπο παιχνιδιού της εφαρμογής, όπως και για την ιστορική αναδρομή σε κάθε ξεχωριστή κωδικοποίηση.



Σχήμα 1: Επιλογή κρυπτογράμματος από την αρχική οθόνη

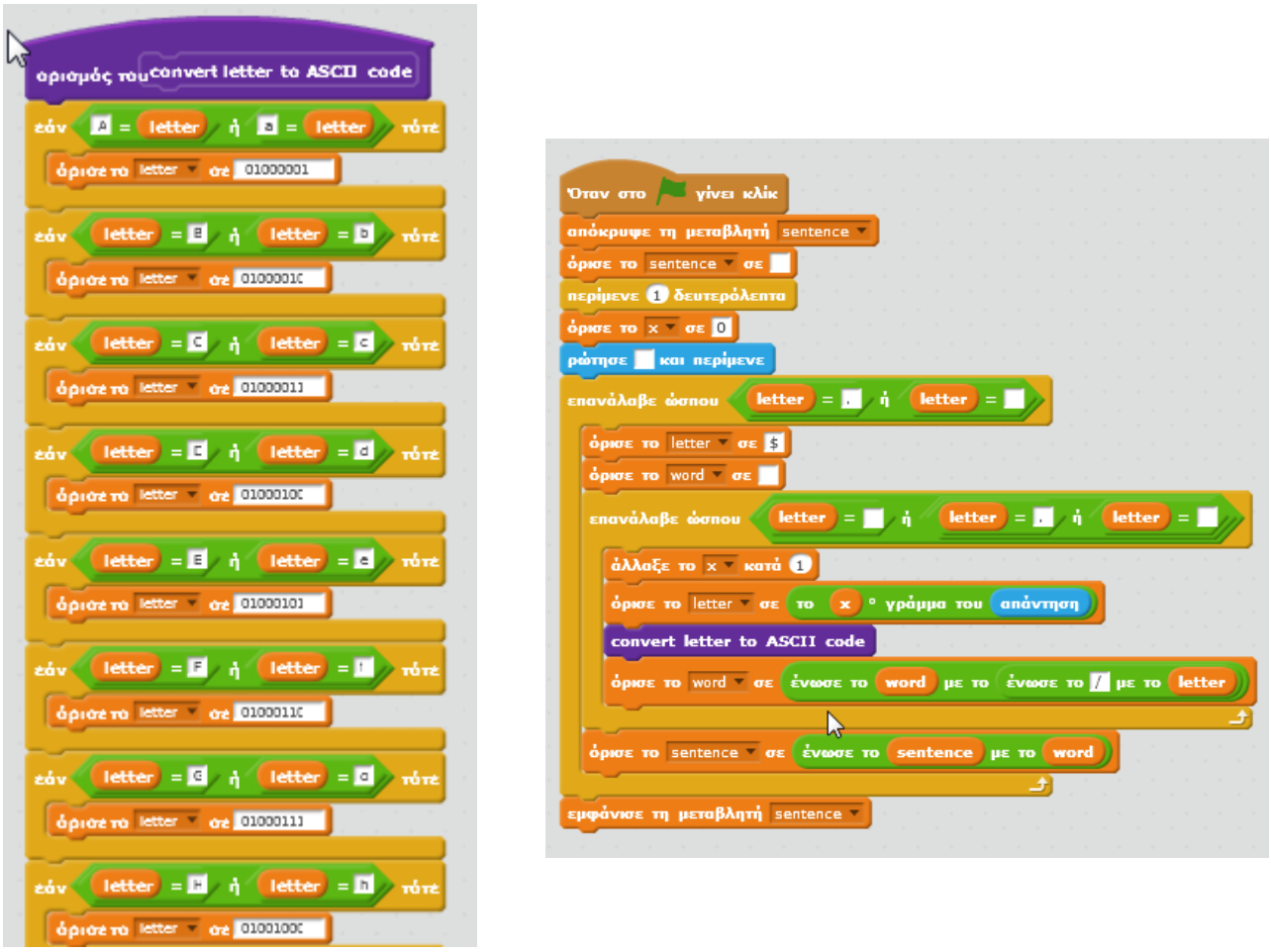


Σχήμα 2: Η επιλογή του μετατροπέα σε κώδικα Μορς



Σχήμα 3: Η μετατροπή σε κρυπτόγραμμα του Καίσαρα

Τελευταίο στάδιο ήταν η φάση του απολογισμού / αναστοχασμού. Στο τέλος του παιχνιδιού αναλύθηκε η εμπειρία των μαθητών/τριων που υλοποίησαν μέσα από τις προηγούμενες φάσεις, αλλά και στο τέλος που έπαιξαν το κάθε ψηφιακό παιχνίδι. Σε αυτή τη φάση οι μαθητές παρέδωσαν μία ηλεκτρονική παρουσίαση, για αυτό που δημιούργησαν. Επίσης, έλαβαν μέρος σε ανοικτή συζήτηση για την εμπειρία που αποκόμισαν.



Σχήμα 4: Παραδείγματα του αλγορίθμου

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Ο σχεδιασμός και η υλοποίηση ψηφιακών παιχνιδιών, στα πλαίσια του μαθήματος Πληροφορικής στο Γυμνάσιο, έχει στη συγκεκριμένη μελέτη περίπτωσης περισσότερο θετικά παρά αρνητικά αποτελέσματα στη διαδικασία μάθησης των μαθητών που την παρακολούθησαν. Αναθερμάνθηκε το ενδιαφέρον των μαθητών για τον προγραμματισμό και το μάθημα της Πληροφορικής. Κατανόησαν τι είναι η υπολογιστική σκέψη και τι είδους δεξιότητες χρειάζεται κάποιος, για να υλοποιήσει ένα ολοκληρωμένο, ψηφιακό παιχνίδι στο τόσο σημαντικό θέμα της Κρυπτογραφίας. Χρησιμοποίησαν τη φαντασία και τη δημιουργικότητα τους, για να υλοποιήσουν ένα δικό τους, πρωτότυπο σενάριο ως ψηφιακό

παιχνίδι που συνδύαζε στόχους μάθησης. Εφάρμοσαν μέσα από το παιχνίδι, όλα όσα έμαθαν στη διδασκαλία της θεωρίας του μαθήματος. Αυτή η προσέγγιση δίνει μία άλλη διάσταση στη διδασκαλία του μαθήματος της Πληροφορικής και ειδικά, όταν υλοποιείται σε ένα οπτικό περιβάλλον προγραμματισμού, όπως είναι το Scratch. Η πλειοψηφία των μαθητών/τριων ήταν ενθουσιασμένοι και δήλωσαν, ότι θα συμμετείχαν ξανά σε ένα τέτοιο εγχείρημα. Ανέπτυξαν σίγουρα και αρκετές κοινωνικές δεξιότητες, αφού διαπίστωσαν, ότι το κομμάτι της σωστής και αποδοτικής συνεργασίας των μελών μιας ομάδας είναι καταλυτικό, για την επίτευξη των στόχων που έχει θέσει. Οι μαθητές/τριες – παίκτες/κτριες κάνουν επιτυχημένα τα πρώτα προγραμματιστικά τους βήματα με τη δημιουργία ψηφιακών παιχνιδιών με σαφείς στόχους μάθησης.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] Κάτος Α.Β., Στεφανίδης Χ. Γ. (2005). Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης. Εκδόσεις Ζυγός.

[2] Pincock, S. (2006). *Κρυπτογραφία, Κώδικες και Κρυπτογράμματα*. Εκδοτικός Οίκος Τραυλός.

[3] Hankerson, O.R. (2010). *Βασικές Αρχές Θεωρίας Κωδικοποίησης και Κρυπτογραφίας*. Εκδόσεις Κλειδάριθμος.

[4] Alessi, M.S., & Trollip, S.R. (2001) *Multimedia for learning: methods and development*. Pearson.

[5] Freitas, de, S. (2007) *Learning in Immersive worlds. A review of game-based learning*. Pearson

[6] Greenfield, P.M. (1998). The Cultural Evolution of IQ. In U. Nesser (ed.), *The Rising Curve: Long Term Gains in IQ and Related Measures* (pp. 81 – 123), Washington DC, American Psychological Association.

[7] Juul, J.(2005). Half-real: *Video games between real rules and fictional worlds.* Cambridge Ma: MIT Press

[8] Rollings, A., & Adams, E. (2003). *Game Design*, McGraw-Hill.

[9] Rouse III, R. (2005). *Game Design Theory and Practice*. Plano, Texas: Wordware Publishing Inc.

[10] Prensky, M. (2003). *Digital game-based learning*. ACM Computers in Entertainment, Vol. 1, No 1, pp. 1-4.

[11] Bauer, F. L. (2002). *Decrypted Secrets*, Berlin: Springer Verlag.