

ENDY A H R O H N L S  
 T N R E Y U L D S L L S L  
 A T I H N R A R P E S L N I  
 E N R A H C T E N E U D R  
 Λ E I O Y T E Y Q H E E N  
 N A T A M A T E G Y E E  
 A R M A E E E T N E T I E

ΧΑΡΗΣ Β. ΓΕΩΡΓΙΟΥ

Ερευνητής Πληροφορικής, M.Sc., Ph.D.

# Cryptos

## Ένα γλυπτό-μνημείο για τους Κώδικες και τα μυστικά

Από τη μηχανή «Αίνιγμα» των Γερμανών κατά τον Β' Παγκόσμιο Πόλεμο, το χειρόγραφο του Βόνιτς, μέχρι τον δίσκο της Φαισιού, ανάμεσα σε ακατάληπτες επιγραφές, περιεργά γραφήματα και άγνωστα ιδεογράμματα από το παρελθόν, ένα σύγχρονο καιασκεύασμα αποτελεί έναν εξίσου προκλητικό και ανθεκτικό γρίφο. Το γλυπτό «KRYPTOS», που διακοσμεί τον προσήλιο χώρο των νέων κτιρίων της Κεντρικής Υπηρεσίας Πληροφοριών (CIA) των ΗΠΑ, εξακολουθεί να κρατά μυστικό το αληθινό περιεχόμενο του κρυπτογραφημένου μηνύματος της επιγραφής του, δύο και πλέον δεκαετίες από την καιασκευή του.

# THE ROOM

**Η** λέξη «ΚΡΥΠΤΟΣ» αποτελεί αυτούσια μεταφορά στα αγγλικά της ελληνικής λέξης «κρυπτός» με λατινικούς χαρακτήρες, δηλαδή «κρυφός, μυστικός (=εν-κρυπτός)». Στα αγγλικά υπονοεί το συνθετικό «κρυπτο-», όπως χρησιμοποιείται στις λέξεις «cryptography» (κρυπτογραφία) και «cryptosystem» (κρυπτοσύστημα).

Το όνομα «ΚΡΥΠΤΟΣ» επινοήθηκε από τον Αμερικανό καλλιτέχνη Jim Sanborn για το γλυπτό που κατασκεύασε και εγκατέστησε στο νέο κτιριακό συγκρότημα της Κεντρικής Υπηρεσίας Πληροφοριών (CIA) των ΗΠΑ τον Νοέμβριο του 1990. Κατά την κατασκευή των νέων κτιρίων, η αρμόδια υπηρεσία της CIA προκήρυξε διαγωνισμό για καλλιτεχνικά δημιουργήματα, με συνολικό προϋπολογισμό 250.000 δολάρια, με σκοπό τη διακόσμηση του περιβάλλοντος χώρου. Ο Sanborn κέρδισε τον διαγωνισμό το 1988 και δύο χρόνια αργότερα παρουσίασε τη σύνθεσή του, με κεντρικό θέμα τη συλλογή πληροφοριών. Όμως, με την πάροδο των ετών, η έμπνευσή του να αποτυπώσει σε αυτή μια σειρά κρυπτογραφημένων μηνυμάτων με άγνωστο περιεχόμενο κατέστησε το έργο του ένα μνημείο αφιερωμένο στη δύναμη του να κατέχει κάποιος ένα μυστικό, όσο σήμαντο και αν είναι.

Στην πραγματικότητα, πρόκειται για μια σύνθεση από διάφορα αντικείμενα, μεταλλικές πλάκες, κομμάτια κόκκινου και πράσινου γρανίτη, λευκό χαλαζία, μαγνητίτη και απολιθωμένους κορμούς δένδρων, διασπαρμένα στον περιβάλλοντα χώρο γύρω από τα κτίρια, με κεντρικό θέμα μια μεγάλη χάλκινη κατασκευή σε σχήμα τυλιγμένου χαρτίου εκτύπωσης. Πάνω στην κεντρική χάλκινη πλάκα που έχει διαμορφωθεί σε σχήμα «S» υπάρχει χαραγμένη μια σειρά από λατινικούς χαρακτήρες που σχηματίζουν ένα κρυπτογραφημένο κείμενο.

Το τι ακριβώς περιλαμβάνεται σε αυτό το μήνυμα-γράφο αποτελεί ακόμα και σήμερα ένα μυστήριο και μια άσκηση για τους ικανότερους αναλυτές της CIA, που το αντικρίζουν καθημερινά στον υπαίθριο χώρο έξω από την κεντρική καφετέρια των γραφείων. Ο Sanborn αποκάλυψε πως για να διατηρηθεί το μυστήριο μέχρι την επίσημη παρουσίαση, η κατασκευή του γλυπτού έγινε κυρίως κατά τις θραβινές ώρες.

Το κρυπτογράμμα που απεικονίζεται στην κεντρική κατασκευή του γλυπτού αποτελείται στην πραγματικότητα από δύο

τμήματα. Στο αριστερό μισό καταγράφεται ένα ενιαίο σύνολο από 869 λατινικούς χαρακτήρες, 865 κανονικούς και 4 ερωτηματικά, το οποίο αποτελεί το κρυπτογραφημένο μήνυμα καθαυτό. Στο δεξιό μισό υπάρχει ένας πίνακας χαρακτήρων, με συγκεκριμένη διάταξη και παρουσίαση, ο οποίος αποτελεί τη βάση της μεθόδου που χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση του αριστερού μισού του γλυπτού. Για να χρησιμοποιηθεί σωστά ο πίνακας των χαρακτήρων απαιτούνται μία ή δύο λέξεις-κλειδιά, βάσει των οποίων εφαρμόζονται συγκεκριμένες αναδιτάξεις και στοιχίσεις των σειρών των χαρακτήρων, ώστε η αποκρυπτογράφηση να γίνει σωστά.

Για τη σχεδίαση του γλυπτού «ΚΡΥΠΤΟΣ» και την επιλογή των κατάλληλων κρυπτογραφικών μεθόδων, ο Jim Sanborn συνεργάστηκε στενά με τον Ed Scheidt, συνταξιούχο υπάλληλο της CIA και τότε πρόεδρο του Κρυπτογραφικού Κέντρου της υπηρεσίας. Με τη βοήθειά του, ο Sanborn σχεδίασε ένα κρυπτογράμμα που αποτελείται από τέσσερα επιμέρους τμήματα, όπως αποκαλύφθηκε μετά τις πρώτες προσπάθειες κρυπτανάλυσης του γλυπτού και την αποκρυπτογράφηση του





Η κύρια κατασκευή του γλυπτού «KRYPTOS», στον προούλιο χώρο των νέων κτιρίων της CIA στο Langley της Virginia στις ΗΠΑ. Στη βάση της κατασκευής διακρίνεται το κυκλικό σπινθίρι και τα κομμάτια μαγνητίτη και γρανίτη που το συνοδεύουν.

μηνύματος του πρώτου τμήματος. Συγκεκριμένα, τα κρυπτογράμματα στο πρώτο και στο δεύτερο τμήμα βασίζονται σε μια πολυαλφαριθμητική μέθοδο αντικατάστασης ή αλλιώς «πίνακα κρυπτογράφησης», η οποία αποτελεί παραλλαγή μιας αρκετά παλιάς και πολύ γνωστής μεθόδου με το όνομα Βιζενέρ.

Κώδικες αυτού του τύπου είναι εξαιρετικά δύσκολο να παραβιαστούν χωρίς τη χρήση ηλεκτρονικού υπολογιστή και εξειδικευμένων προγραμμάτων. Αν χρησιμοποιηθούν λέξεις-κλειδιά μεγαλύτερα της μιας λέξης (μερικών χαρακτήρων).

Στην περίπτωση του γλυπτού «KRYPTOS», ο δημιουργός του φρόντισε να παράσχει τον βασικό πίνακα κρυπτο-

γράφησης, στο δεξιό τμήμα της κεντρικής κατασκευής, δίνοντας μάλιστα και τη μια από τις δύο λέξεις-κλειδιά, που δεν είναι τίποτα άλλο παρά το ίδιο το όνομα του γλυπτού («KRYPTOS»). Το κρυπτόγραμμα στο τρίτο τμήμα έχει κατασκευαστεί με μια διαφορετική, απλούστερη μέθοδο κρυπτογράφησης, συγκεκριμένα μιας απλής αντικατάστασης με μετὰ-θέση-αναδιάταξη σειρών και στηλών. Το τέταρτο τμήμα, μήκους μόλις 97 χαρακτήρων, παραμένει ακόμα και σήμερα απαράβιαστο, παρά τις επίμονες προσπάθειες εκατοντόνων ανθρώπων, ειδικών και μη με την κρυπτογραφία.

Μέρος των λέξεων-κλειδίων που χρησιμοποιούνται για την αποκρυπτογράφη-

ση του γλυπτού εμφανίζονται με τη μορφή έμμεσων υποδείξεων, παρατηρήσεων, ακόμα και χαραγμένων μνημάτων σε μορφή κώδικα Μορς, στα αντικείμενα που είναι διάσπαρτα σε κάποια απόσταση από την κεντρική κατασκευή. Παρόλα αυτά, ελάχιστα είναι πλέον τα στοιχεία που μπορούν να εσυχθούν για το περιεχόμενο του τέταρτου κρυπτογράμματος, το οποίο εξακολουθεί να αποτελεί ιδιαίτερα δύσκολο γρίφο, δύο δεκαετίες και πλέον από την κατασκευή του.



## ΕΝΑ ΜΥΣΤΙΚΟ ΜΕ ΜΕΓΑΛΗ ΙΣΤΟΡΙΑ

Από την ημέρα της επίσημης παρουσίασης του γλυπτού στις 3 Νοεμβρίου του 1990, τα κρυπτογράμματα του «KRYPTOS» έχουν μελετηθεί και αναλυθεί από χιλιάδες ανθρώπους, επιστήμονες αλλά και απλούς ανθρώπους, που προσπάθησαν να αποκαλύψουν τα μυστικά μηνύματα που κρύβονται κάτω από τα ατελείωτα σύμβολα και γράμματα της κεντρικής επιγραφής.

Ο Scheidt, μέντορας του Sanborn στην τέχνη των κωδικών και της παραδοσιακής κρυπτογραφίας, σε συνέντευξή του πριν μερικά χρόνια ανέφερε πως όταν συνεργάστηκε με τον καλλιτέχνη ένωσε πως έπρεπε να ισορροπήσει μεταξύ δύο άκρων. Να τον βοηθήσει να κατασκευάσει κάτι ενδιαφέρον, όχι υπερβολικά δύσκολο να «απάνει» από κάποιον ερασιτέχνη κρυπτανάλυτη, αλλά ούτε και υπερβολικά εύκολο που θα αποκάλυπτε το μυστικό μέσο σε λίγες μόνο μέρες. Ταυτόχρονα, όμως, δεν ήθελε με κανένα τρόπο να αποκάλυψει στον Sanborn ο,τιδήποτε σχετικά με το τι συμβαίνει και πώς πραγματικά λειτουργεί σήμερα η υπηρεσία (CIA). Σύμφωνα με τη δική του αρχική εκτίμηση για το γλυπτό, τα πρώτα τρία κρυπτογράμματα ήταν σχεδιασμένα έτσι, ώστε να «σπάσουν» ύστερα από προσπάθειες μερικών εβδομάδων ή μηνών, ενώ το τέταρτο και πιο δύσκολο κρυπτόγραμμα, καθώς και ολόκληρος ο «γρίφος»

**Η πρώτη επίσημη ανακοίνωση της αποκρυπτογράφησης των τριών πρώτων μηνυμάτων του γλυπτού πραγματοποιήθηκε το 1999 από τον James Gillogly, Αμερικανό επιστήμονα πληροφορικής από τη νότια Καλιφόρνια.**



του γλυπτού σε διάστημα όχι μεγαλύτερο από επτά χρόνια. Εκ του αποτελέσματος, αποδείχθηκε ότι οι εκτιμήσεις του ήταν υπερβολικά αισιόδοξες.

Η πρώτη επίσημη ανακοίνωση της αποκρυπτογράφησης των τριών πρώτων μηνυμάτων του γλυπτού πραγματοποιήθηκε το 1999 από τον James Gillogly, Αμερικανό επιστήμονα πληροφορικής από τη νότια Καλιφόρνια. Για την αποκρυπτογράφηση ο Gillogly χρησιμοποίησε ένα τυπικό ηλεκτρονικό υπολογιστή της εποχής με επεξεργα-

ματα του «KRYPTOS» ήδη από το 1992, χρησιμοποιώντας έναν ηλεκτρονικό υπολογιστή.

Αν και οι τρεις ανακοινώσεις θεωρούνται ισοδύναμες ως προς το περιεχόμενο, καθώς αποκάλυπταν την ίδια λύση για τα αποκρυπτογραφημένα μηνύματα στα τρία πρώτα τμήματα, ωστόσο μόνο η επίλυση του Gillogly ανακοινώθηκε δημόσια εξ' αρχής και έδωσε άμεσα τη δυνατότητα ανεξάρτητης επιβεβαίωσης. Έτσι, η κοινότητα των ερασιτεχνών κρυπταναλυτών και φα-

ποτε ιδέα, από πολύπλοκα μαθηματικά μέχρι αστρολογία, με περίπου 130 αναρτήσεις νέων μηνυμάτων κάθε μήνα. Ο Sanborn ανακοίνωσε στην ομάδα πως η λύση που είχε γίνει αποδεκτή ως σωστή για το κρυπτογράμμα του δεύτερου τμήματος ήταν στην πραγματικότητα λάθος, καθώς από δικό του σφάλμα είχε παραλείψει για αισθητικούς λόγους ένα «X» προς το τέλος του κρυπτογραφημένου κειμένου. Το αποτέλεσμα ήταν το αποκρυπτογραφημένο μήνυμα να τελειώνει: «...FORTY FOUR SECONDS

στη Pentium II και κατάλληλα προγράμματα λογισμικού που δημιούργησε ο ίδιος.

Αμέσως μετά την ανακοίνωση του Gillogly, η CIA αποκάλυψε ότι ένας δικός της αναλυτής με το όνομα David Stein είχε επίσης «παράσει» τα τρία πρώτα κρυπτογράμματα (K1, K2 και K3 όπως αναφέρονται) λίγο καιρό πριν, το 1998. Σύμφωνα με την ανακοίνωση της CIA, για την επίλυση ο Stein είχε χρησιμοποιήσει μόνο χαρτί και μολύβι και είχε αφιερώσει περίπου 400 ώρες εκτός της κανονικής εργασίας του. Η ανακοίνωση της λύσης, καθώς και λεπτομέρειες της μεθοδολογίας που ακολούθησε, είχε παρουσιάσει ο ίδιος σε αμφιθέατρο της CIA τον Φεβρουάριο του 1998, όμως η συγκεκριμένη εκδήλωση παρέμεινε μυστική μέχρι την επίσημη ανακοίνωση της υπηρεσίας, ένα χρόνο αργότερα.

Σχεδόν ταυτόχρονα με την ανακοίνωση της CIA, μια άλλη υπηρεσία πληροφοριών των ΗΠΑ, η NSA/CSS (National Security Agency/Central Security Service - Εθνική/Κεντρική Υπηρεσία Ασφαλείας), εξέδωσε τη δική της σχετική ανακοίνωση, σύμφωνα με την οποία αναλυτές της είχαν καταφέρει να «παράσουν» τους κώδικες των κρυπτογραμμάτων K1, K2 και K3, όμως δεν αποκάλυψε τα ονόματά τους εκείνη τη στιγμή. Αρκετά αργότερα, το 2005, ανακοίνωσε ότι στην εν λόγω ομάδα επικεφαλής ήταν ο Kan Miller, ενώ συμμετείχαν ο Dennis McDaniels και δύο ακόμη αναλυτές, οι οποίοι παρέμειναν ανώνυμοι. Η ομάδα της NSA είχε καταφέρει να αποκρυπτογραφήσει τα τρία πρώτα τμή-

ματικών του «KRYPTOS» τη θεωρούν ως την πρώτη «δημόσια» επίλυση των κρυπτογραμμάτων. Η επίλυση του Stein της CIA θεωρείται επίσης επιβεβαιωμένη σύμφωνα με το υλικό που δημοσιεύτηκε μαζί με την ανακοίνωση της υπηρεσίας. Δεν συμβαίνει όμως το ίδιο και για την επίλυση της ομάδας της NSA, της οποίας η εγκυρότητα βασίζεται κυρίως σε ένα και μοναδικό σχετικό δημοσίευμα στο «Sun Journal» το 2000, δηλαδή δύο χρόνια μετά τη δημοσίευση της επίλυσης του Stein.

Παρόλο που και οι τρεις αυτές ανακοινώσεις ουσιαστικά θεωρούνται ταυτόσημες, περιείχαν ένα βασικό σφάλμα. Συγκεκριμένα, στις 10 Οκτωβρίου του 2005 η Monei Freidrich, Καναδή μηχανικός ηλεκτρονικών υπολογιστών από το Βανκούβερ, ανακοίνωσε τη δική της επίλυση. Στο δεύτερο κρυπτογράμμα, το δικό της αποκρυπτογραφημένο μήνυμα τελειώνει με τους χαρακτήρες «...WESTXLAYERTWO», αντί «...WESTIDBYROWS» που ανέφεραν οι προηγούμενες λύσεις. Πράγματι, στις 19 Απριλίου του 2006, δηλαδή έξι μήνες μετά την ανακοίνωση της Freidrich, ο Sanborn επικοινωνήσε με την ομάδα Kryptos, μια διαδικτυακή κοινότητα στο «Yahoo! Groups» που ασχολείται με την αποκρυπτογράφηση του γλυπτού και ανακοινώνει δημόσια τις πιθανές λύσεις. Η συγκεκριμένη ομάδα δημιουργήθηκε τον Μάιο του 2003 και τα σχεδόν 2.500 μέλη της ασχολούνται φανατικά με τη μελέτη και την ανάλυση της ομώνυμης κατασκευής, δοκιμάζοντας οποιαδή-

WEST ID BY ROWS», ενώ στο σωστό είναι «...FORTY FOUR SECONDS WEST X LAYER TWO». Η ανακοίνωση του σφάλματος από τον Sanborn ουσιαστικά επιβεβαίωσε τη μοναδική, τελικά, εξ' ολοκλήρου ορθή επίλυση του κρυπτογράμματος K2.

Μολονότι ο Sanborn εργάστηκε στενά με τον Scheidt στα αρχικά στάδια της σχεδίασης των κρυπτογραμμάτων, ο καλλιτέχνης αποκάλυψε σε συνέντευξή του ότι η τελική μορφή των μεθόδων και τα ίδια τα μηνύματα κρυπτογραφήθηκαν από τον ίδιο - ο Scheidt δεν μπορεί να γνωρίζει το περιεχόμενό τους γιατί απλά δεν τα έχει δει πο-





τέ. Μάλιστα, σύμφωνα με τον Sanborn, ούτε καν ο τότε διευθυντής της CIA William Webster δεν γνωρίζει την πλήρη απάντηση. Όπως είπε μάλιστα, ειδικά για το τέταρτο τμήμα που παραμένει ακόμα και σήμερα α-παρβασίσο, κάποια στιγμή θα αποκρυπτο-

θώς δεν έχει καμία απολύτως σχέση με τις εικασίες και τη μυθοπλασία που παρουσιάζει ο Dan Brown στα διβλία του.

## Η ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ ΤΩΝ ΜΗΝΥΜΑΤΩΝ ΣΤΑ ΤΜΗΜΑΤΑ Κ1, Κ2 ΚΑΙ Κ3

Το περιεχόμενο των τριών πρώτων κρυπτογραμμάτων, που αποκαλύφθηκε σχεδόν μια δεκαετία από τη δημιουργία του «ΚΡΥΠΤΟΣ», αποτελεί ένα μίγμα σχεδόν ποιητικών αφηγήσεων, κατασκευάσι-μου του καλλιτέχνη, ο οποίος θέλησε να προσδώσει ένα μυστικιστικό χαρακτήρα στο έργο του.

στο προς το παρόν, με το τέταρτο τμήμα και την αποκρυπτογράφησή του.

## Δεύτερο Τμήμα (Κ2)

«IT WAS TOTALLY INVISIBLE HOWS THAT POSSIBLE ? THEY USED THE EARTHS MAGNETIC FIELD X THE INFORMATION WAS GATHERED AND TRANSMITTED UNDERGRUUND TO AN UNKNOWN LOCATION X DOES LANGLEY KNOW ABOUT THIS ? THEY SHOULD ITS BURIED OUT THERE SOMEWHERE X WHO KNOWS THE EXACT LOCATION ? ONLY WW THIS WAS HIS LAST MESSAGE X THIRTY EIGHT DEGREES FIFTY SEVEN

**Οι παγοκρύσταλλοι αντιμετώπιστηκαν για πρώτη φορά με επιστημονικό τρόπο το 1611 από τον Johannes Kepler ο οποίος προσπάθησε να απαντήσει στο ερώτημα γιατί οι παγοκρύσταλλοι εμφανίζουν πάντα συμμετρία 6ης τάξης.**



γραφηθεί και θα μπορούσαν να το διαβάσουν, αλλά δεν είναι σίγουρο πως θα το κατανοήσουν. Το περιεχόμενο είναι πολύ ασαφές και ένα ακόμα αίνιγμα από μόνο του, ή όπως ανέφερε χαρακτηριστικά, είναι ένας «γρίφος μέσα στον γρίφο».

Ο πολύ γνωστός συγγραφέας μυθιστορημάτων Dan Brown είναι ένας από τους φανατικούς θαυμαστές του γλυπτού «ΚΡΥΠΤΟΣ», το οποίο έχει αναφέρει, τόσο με έμμεσο όσο και με άμεσο τρόπο, σε δύο από τα πιο επιτυχημένα έργα του. Συγκεκριμένα, στο διβλίο του «Κώδικας Ντα Βίντσι» υπάρχουν δύο αναφορές, στο χάρτινο εξώφυλλο της αμερικανικής έκδοσης: Η πρώτη είναι οι συντεταγμένες του γεωγραφικού σημείου (σε αντεστραμμένη γραφή, με «27» αντί «28» στο γεωγραφικό πλάτος) που αναφέρεται στο μήνυμα του κρυπτογράμματος Κ2, ενώ η δεύτερη είναι η φράση «μόνο ο W.W. γνωρίζει», που αναφέρεται στο αντίστοιχο απόσπασμα στο ίδιο μήνυμα. Στο εξώφυλλο της κεντρικής υπόθεσης του έργου του. Αυτό κατά τον Sanborn αποτελεί σημαντική «παράνοση» ως προς την ιδέα που παρουσιάζει το γλυπτό του, κα-

Επειδή δεν υπάρχουν συγκεκριμένα σύμβολα αρχής και τέλους του κάθε τμήματος, τα όρια των κρυπτογραμμάτων αποκαλύφθηκαν μετά από ενδελεχή και επίπονη κρυπτανάλυση, φέρνοντας στο φως κάθε φορά όλο και μεγαλύτερα αναγνώσιμα μηνύματα εκεί που πριν υπήρχαν μόνο σειρές ακατανόητων λατινικών χαρακτήρων.

## Πρώτο Τμήμα (Κ1)

«BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF IQLUSION»

### Μετάφραση

«Μεταξύ της ανεπισημάντης σκίασης και της απουσίας φωτός βρίσκεται η λεπτή διαφορά της παραίτησης/οφθαλμαπάτης».

Η λέξη «IQLUSION» έχει αποκρυπτογραφηθεί ακριβώς έτσι, δηλαδή με το γράμμα «Q» αντί του «L» που θα έδινε τη σωστή λέξη «ILLUSION». Ο δημιουργός του «ΚΡΥΠΤΟΣ» έχει επιβεβαιώσει ότι αυτή είναι όντως η σωστή μετάφραση, καθώς και ότι τέτοια «σφάλματα» στα αρχικά μηνύματα είναι εσκεμμένα, υπονοώντας ότι συνδέονται με κάποιο τρόπο, άγνω-

MINUTES SIX POINT FIVE SECONDS NORTH SEVENTY SEVEN DEGREES EIGHT MINUTES FORTY FOUR SECONDS WEST X LAYER TWO»

### Μετάφραση

«Ήταν εντελώς αόρατο, πως (είναι) ήταν δυνατόν; Χρησιμοποίησαν το μαγνητικό πεδίο της Γης (X) Η πληροφορία(ες) συλλέχθηκαν και μεταδόθηκαν υπογειως προς μια άγνωστη τοποθεσία (X) Το Langley το γνωρίζει αυτό; Θα πρέπει (να το γνωρίζει), είναι θαμμένο κάπου εκεί έξω (X) Ποιος γνωρίζει την ακριβή τοποθεσία; Μόνο ο W.W. Αυτό ήταν το τελευταίο του μήνυμα (X) 28° 57' 6.5" Β / 77° 6' 44" Δ (X) Επίπεδο δύο».

Όπως και στο πρώτο κρυπτόγραμμα του γλυπτού, έτσι και εδώ, υπάρχει ένα ορθογραφικό σφάλμα στη λέξη «UNDERGRUUND», αντί για «UNDERGROUND», που κατά τον Sanborn είναι επίσης εσκεμμένο και πιθανότατα συνδέεται με την αποκρυπτογράφηση του τέταρτου τμήματος.

Η αναφορά στον «W.W.» θεωρείται σχεδόν σίγουρο πως συνδέεται με τον William Webster, διευθυντή της CIA τον Νοέμβριο 1990, όταν το γλυπτό τοποθετήθηκε εκεί, στον προαύλιο χώρο των κεντρικών κτιρίων στο Langley της Virginia

otics ΗΠΑ. Η συγκεκριμένη αναφορά στο μήνυμα συνδέεται με την επιθεώρηση από τον Sanborn ότι, μαζί με την τοποθέτηση του γλυπτού, παρέδωσε στον διευθυντή Webster ένα φάκελο με την πλήρη λύση και των τεσσάρων κρυπτογραμμάτων που παρουσιάζονταν σε αυτό, χωρίς όμως, όπως είπε, να του αποκαλύψει ολόκληρο τον «γρίφο».

Η γεωγραφική τοποθεσία που αναφέρεται στο τελευταίο τμήμα του μηνύματος είναι στην πραγματικότητα ένα σημείο περίπου 50 μέτρα νοτιοανατολικά του γλυπτού, όπου όμως δεν φαίνεται να υπάρχει τίποτα σημαντικό. Σε συνέντευξη που έδωσε το 2005, ο Sanborn ανέφερε

ούργησα ένα μικροσκοπικό άνοιγμα στην πάνω αριστερή γωνία και μετά, διευρύνοντας λίγο την τρύπα, έβαλα μέσα το κέρι και καίταξα μέσα. Ο ζεστός αέρας που εξερχόταν από την οίθουσα έκανε τη φλόγα να τρεμοπαιζει, αλλά εκείνη τη στιγμή λεπτομέρειες από το δωμάτιο στο εσωτερικό εμφανίστηκαν μέσα από την ομίχλη (X) Μπορείτε να διακρίνετε τίποτα (Q);

Όπως και στα δύο προηγούμενα κρυπτογράμματα, εδώ το «εσκεμμένο» ορθογραφικό σφάλμα είναι στη λέξη «DESPARATELY» αντί για «DESPERATELY» που είναι το σωστό. Αξίζει θύβια να σημειωθεί ότι αν αντί της αλλαγής του γράμματος «Α» σε «Ε» διορθωθεί το γράμμα «Ε»

σε «Ι», δημιουργείται η λέξη «DISPARATELY» που σημαίνει «αταίριαστος» ή «ανόμοιος», ένα προφανές λογοπαίγνιο του δημιουργού σχετικά με αυτά τα «τυχαία» ορθογραφικά σφάλματα. Πολλοί μάλιστα το θεωρούν ως σαφή επιθεώρηση πως αυτά τα ορθογραφικά λάθη έχουν έντονη εξαιρετική σημασία για την πλήρη αποκρυπτογράφηση του γλυπτού, ιδιαίτερα του τέταρτου κρυπτογράμματος που παραμένει ακόμα και σήμερα απαράσιτο.

Το συγκεκριμένο μήνυμα στο τρίτο τμήμα αποτελεί παράφραση ενός αποσπάσματος από το βιβλίο του H. Carter «Ο τάφος του Τουταγχαμών» (1923), του Βρετανού αρχαιολόγου και αιγυπτολόγου που

# HENDYAHROHATYEU

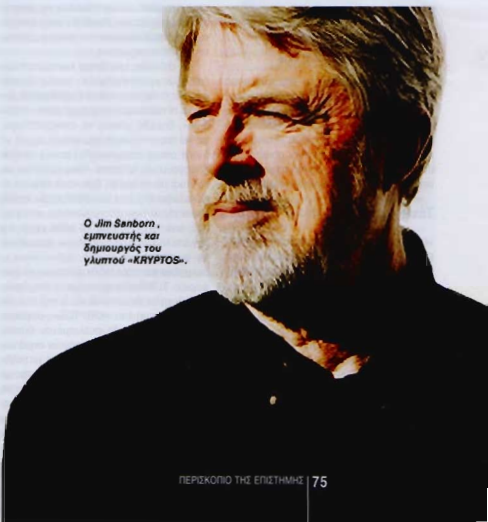
πως το συγκεκριμένο σημείο αφορά κάτι που «έγινε εκεί» ή που «έκανε ο ίδιος» όταν θρικόταν στον χώρο κατά την κατασκευή του «KRYPTOS», αρνήθηκε όμως να επιθεωρήσει ή να διαψεύσει αν πρόκειται για κάτι που έχει τοποθετήσει ή θάψει εκεί.

## Τρίτο Τμήμα (K3)

«SLOWLY DESPARATLY SLOWLY THE REMAINS OF PASSAGE DEBRIS THAT ENCUMBERED THE LOWER PART OF THE DOORWAY WAS REMOVED WITH TREMBLING HANDS I MADE A TINY BREACH IN THE UPPER LEFT HAND CORNER AND THEN WIDENING THE HOLE A LITTLE I INSERTED THE CANDLE AND PEERED IN THE HOT AIR ESCAPING FROM THE CHAMBER CAUSED THE FLAME TO FLICKER BUT PRESENTLY DETAILS OF THE ROOM WITHIN EMERGED FROM THE MIST X CAN YOU SEE ANYTHING Q ?»

### Μετάφραση

«Αργά, (απελπιστικά) αργά, τα υπολείμματα των ερειπίων του περάσματος, που εμπόδιζαν το κάτω μέρος της εισόδου, απομακρύνθηκαν. Με τρεμάμενα χέρια δημι-



Ο Jim Sanborn, εμπνεστής και δημιουργός του γλυπτού «KRYPTOS».





## ΜΕΘΟΔΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ - ΠΙΝΑΚΕΣ ΒΙΖΕΝΕΡ

από την κανονική τους θέση και τοποθετώντας τα στην αρχή. Η υπόλοιπη σειρά συμπληρώνεται με την κανονική διαδοχή των υπόλοιπων γραμμικών. Έτσι, η τελική «τροποποιημένη» σειρά των 26 λατινικών χαρακτήρων είναι αυτή που απεικονίζεται της δεύτερης σειρά του δεξιού τμήματος του γλυπτού (η πρώτη χρησιμοποιείται μόνο για αναφορά), με επιπλέον επανάληψη των πρώτων τεσσάρων γραμμικών από την αρχή, ώστε να εμφανίζεται τελικά μια πλήρης σειρά 30 χαρακτήρων στο γλυπτό:

KRYPTOSABCDEFGHIJLMNQUVWXZKRYPT

Στη συνέχεια, η ίδια τροποποιημένη σειρά των 26 λατινικών χαρακτήρων επαναλαμβάνεται ακριβώς 26 φορές, ή μία κάθε από την άλλη, όσα και τα γράμματα του λατινικού αλφαβήτου. Στο δεξιό μισό του γλυπτού «KRYPTOS» αυτά διακρίνονται με σαφήνεια, με τη στήλη αναφοράς των 26 λατινικών χαρακτήρων και ακριβώς δίπλα μια σειρά των 26 (30) χαρακτήρων για κάθε ένα από αυτά. Φαίνεται επίσης ότι σε κάθε επόμενη σειρά, οι χαρακτήρες εμφανίζονται «μεταποιοιούνται» κατά μία θέση αριστερά. Αυτή ακριβώς είναι η μορφή που χρησιμοποιείται στην απλή μέθοδο Βιζενέρ, δηλαδή με μία και μόνο λέξη-κλειδί («KRYPTOS»). Στη συγκεκριμένη περίπτωση, η παραλλαγή Κουαγκάμ-3 χρησιμοποιεί και μια δεύτερη λέξη-κλειδί, η οποία εφαρμόζεται κάθετα, για να καθορίσει πώς ακριβώς θα πραγματοποιηθεί η στήλη των σειρών των 26 χαρακτήρων.

Όσο το πρώτο, όσο και το δεύτερο κρυπτόγραμμα στο γλυπτό «KRYPTOS», βασίζονται ακριβώς στη μέθοδο κρυπτογράφησης Κουαγκάμ-3, με πρώτη λέξη-κλειδί και στις δύο περιπτώσεις την «KRYPTOS», αλλά διαφορετική δεύτερη λέξη-κλειδί. Για το πρώτο τμήμα, η δεύτερη λέξη-κλειδί είναι η «PALIMPSEST» («πάλιψηστο»), ενώ για το δεύτερο τμήμα η δεύτερη λέξη-κλειδί είναι η «ABSCSSA» («τετηγμένη»). Τοποθετώντας κάθε φορά τη συγκεκριμένη δεύτερη λέξη-κλειδί κάθετα, η σειρά των 26 λατινικών χαρακτήρων μετατοπίζεται προς τα αριστερά, «ολοφαινονο» για όσες θέσεις απαιτείται, ώστε η λέξη-κλειδί να σχηματιστεί κάθετα στο αριστερό μέρος του πίνακα. Τέλος, το τμήμα που «κλεινόμε» από τα αριστερά μεταφέρεται στο τέλος της σειράς στα δεξιά, ώστε να σχηματιστεί ο τελικός πίνακας πολυαλφαβητικής αντικατάστασης. Στον νέο αυτό πίνακα, η πρώτη κάθετη στήλη περιλαμβάνει ακριβώς τη συγκεκριμένη (δευτέρα) λέξη-κλειδί.

Πρακτικά, η παραπάνω διαδικασία διαφέρει από την απλή μέθοδο των πινάκων Βιζενέρ μόνο στο ότι χρησιμοποιεί δύο λέξεις-κλειδιά αντί για ένα: Το πρώτο για την αναδιάταξη της κανονικής σειράς των 26 χαρακτήρων του λατινικού αλφαβήτου, ενώ το δεύτερο για την οριζόντια «ολίσθηση» και μερική αναδιάταξη των χαρακτήρων σε κάθε σειρά, σύμφωνα με μια συγκεκριμένη «ευθυγράμμιση» στην πρώτη στήλη, η οποία προκύπτει ακριβώς από τη δεύτερη λέξη-κλειδί. Ο παρακάτω πίνακας αντικατάστασης παρουσιάζει την τελική του μορφή, όπως ακριβώς εφαρμόζεται για το πρώτο κρυπτόγραμμα K1 του γλυπτού «KRYPTOS», χρησιμοποιώντας ως πρώτη λέξη-κλειδί την «KRYPTOS» και ως δεύτερη λέξη-κλειδί την «PALIMPSEST» (κάθετα, στην πρώτη στήλη). Η πρώτη σειρά χρησιμοποιείται ως αναφορά, ενώ ο τελικός πίνακας αντικατάστασης εμφανίζεται στις δέκα αριθμημένες σειρές ακριβώς από κάτω, από «0» έως «9», όσα και τα γράμματα της δεύτερης λέξης-κλειδί:

KRYPTOSABCDEFGHIJLMNQUVWXZKRYPT  
0 P T O S A B C D E F G H I J L M N Q U V W X Z K R Y  
1 A B C D E F G H I J L M N Q U V W X Z K R Y P T O S  
2 L M N Q U V W X Z K R Y P T O S A B C D E F G H I J  
3 I J L M N Q U V W X Z K R Y P T O S A B C D E F G H  
4 M N Q U V W X Z K R Y P T O S A B C D E F G H I J L  
5 P T O S A B C D E F G H I J L M N Q U V W X Z K R Y  
6 S A B C D E F G H I J L M N Q U V W X Z K R Y P T O  
7 E F G H I J L M N Q U V W X Z K R Y P T O S A B C D  
8 S A B C D E F G H I J L M N Q U V W X Z K R Y P T O  
9 T O S A B C D E F G H I J L M N Q U V W X Z K R Y P

Σύμφωνα με τη μέθοδο Βιζενέρ, για την αποκρυπτογράφηση του πρώτου κρυπτογράφματος του γλυπτού «KRYPTOS» η διαδικασία είναι πλέον πολύ απλή: Το πρώτο γράμμα του κρυπτογράφματος έχει θέση αναφοράς «0», δηλαδή την πρώτη θέση στον πίνακα. Σε αυτή τη σειρά εντοπίζεται το συγκεκριμένο «κρυπτογραφημένο» γράμμα, που είναι το «E». Ακολουθώντας τη συγκεκριμένη στήλη προς τα πάνω, εντοπίζεται στη σειρά αναφοράς το αντίστοιχο «αποκρυπτογραφημένο» γράμμα, που είναι το «B». Το ίδιο ακριβώς εφαρμόζεται για κάθε επόμενο γράμμα του κρυπτογραφημένου μηνύματος, αντικαθιστώντας τα διαδοχικά με το αντίστοιχο γράμμα στη σειρά αναφοράς. Έτσι, τα πρώτα επτά γράμματα «EMUJPHZ» του πρώτου κρυπτογράφματος του γλυπτού μετατρέπονται αντίστοιχα σε «BETWEEN»:  
Αριθμός θέσης:  
012345678901234567890...  
012345678901234567890...

Κρυπτόγραμμα:  
EMUJPHZRFAXYUSDIKJZLDRKNSHGNI...  
Μήνυμα:  
BETWEENSUBTLESHADINGANDTHEABSE...

Αξιζει να σημειωθεί πως στη λέξη «BETWEEN» ο λατινικός χαρακτήρας «E» εμφανίζεται ήδη τρεις φορές, κάτι αναμενόμενο, αφού αποτελεί το γράμμα με τη μεγαλύτερη συχνότητα εμφάνισης στην αγγλική γλώσσα. Σε μια απλή μέθοδο αντικατάστασης, όπως αυτή του Κάισαου, κάθε γράμμα στο αρχικό μήνυμα αντικαθίσταται πάντα με το ίδιο γράμμα στο κρυπτογραφημένο μήνυμα. Αυτό σημαίνει ότι, αν μια τέτοια μέθοδος εφαρμόζονταν στη συγκεκριμένη περίπτωση, οι πρώτες επτά χαρακτήρες στο κρυπτόγραμμα θα περιλάμβαναν αντίστοιχα τρεις φορές κάποιο λατινικό γράμμα αντί του «E» και μάλιστα σε δύο διαδοχικές θέσεις. Το γεγονός της μεγάλης συχνότητας εμφάνισης, καθώς και της διαδοχικής εμφάνισης δύο φορές, θα έκανε πολύ εύκολο τον συσχετισμό του συγκεκριμένου «κρυπτογραφημένου» χαρακτήρα με το γράμμα «E», αν ήταν γνωστό ότι το μήνυμα είναι γραμμένο στην αγγλική γλώσσα. Η αποκάλυψη ενός και μόνο τέτοιου χαρακτήρα με υψηλή συχνότητα εμφάνισης σε ένα κρυπτόγραμμα θα ήταν ίσως αρκετή για τη σταδιακή αποκάλυψη του κλειδιού και του υπόλοιπου κρυπτογραφημένου μηνύματος. Παρόλα αυτά, με την παραπάνω πολυαλφαβητική μέθοδο τύπου Βιζενέρ, είναι φανερό ότι ο χαρακτήρας «E» κρυπτογραφείται τρεις φορές με διαφορετικό γράμμα, με αποτέλεσμα το κρυπτόγραμμα «EMUJPHZ...» να μη προσομοιάζει σε τίποτα με τη λέξη «BETWEEN...» στο αρχικό μήνυμα.

Η παραπάνω ιδιότητα των πολυαλφαβητικών μεθόδων κρυπτογράφησης οφείλεται στη χρήση διδιάστατων πινάκων αντικατάστασης, με μία ή δύο λέξεις-κλειδιά, που προκαλούν αυξημένη στατιστική διασπορά στην εμφάνιση των χαρακτήρων στα κρυπτογράμματα και μεγάλη δυσκολία στην κρυπτανάλυση μέσω συσχέτισης εμφάνισης. Η δυσκολία αυτή αυξάνεται σημαντικά με την αύξηση του μήκους των λέξεων-κλειδιών. Παρόλα αυτά, με τη χρήση σύγχρονων ηλεκτρονικών υπολογιστών είναι δυνατή η κρυπτανάλυση μέσω συσχέτισης εμφάνισης αλκίλων τμημάτων του κρυπτογράφματος, μεγάλους ανάλογα με το υποθετικό μήκος της λέξης-κλειδιού (χαρακτήρες σε ζεύγη, τριάδες, τετράδες, κλπ.), αρκεί το συνολικό μέγεθος του κρυπτογράφματος να είναι αρκετά μεγάλο για μια τέτοια στατιστική ανάλυση.





ποιες δημόσιες ανακοινώσεις μεθοδολογικών και τεχνικών ανάλυσης του κειμένου, οι οποίες υποτίθεται πως αποδείκνυαν ότι το έργο δεν είναι τίποτα άλλο παρά μια καλοεχρησιμοποιημένη φάρσα, όμως τίποτα από αυτά δεν εξακριβώθηκε τελικά με οδισφιόσθητο τρόπο. Οι πιθανές εξηγήσεις και ερμηνείες του χειρογράφου συνεχίζονται μέχρι και σήμερα.

Μια εξίσου διάσημη αλλά πολύ πιο «σκοτεινή» περίπτωση παρόμοιων απαράθιστων κρυπτογραμμάτων είναι μια σειρά από 20 και πλέον επιστολές του κατά συρροή δολοφόνου του «Ζωδιακού Κύκλου» («Zodiac killer») που απέστειλε σε εφημερίδες και αστυνομικές υπηρεσίες κατά την περίοδο της δράσης του στην ευρύτερη περιοχή του San Francisco των ΗΠΑ, μεταξύ 1966 και 1974. Οι αρχικές επιστολές, οι οποίες θεωρούνται σίγουρα αυθεντικές και



*Κοντινή άποψη της μεταλλικής πλάκας, τοποθετημένης ανάμεσα σε κομμάτια πέτρας, με χαραγμένο μήνυμα σε κώδικα Μορς. Το περιχόμενο μήνυμα σε κώδικα παραπέμπει στη λέξη «PALIMPSEST», η δεύτερη λέξη «κλειδί για την αποκρυπτογράφηση του κρυπτογράμματος Κ.Ι.*

όμοια σχετιζόμενες με συγκεκριμένες επιθέσεις, ήταν τέσσερις και περιείχαν σειρές από σύμβολα και ιδιοεργράμματα, ενώ οι μέθοδοι κρυπτογράφησης ήταν κυρίως συνδυασμός τεχνικών αντικατάστασης και κωδικοσελίδων μιας χρήσης («one-time pads»). Τα τέσσερα βασικά μηνύματα περιελάμβαναν χειρόγραφα κρυπτογράμματα μήκους μερικών εκατοντάδων συμβόλων. Αυτό αυτά, μόνο το ένα έχει επιβεβαιωμένα αποκρυπτογραφηθεί, ενώ τα υπόλοιπα είτε έχουν αποκρυπτογραφηθεί μερικώς είτε έχουν δεχθεί πολλές διαφορετικές λύσεις. Το 2004 η υπόθεση χαρακτηρίστηκε ως επίσημα «ανεπιβεβαιωμένη», όμως το 2007 άνοιξε εκ νέου, ενώ από το 2009 μέχρι και σήμερα υπάρχει σημαντικό ενδιαφέρον από τις αμερικανικές αρχές στην περιοχή του San Francisco και της κομητείας του Riverside που συνδέεται άμεσα με τα γεγονότα.

Από τα αρχαία ευρήματα, αναμφισβήτητα δύο από τους πιο δημοφιλείς απαράθιστους κώδικες είναι αυτοί του «Δίσκου της Φαιστός» και της «Γραμμικής Γραφής Α'». Ο δίσκος της Φαιστός είναι ένα πήλινο κατασκευάσμα διαμέτρου περίπου 15 εκατοστών, το οποίο ανακαλύφθηκε στις αρχές του 20ού αιώνα στην Κρήτη και πιστεύεται πως ανήκει χρονολογικά στο 1800 π.Χ. Στον δίσκο υπάρχουν 241 σύμβολα και στις

**Ο δίσκος της Φαιστός είναι ένα πήλινο κατασκευάσμα διαμέτρου περίπου 15 εκατοστών, το οποίο ανακαλύφθηκε στις αρχές του 20ού αιώνα στην Κρήτη και πιστεύεται πως ανήκει χρονολογικά στο 1800 π.Χ.**

δύο όψεις, ενός άγνωστου αλφαριθμητικού 45 συνολικά χαρακτήρων. Το ακριβές περιεχόμενο του κειμένου παραμένει άγνωστο ακόμα και σήμερα, παρόλο που έχουν προταθεί διάφορες λύσεις με εντελώς διαφορετικό νόημα. Σχετικά με τον δίσκο της Φαιστός, είναι και μια σειρά από άλλα ευρήματα με επιγραφές αποτυπωμένες σε γραφή Γραμμική Α', επίσης από το 1800 π.Χ. Συγκεκριμένα, πιστεύεται πως τα σύμβολα στον δίσκο της Φαιστός ίσως μπορούν να χρησιμοποιηθούν για την αποκρυπτογράφηση των συμβόλων της Γραμμικής Α', χωρίς όμως αυτό να έχει επιβεβαιωθεί στην πράξη, κυρίως λόγω του μικρού μήκους των διαθέσιμων κρυπτογραμμάτων. Αντίθετα, η μεταγενέστερη γραφή Γραμμική Β', η οποία μοιάζει αρκετά με τη Γραμμική Α', αποκρυπτογραφήθηκε πλήρως το 1952, κα-

θώς υπήρχαν πλήθος από σχετικά ευρήματα με κρυπτογράμματα σε αυτή τη γραφή.

Από τους πιο διάσημους σύγχρονους κώδικες που τελικά δεν παρέμειναν απαράθιστοι είναι αναμφισβήτητα ο αλγόριθμος της μηχανής «Αίνιγμα» («Enigma»), η οποία αποτέλεσε τη βασική μέθοδο κατασκευής κρυπτογραφημένων μηνυμάτων του Γερμανικού Ναυτικού κατά τον Β' Παγκόσμιο Πόλεμο. Η μηχανή «αίνιγμα» ήταν στην πραγματικότητα μια εξαιρετικά σύνθετη κατασκευή, αρχικά μηχανική και στη συνέχεια μερικώς ηλεκτρονική, που επέτρεπε τη δακτυλογράφηση μηνυμάτων σε γραφομηχανή και την αυτόματη εκτύπωσή τους ως τηλεγραφικά κρυπτογράμματα. Οι μέθοδοι κρυπτογράφησης που χρησιμοποιούσε περιελάμβαναν συνδυασμό μεθόδων αντικατάστασης και κωδικοσελίδων



Μερική όψη του δίσκου της Φαιστός, στο αρχαιολογικό μουσείο του Ηρακλείου στην Κρήτη. Διακρίνονται μερικά από τα 45 συνολικά σύμβολα του άγνωστου αλφαβήτου που χρησιμοποιείται στην επιγραφή.

με μεταβλητούς κώδικες-κλειδιά, καθιστώντας την παραδίση των κρυπτογραμ-

μάτι της ανθρώπινης Ιστορίας. Επηρεάζουν την έκβαση γεγονότων, αποκαλύπτουν κρυφές λεπτομέρειες προσώπων και καταστάσεων, αλλά κυρίως εξάπτουν τη φαντασία όσων ασχολούνται μαζί τους και κυριεύονται από την επιθυμία να μάθουν τα μυστικά που κρύβουν.

Το γλιπτό «ΚΡΥΠΤΟΣ» αποτελεί έναν από τους πολλούς κρυπτογραφικούς γρίφους που εξακολουθούν να παραμένουν απαράβιαστοι και να προκαλούν το ενδιαφέρον ερασιτεχνών κρυπταναλυτών και ανθρώπων κάθε ειδικότητας και επαγγέλματος από ολόκληρο τον κόσμο. Παρότι αποτελεί απλώς ένα καλλιτεχνικό δημιούργημα, εξακολουθεί να ανήκει στη μικρή και εξαιρετική εκείνη κατηγορία των απαράβιαστων κωδικών, που συνεχίζουν να προκαλούν και να κρύβουν μέχρι σήμερα τα μικρά ή μεγάλα μυστικά τους. ■

- <http://www.elonka.com/kryptos/KryptosAerial.html>  
 (10) Kim Zetter: KRYPTOS ARTIST LAUNCHES WEBSITE TO RECEIVE SOLUTIONS, 10/11/2010, <http://www.wired.com/threatlevel/2010/11/kryptos-web-site/>  
 (11) Justin Redman, David Enzor: CRACKING THE CODE, CNN U.S., 20/6/2005, [http://articles.cnn.com/2005-06-19/us/cracking.the.code.1\\_code/kryptos-sculture-robert-langdon?\\_s=PM:US](http://articles.cnn.com/2005-06-19/us/cracking.the.code.1_code/kryptos-sculture-robert-langdon?_s=PM:US)  
 (12) THE KRYPTOS STORY, Central Intelligence Agency - Official Website, 17/5/2010, <http://www.cia.gov/about-cia/headquarters-tour/kryptos/fish-movie-text.html>  
 (13) Yahoo! Groups, KRYPTOS (description), 13/8/2011, <http://tech.groups.yahoo.com/groups/kryptos/>  
 (14) Kim Zetter: QUESTIONS FOR KRYPTOS' CREATOR, 20/1/2005, <http://www.wired.com/techbiz/media/news/2005/01/66337?currentPage=all>



μάτων εξαιρετικά δύσκολη για εκείνη την εποχή. Τελικά, η ομάδα αναλυτών της Βρετανίας στο Bletchley Park, της οποίας εξέχων μέλος ήταν και ο Alan Turing, θεμελιώτης της θεωρίας υπολογισμού και πολυπλοκότητας στην επιστήμη της Πληροφορικής, κατάφεραν να «σπάσουν» τον κώδικα του «Αίνιγμα». Όπως αποκαλύφθηκε πολλά χρόνια αργότερα, τη δεκαετία του 70, η επίλυση βασίστηκε εν μέρει στην εργασία Πολωνών κρυπταναλυτών το 1932 και στην αποκάλυψή τους σε Γάλλους και Βρετανούς συμμάχους το 1939, όμως η μεταγενέστερη έκδοση του «Αίνιγμα» για το Γερμανικό Ναυτικό ήταν πιο σύνθετη και πολύ πιο δύσκολο να παραβιαστεί. Με τη βοήθεια των πρωτόγονων υπολογιστών της εποχής, κατάφεραν να ανακαλύψουν τα κλειδιά και να πετύχουν την πλήρη αποκρυπτογράφηση των μηνυμάτων των Γερμανικού Ναυτικού μέσα σε μερικές μόλις ώρες, κάτι που επηρέασε αποφασιστικά την έκβαση του Β' Παγκοσμίου Πολέμου.

## ΕΠΙΛΟΓΟΣ

Οι κώδικες και οι κρυπτογραφικοί γρίφοι αποτέλεσαν πάντα ένα ξεχωριστό κομ-

## ΒΙΒΛΙΟΓΡΑΦΙΑ

- (1) Wikipedia, KRYPTOS, 13/8/2011, <http://en.wikipedia.org/wiki/Kryptos>  
 (2) KRYPTOS FAQ, 4/5/2011, <http://elonka.com/kryptos/faq.html>  
 (3) ELONKA'S LIST OF FAMOUS UNSOLVED CODES AND CIPHERS, 8/8/2010, <http://www.elonka.com/UnsolvedCodes.html>  
 (4) Kim Zetter: TYPO CONFOUNDS KRYPTOS SLEUTHS, 20/4/2006, <http://www.wired.com/print/science/discoverscience/news/2006/04/70701>  
 (5) John Schwartz: CLUES TO STUBBORN SECRET IN C.J.A.'S BACKYARD, The New York Times, 20/11/2010, <http://www.nytimes.com/2010/11/21/us/21codecharts.html?hp>  
 (6) Steven Levy: MISSION IMPOSSIBLE: THE CODE EVEN THE CIA CAN'T CRACK, 20/4/2009, [http://www.wired.com/science/discoveries/magazine/17-05/1\\_kryptos?currentPage=all](http://www.wired.com/science/discoveries/magazine/17-05/1_kryptos?currentPage=all)  
 (7) Kim Zetter: SOLVING THE ENIGMA OF KRYPTOS, 21/1/2005, <http://www.wired.com/culture/lifestyle/news/2005/01/66337?currentPage=all>  
 (8) Wikipedia, JIM SANBORN, 13/8/2011, [http://en.wikipedia.org/wiki/Jim\\_Sanborn](http://en.wikipedia.org/wiki/Jim_Sanborn)  
 (9) KRYPTOS - THE BIRD'S EYE VIEW, 13/8/2011,

- (15) Stephan Pincock: KRYPTΟΓΡΑΦΙΑ (CODEBREAKER), Elwin Street Ltd (2006), ΕΚΔΟΣΕΙΣ ΠΡΑΥΟΣ, 2008.  
 (16) Jon Swaine: CIA'S KRYPTOS SCULPTURE CLOSE TO BEING SOLVED, Telegraph, 21/11/2010, <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/8149792/CIA-s-Kryptos-sculpture-close-to-being-solved.html>  
 (17) John Schwartz: ORIGINAL DECODING CHARTS FOR 'KRYPTOS', The New York Times, 20/11/2010, [www.nytimes.com/2010/11/21/us/21codecharts.html](http://www.nytimes.com/2010/11/21/us/21codecharts.html)  
 (18) TOP 10 UNCRACKED CODES, 1/10/2007, <http://listverse.com/2007/11/01/top-10-uncracked-codes/>  
 (19) Wikipedia, VIGENERE CIPHER, 19/12/2011, [http://en.wikipedia.org/wiki/Vigenere\\_cipher](http://en.wikipedia.org/wiki/Vigenere_cipher)  
 (20) Jim Gillogly: KRYPTOS SCULPTURE PIX (Pictures Gallery), 19/12/2011, <http://www.voyrich.net/Kryptos/>



# ΠΕΡΙΣΚΟΠΙΟ

ΤΗΣ ΕΠΙΣΤΗΜΗΣ

**50%**  
ΕΚΠΤΩΣΗ  
ΣΕ ΒΙΒΛΙΑ & ΠΕΡΙΟΔΙΚΑ  
(σελ. 6)



## Αναγέννηση της καρδιάς

Νέες ελπίδες για την αναστροφή των συνεπειών ενός εμφράγματος



## Ανιχνώντας ενέργεια από τα ραδιοκύματα

## Συστήματα φωτισμού με

# LED

Η τεχνολογία του μέλλοντος

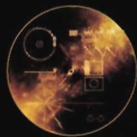
# Αποστολή Juno

Αποκαλύπτοντας τα μυστικά του Δία



## Cryptos

Ένα γλυπτό-μνημείο για τους κώδικες και τα μυστικά



## Το παράδοξο του Fermi

Αν υπάρχουν εξωγήινοι, γιατί δεν έχουμε έλθει ακόμη σε επαφή μαζί τους;



9 771105 712006

03>