Κρυπτογραφία

Εργασία εξαμήνου (1)

Εκπονήθηκε από τις:

Όλγα Βασιλείου, 01691

Χριστίνα Παναγιώτα Κομμάτα, 01637

Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική

2021-2022

Project 1 – The map

Στην παρούσα εργασία αποκρυπτογραφούμε τα τρία μηνύματα του δοθέντα χάρτη ώστε να συλλέξουμε πληροφορίες για κάποια τοποθεσία. Σύμφωνα με την εκφώνηση της εργασίας, το κάθε μήνυμα περιέχει πληροφορία που είναι απαραίτητη για τα επόμενα.

Κρυπτοκείμενο 1:

Το πρώτο κρυπτοκείμενο βρίσκεται στο κάτω μέρος του χάρτη. Εξετάζοντας τον αλγόριθμο κρυπτογράφησης του κειμένου, διαπιστώνουμε ότι πρόκειται για μονοαλφαβητική αντικατάσταση. Στην μονοαλφαβητική αντικατάσταση διατηρείται η συχνότητα εμφάνισης γραμμάτων, η οποία φαίνεται παρακάτω.

Γράμμα	Συχνότητα εμφάνισης (%)	Γράμμα	Συχνότητα εμφάνισης (%)
a	8.167	n	6.749
b	1.492	o	7.507
c	2.782	p	1.929
d	4.253	q	0.095
e	12.702	r	5.987
f	2.228	s	6.327
g	2.015	t	9.056
h	6.094	u	2.758
i	6.966	v	0.978
j	0.153	w	2.360
k	0.772	x	0.150
l	4.025	y	1.974
m	2.406	z	0.074

Εικόνα 1. Συχνότητα εμφάνισης (Διάλεξη 3: Βασικοί αλγόριθμοι)

Έπειτα από μερικές δοκιμές με βάση τις δοθείσες συχνότητες, επιτυγχάνεται η σωστή αντιστοίχιση των γραμμάτων του κρυπτοκειμένου με τα γράμματα του απλού κειμένου. Παρακάτω φαίνεται η αντιστοίχιση αυτή, καθώς και το κρυπτογραφημένο και αποκρυπτογραφημένο κείμενο.

x (σύνολο εμφάνισης: 147) = e	c (29) = f
u (113) = t	z (28) = u
d (112) = a	a (27) = p
v (108) = o	t (24) = y
k (79) = r	e (22) = v
q (73) = n	j (19) = w
r (65) = i	h (18) = g
p (64) = s	i (17) = b
m (56) = h	b (14) = k
l (47) = m	o (5) = x
g (46) = l	y (2) = z
s (44) = d	w (2) = j
n (34) = c	f (1) = q

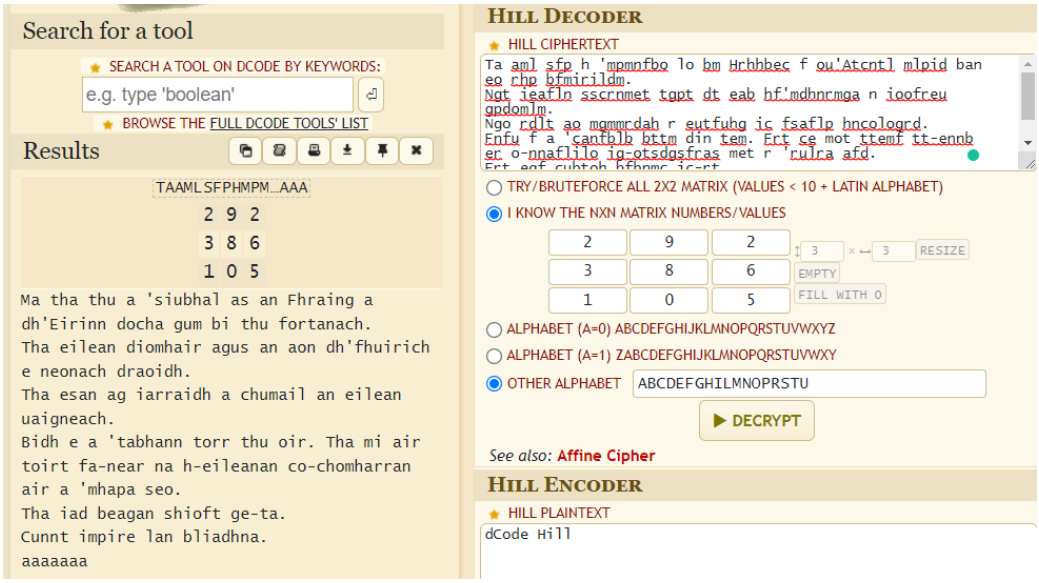
Κρυπτοκείμενο	Αποκρυπτογραφημένο κείμενο
Mxggv pukdqhxk, Jxgnvlx uv Ckd Ldzkv'p ndkuvhkdamt puzsrv du Lvqdpuxkt vc Pu. Lrnmdxg rq umx Kxazigrn vc Exqrnx. R mdex rquxkerxjxs umx lvpu cdlvzp ukdexgxkp vc lt dhx dqs R mdex nkxduxs umx ixpu ldap xexk xorpuxs. Xexktivst bqvjp umdu lt ldap dkx umx crqxpu vqxp. Auvgxlt'p qvkumxkq vkrxqudurvq rp jkvqh. Auvgxlt'p lda rp qv gvqhxk dnnzkdux. Ru mdp ixxq nkxduxs idpxs vq rqcvkldurvq sdurqh ckvl gvqh ixcvkx lznm vc umx jvkgs mds ixxq umvkvzhmgt xoagvkxs. Umx axvagx jmv ixgrxex rq d cgdu Xdkum dkx lrpudbxq. Ru svxp qvu udbx d hxqrzp uv pxx d pmra pdrg vexk umx mvkryvq vk uv gvvb svjq vq d agdrq ckvl d lvzqudrq dqs umxkxit kxdgryx umx nzkeduzkx vc umx Xdkum. Xexktivst, rq bqvjq jvkgs, ckvl Gvqsvq uv Bmdkuvzl dqs ckvl Qvzdbnmvuu uv Brxe ndq exkrct umdu lt jvkgs lda, ldaad lzqsr, rp d ldwvk ndkuvhkdamrndg jvkb umdu nvlargxp dgg umx hxvhkdamrndg bqvjgxshx vc vzk urlx. Umx Ckd Ldzkv jvkgs lda nvexkp vexk crex pfzdkx lxuxkp. Umx lda rp xoukxlxgt sxudrgxs dqs nvqudrqp ldqt umvzpdqsp vc uxoup dqs rggzpukdurvqp. Ru uvvb pxexkdg txdkp uv nvlagxux dqs rp umx lvpu sxudrgxs dqs dnnzkdux jvkgs lda umdu mdex ixxq xexk akvsznxs. Umkvzhm lt ukdexgp R mdex hdumxkxs ldqt cdpnrqdurqh irup vc rqcvkldurvq divzu d ltpuxkrvzp rpgdqs umdu xorpuxs rq pvlx ldap vc umx adpu. ...wzpu nvzqu umx ndarudgp vc bqvjq jvkgs dqs tvz jrgg mdex umx bxt uv sxnktau umx igvnbp vc umx pxnkxu lxppdhx cvzqs vq umx dknurn vnxdq...dqs ix djdkx umdu umx lxppdhx mdp ixxq jkruuxq it d Pnvurpm Nxgu ckrxqs vc lrqx	Hello stranger, Welcome to Fra Damro's cartography studio at Monastery of St. Michael in the Republic of Venice. I have interviewed the most famous travelers of my age and I have created the best maps ever existed. Everybody knows that my maps are the finest ones. Ptolemy's northern orientation is wrong. Ptolemy's map is no longer accurate. It has been created based on information dating from long before much on the world had been thoroughly explored. The people who believe in a flat Earth are mistaken. It does not take a genius to see a ship sail over the horizon or to look down on a plain from a mountain and thereby realize the curvature of the Earth. Everybody, in known world, from London to Khartoum and from Nouakchott to Kiev can verify that my world map, Mappa Mundi, is a major cartographical work that compiled all the geographical knowledge of our time. The Fra Damro world map covers over five square meters. The map is extremely detailed and contains many thousands of texts and illustrations. It took several years to complete and is the most detailed and accurate world map that have been ever produced. Through my travels I have gathered many fascinating bits of information about a mysterious island that existed in some maps of the past. ...just count the capitals of known world and you will have the key to decript the blocks of the secret message found on the arctic ocean...and be aware that the message has been written by a Scotish Celt friend of mine

Κρυπτοκείμενο 2:

Το δεύτερο κρυπτοκείμενο στο πάνω μέρος του χάρτη είναι αποτέλεσμα κρυπτογράφησης με τον αλγόριθμο Hill. Σύμφωνα με το αποκρυπτογραφημένο κείμενο 1, το κλειδί αποκρυπτογράφησης του κρυπτοκειμένου 2 είναι ένας πίνακας 3x3, με κάθε κελί να αντιστοιχεί σε πλήθος πρωτευουσών του τότε γνωστού κόσμου, όπως φαίνεται παρακάτω.

Εικόνα 2. Πίνακας-κλειδί με βάση τον χάρτη

Έχοντας στη διάθεσή μας το κλειδί, αξιοποιούμε το online εργαλείο https://www.dcode.fr/hill-cipher για την αποκρυπτογράφηση του κειμένου, χρησιμοποιώντας τον παραπάνω πίνακα-κλειδί και την κελτική αλφάβητο (ABCDEFGHILMNOPRSTU).



Εικόνα 3. Αποκρυπτογράφηση του αλγορίθμου Hill

Στη συνέχεια, χρησιμοποιούμε τη μετάφραση Google, δεδομένου ότι το κείμενο είναι σε Σκωτσέζικη γλώσσα. Το αποκρυπτογραφημένο κείμενο είναι το ακόλουθο:

If you are traveling from France to Ireland you may be lucky.

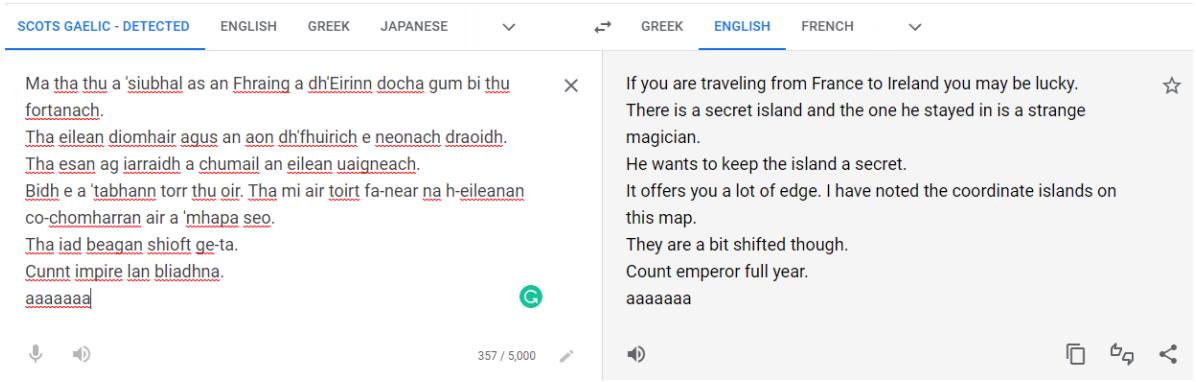
There is a secret island and the one he stayed in a strange magician.

He wants to keep the island a secret.

It offers you a lot of edge. I have noted the coordinate islands on this map.

They are a bit shifted though.

Count emperor full year.



Εικόνα 4. Google translate - τελική αποκρυπτογράφηση

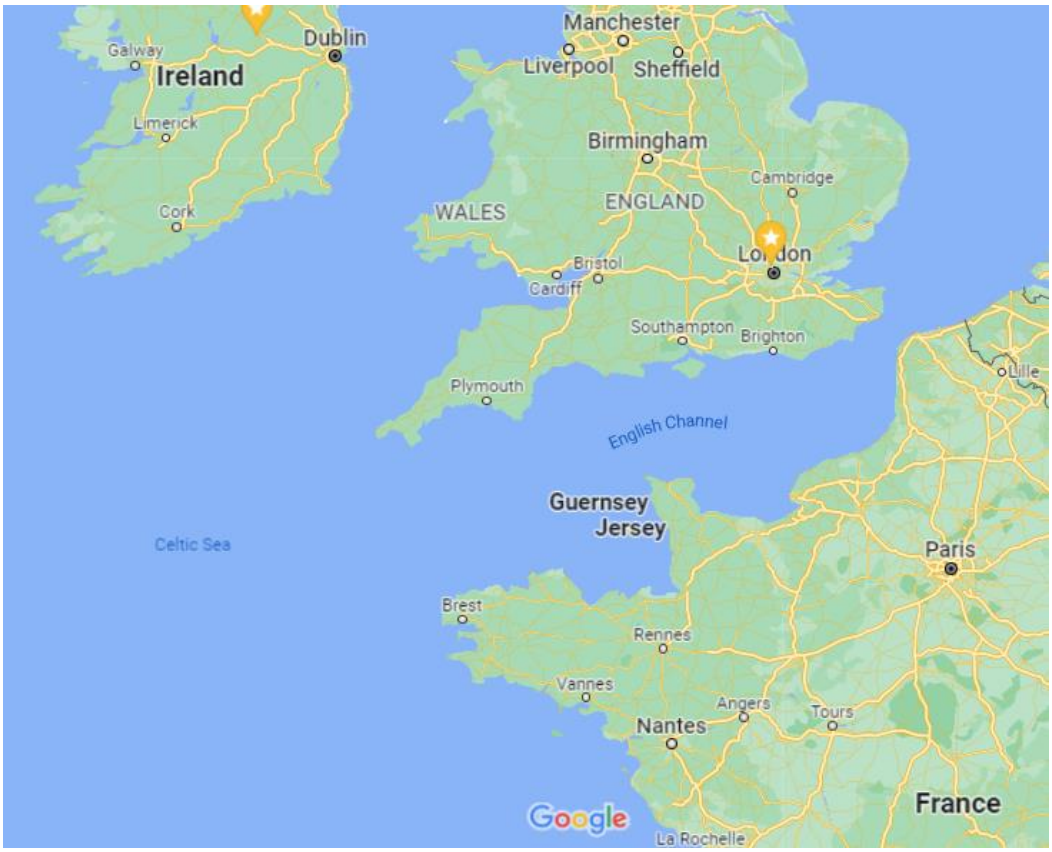
Κρυπτοκείμενο 3:

Το τρίτο και τελευταίο κείμενο έχει κρυπτογραφηθεί με τον αλγόριθμο του Καίσαρα, ο οποίος είναι αλγόριθμος μετατόπισης. Συγκεκριμένα, αφαιρούμε το κλειδί αποκρυπτογράφησης, δηλαδή την ηλικία του Ιούλιου Καίσαρα, από το κάθε στοιχείο των δοθεισών συντεταγμένων (17°0'34'' 68°2'48''). Για την εύρεση των νέων συντεταγμένων, βρίσκουμε το υπόλοιπο της διαίρεσης κάθε διαφοράς με το αντίστοιχο όριο (90° για το γεωγραφικό πλάτος, 180° για το γεωγραφικό μήκος, 60 για τα λεπτά και τα δευτερόλεπτα). Οι πράξεις φαίνονται αναλυτικά παρακάτω:

(17-55) mod 90 = -38 mod 90 = 52
(0-55) mod 60 = -55 mod 60 = 5
(34-55) mod 60 = -21 mod 60 = 39
(68-55) mod 180 = 12 mod 180 = 12
(2-55) mod 60 = -53 mod 60 = 7
(28-55) mod 60 = -27 mod 60 = 33

Η ακριβής τοποθεσία με τις παραπάνω συντεταγμένες είναι στη Γερμανία (52°5'39'' 12°7'33"). Δεδομένου, όμως, ότι το νησί που αναζητούμε βρίσκεται μεταξύ της Γαλλίας και της Ιρλανδίας, συμπεραίνουμε ότι πρόκειται για το νησί **Jersey** (49°12'34'' 2°7'30").

Εικόνα 5. Απόσταση τελικής τοποθεσίας από νησί



Εικόνα 6. Ζητούμενο νησί