Κύριε Πρύτανη, Κύριοι Αντιπρυτάνεις, Κύριοι Κοσμήτορες

Αγαπητοί συνάδελφοι

Αγαπητοί φοιτητές

Το πρωί της 28ης Οκτωβρίου του 1940 οι σχετικά λίγοι κάτοχοι ραδιοφωνικών συσκευών άκουσαν τον εκφωνητή Κώστα Σταυρόπουλο να μεταδίδει με παλλόμενη από συγκίνηση φωνή το εξής μήνυμα «Εδώ ραδιοφωνικός σταθμός Αθηνών. Έκτακτον ανακοινωθέν. Η Ελλάς από της έκτης πρωινής της σήμερον ευρίσκεται εις εμπόλεμον κατάστασιν προς την Ιταλίαν. Μεταδίδομε το πρώτο ανακοινωθέν του Ελληνικού Γενικού Στρατηγείου: Αι ιταλικαί στρατιωτικαί δυνάμεις, προσβάλλουν από της 05:30 πρωινής της σήμερον, τα ημέτερα τμήματα προκαλύψεως της Ελληνοαλβανικής Μεθορίου. Αι ημέτεραι δυνάμεις, αμύνονται του Πατρίου εδάφους».

Η ιταλική επίθεση δεν ήταν κεραυνός εν αιθρία. Οι ελληνικές διαβιβάσεις παρακολουθούσαν τους ιταλικούς ασυρμάτους διαρκώς. Είχαν πλήρη εικόνα για τον τρόπο που επικοινωνούσαν οι ιταλοί στρατιωτικοί ο οποίοι χρησιμοποιούσαν ασυρμάτους χωρίς κρυπτογράφηση καθότι πίστευαν ότι οι έλληνες δεν διαθέτουν αρκετούς για να τους παρακολουθούν. Ήταν λάθος τους. Πριν την έναρξη του πολέμου η Ελλάδα είχε προμηθευτεί μυστικά ικανό αριθμό ασυρμάτων για να παρακολουθεί τις ιταλικές ενδοεπικοινωνίες.

Η σημερινή ομιλία αφορά τη συμβολή των μαθηματικών μέσω της κρυπτογραφίας στη νίκη κατά του ναζισμού. Εξ ου και ο τίτλος «Ένα μαθηματικό Enigma και ο πόλεμος κατά του ναζισμού». Θα προσπαθήσουμε να φωτίσουμε με αυτό τον τρόπο μια αρκετά περίπλοκη πλευρά του Δευτέρου Παγκοσμίου Πολέμου εκεί που κατά πολλούς ιστορικούς κρίθηκε καθοριστικά η νίκη των συμμάχων. Η αξιοποίηση και η διαχείριση των πληροφοριών είχε πολύ μεγαλύτερη συμβολή στη νίκη από ότι νομιζόταν αρχικά με την σχετική έρευνα να συνεχίζει να φέρνει στο φως άγνωστα στοιχεία αλλά και τεχνολογικές και επιστημονικές πλευρές καινούργιες για τα δεδομένα της εποχής. Εξάλλου οι ανάγκες του πολέμου οδήγησαν στην κατασκευή του πρώτου προγραμματιζόμενου ηλεκτρονικού υπολογιστή. Ήταν η πρώτη φορά

που δημιουργήθηκε ένας παράλληλος με τον πραγματικό ψηφιακός κόσμος βασισμένος στην αριθμητική αναπαράσταση μέσω των διακριτών μαθηματικών και της μαθηματικής λογικής.

Οι κρυπτογραφημένες επικοινωνίες αποτελούν μέρος αυτού που στην ελληνική στρατιωτική ορολογία ονομάζονται διαβιβάσεις. Μολονότι ο ρόλος τους ήταν ιδιαίτερα σημαντικός στο έπος του 1940, δεν έχει αναδειχθεί, με το πρώτο και μοναδικό εξ όσων γνωρίζω σχετικό βιβλίο να έχει εκδοθεί μόλις τον Ιούνιο του 2021. Είναι όμως βέβαιο ότι οι Έλληνες είχαν πολλές και σημαντικές επιτυχίες υποκλοπής Ιταλικών ραδιοεπικοινωνιών σε βαθμό τέτοιο, ώστε να αποκτήσουν θρυλικές διαστάσεις, τουλάχιστον τους πρώτους μήνες. Επίσης τόσο οι Ιταλοί όσο και οι Γερμανοί δεν κατάφεραν να σπάσουν τους ελληνικούς κώδικες ούτε του στρατού ούτε του ναυτικού.

Η γερμανική επιχείρηση Ερμής, όπως ήταν το συνθηματικό όνομα της επιχείρησης κατάληψης της Κρήτης από 20 Μαίου έως την 1η Ιουνίου του 1941, που έμεινε στην ιστορία ως Η Μάχη της Κρήτης, είναι η πρώτη επιχείρηση μεγάλης κλίμακας τα σχέδια της οποίας ήταν γνωστά στους συμμάχους μέσα από το σπάσιμο του Γερμανικού κώδικα επικοινωνιών. Κάποιοι βέβαια υποστηρίζουν ότι είναι η δεύτερη τέτοια επιχείρηση με πρώτη τη Γερμανική επίθεση στην Ελλάδα μέσω Βουλγαρίας. Σύμφωνα με τον ιστορικό Δημήτρη Λυβάνιο «Το πρωί της 20ής Μαΐου 1941, ένας νεαρός Βρετανός αξιωματικός απολάμβανε ένα αξιοπρεπές πρωινό στα Χανιά, προσκεκλημένος ενός Νεοζηλανδού στρατηγού. Καθώς ανασήκωσε το βλέμμα του προς τον ουρανό, παρατήρησε πλήθος αεροπλάνων και αλεξιπτωτιστών. Οταν ο Κ. Μ. Γούντχαουζ υπέδειξε στον Μπέρναρντ Φρέιμπεργκ, διοικητή των συμμαχικών δυνάμεων της Κρήτης, το αναπάντεχο θέαμα, ο φλεγματικός στρατηγός, αφού συμβουλεύτηκε το ρολόι του, αρκέστηκε να παρατηρήσει: «Ακριβώς στην ώρα τους!». Η ηρεμία του οφειλόταν στο ότι είχε επαρκή, αλλά όχι άριστη, γνώση των γερμανικών κινήσεων. Καθώς η γερμανική κρυπτογραφική μηχανή «Enigma» είχε ήδη «σπάσει», οι Βρετανοί γνώριζαν πλήρως τον σχεδιασμό της εισβολής. Ωστόσο, η πολύτιμη αυτή πηγή πληροφοριών, με το κωδικό όνομα «Ultra», θα έπρεπε να διαφυλαχθεί με κάθε κόστος και κατά συνέπεια ο Φρέιμπεργκ δεν επρόκειτο να έχει πλήρη πρόσβαση στο υλικό που προερχόταν από αυτήν.». Οι πληροφορίες που προέρχονταν από το Ultra είχαν

αυστηρή διαβάθμιση και έφταναν μόνο σε ελάχιστα άτομα στο ψηλότερο δυνατό επίπεδο. Για την μάχη της Κρήτης δεν είναι γνωστό πως τελικά αξιοποιήθηκαν οι πληροφορίες από το Ultra και πόσο ακριβείς ήταν οι πληροφορίες που έφτασαν στον Φρείμπεργκ. Το βέβαιο είναι ότι ο στρατηγός είχε αρκετές πληροφορίες για τις Γερμανικές κινήσεις, εν τούτοις επέλεξε να περιμένει κυρίως αμφίβια επίθεση, ενώ οι Γερμανοί είχαν εστιάσει στη δημιουργία προγεφυρώματος στο αεροδρόμιο του Μάλεμε. Αυτή του η απόφαση έκρινε και την τελική έκβαση της μάχης της Κρήτης. Η μη πλήρης αξιοποίηση των πληροφοριών από τον στρατηγό προκάλεσε εκνευρισμό και απογοήτευση στο επιτελείο της Ultra.

Ποια ήταν όμως η επιχείρηση Ultra; Ήταν η βασική επιχείρηση συλλογής πληροφοριών από τους Γερμανούς μέσα από τεχνικές ηλεκτρονικού πολέμου κατά τη διάρκεια του Δεύτερου Παγκοσμίου Πολέμου. Οργανώθηκε από τη Βρετανία με επίκεντρο τη Σχολή Κυβερνητικών κωδίκων και κρυπτογραφίας στο Μπλέτλσεϊ Πάρκ, 50 μίλια βόρεια του Λονδίνου, και πήρε το όνομά της από το Ultra secret, την ύψιστη διαβάθμιση ασφαλείας.

Σε κάποιες λίγες περιπτώσεις πληροφορίες από την Ultra μεταφέρονταν και σε τρίτους. Για παράδειγμα, είχε μεταφερθεί η πληροφορία για την επιχείρηση Μπαρμπαρόσα της Γερμανικής επίθεσης στη Σοβιετική Ένωση – που όμως ο Στάλιν δεν θεώρησε αξιόπιστη και δεν την αξιοποίησε. Μια από τις σημαντικότερες συνεισφορές της Ultra ήταν στη μάχη του Ατλαντικού. Από τον Ιούνιο του 1941 και μετά οι σύμμαχοι ήταν σε θέση να γνωρίζουν τις κινήσεις των Γερμανικών υποβρυχίων, αυτές για τις οποίες ο Τσώρτσιλ είχε πει ότι ήταν το μόνο που τον φόβισε σε όλο τον πόλεμο. Οι πληροφορίες του Ultra καθόρισαν και το αποτέλεσμα της μάχης υπέρ των Συμμάχων. Μια άλλη χαρακτηριστική συνεισφορά ήταν η επαλήθευση της παραπλάνησης των Γερμανών ότι η απόβαση θα γίνει στο Καλαί και όχι στη Νορμανδία.

Η ύπαρξη και ο ρόλος της Ultra παρέμειναν μυστικές για πολλά χρόνια μετά τον πόλεμο. Μετά το 1974 άρχισε η σταδιακή δημοσιοποίηση πληροφοριών, κυρίως μετά τη δημοσίευση του βιβλίου The Ultra Secret από τον νούμερο δύο της

Βρετανικής αντικατασκοπείας Frederick William Winterbotham που συνεπέβλεπε την επιχείρηση Ultra σε όλη τη διάρκεια του πολέμου. Έχει ενδιαφέρον ότι μετά τη δημοσιοποίηση των σχετικών πληροφοριών άρχισε πιο συστηματική έρευνα από ερευνητές ιστορικούς που οδήγησε και στη μερική αναθεώρηση της μέχρι τότε ιστοριογραφίας για όλο τον Δεύτερο Παγκόσμιο Πόλεμο. Μετά το τέλος του πολέμου, για λόγο που δεν έχει ακόμα εξακριβωθεί σχεδόν όλα τα πρωτότυπα ντοκουμέντα συμπεριλαμβανομένων και των μηχανών κωδικοποίησης και αποκωδικοποίησης αλλά και των υπολογιστικών μηχανών καταστράφηκαν με εντολή του ίδιου του Τσώρτσιλ. Ενδέχεται ο Τσώρτσιλ να κατέληξε σε αυτή την απόφαση για να μην υπάρξει και δεύτερη παράλληλη ιστορία που θα μπορούσαν να εκμεταλλευτούν οι ηττημένοι.

Για την κάλυψη της μυστικότητας της επιχείρησης είχαν ληφθεί μια σειρά από μέτρα: (α) Η «κατασκευή» εικονικών πρακτόρων (πχ το δίκτυο Boniface), (β) η αξιοποίηση πληροφοριών του Ultra στο πεδίο της μάχης μόνο εάν μπορούσε να αποδοθεί και σε δεύτερη πηγή - έτσι, συχνά έκαναν επίτηδες αναγνωρίσεις με αεροσκάφη για να υπάρχει σχετική κάλυψη, (γ) η δέσμευση όλων των εργαζομένων στο Μπλέτσλει Παρκ με τον ύψιστο βαθμό ασφάλειας – τυχόν σπάσιμο της μυστικότητας μπορούσε να τιμωρηθεί με ποινή θανάτου. Το δίκτυο Boniface είχε ιδιαίτερο ενδιαφέρον, καθότι είχε κατασκευαστεί πέραν της εικονικής μορφής πράκτορα, του Boniface, ένα δίκτυο πρακτόρων υποτίθεται σε όλη την Ευρώπη. Οι Γερμανοί είχαν θεωρήσει ότι το δίκτυο είναι υπαρκτό και μάλιστα έκαναν και ειδικές επιχειρήσεις για να συλλάβουν μέλη του δικτύου. Στην πραγματικότητα η συλλογή πληροφοριών γινόταν μέσω των δικτύων που παρακολουθούσε την ανταλλαγή πληροφοριών του Γερμανικού επιτελείου μέσω των συστημάτων Enigma και Lorenz καθώς και των κρυπτογραφικών μηχανών τύπου C-36 (Hagelin).

Η σημασία του Ultra ήταν καθοριστική για την έκβαση του πολέμου. Ο ίδιος ο Τσώρτσιλ είχε πει ότι «με αυτό νικήσαμε», κάτι που επιβεβαιώνει και ο διαπρεπής ιστορικός των Βρετανικών υπηρεσιών πληροφοριών Σιρ Χάρρυ Χίντσλει αλλά και πολλοί άλλοι ιστορικοί. Η αλήθεια βέβαια είναι ότι η επιχείρηση αυτή πέτυχε διότι

στηρίχτηκε και σε κάποια από τα σημαντικότερα μαθηματικά μυαλά της Βρετανίας εκείνης της περιόδου, που αξιοποίησαν και πήγαν πιο πέρα τη δουλειά Πολωνών μαθηματικών πάνω στο ίδιο θέμα. Αξιοποιήθηκαν επίσης παραδοσιακοί κρυπτογράφοι, λύτες σταυρολέξων, σκακιστές, γλωσσολόγοι και μηχανικοί των Βρετανικών ταχυδρομείων. Αξίζει να αναφέρουμε ότι η ομάδα περιελάμβανε αρκετούς ειδικούς από τον χώρο των ανθρωπιστικών επιστημών, δηλαδή κλασσικής φιλολογίας ελληνικής και λατινικής, αρχαίας ιστορίας ακόμα και Αιγυπτιολογίας. Δεν ήταν λίγοι αυτοί που μετά έγιναν καθηγητές στην Οξφόρδη και το Καίμπριτζ, μετά την ολοκλήρωση της επιχείρησης Ultra.

Η κρυπτογραφική συσκευή Enigma ήταν μια ηλεκτρομηχανική συσκευή που χρησιμοποιείτο από τους Γερμανούς για την κωδικοποίηση και αποκωδικοποίηση των μηνυμάτων. Η αρχιτεκτονική τους βασιζόταν σε περιστρεφόμενους δίσκους (ρότορες). Η μηχανή εφευρέθηκε από τον γερμανό μηχανικό Άρθουρ Σέμπιους λίγο μετά τον πρώτο παγκόσμιο πόλεμο. Αρχικά χρησιμοποιήθηκε για εμπορικές και διπλωματικές επικοινωνίες αλλά κατέληξε μετά το 1930 και για πάνω από δέκα χρόνια να είναι η βασική μηχανή κρυπτογράφησης των Γερμανικών ενόπλων δυνάμεων. Οι Γερμανοί πρόσθεσαν επιπλέον κλείδες ασφαλείας όπως για παράδειγμα αλλαγή στις αρχικές θέσεις των ροτόρων καθημερινά, επιπλέον βύσματα, περισσότερους ρότορες (η συσκευή του Γερμανικού ναυτικού είχε 4 ρότορες αντί για τους συνήθεις 3) κλπ. Με την γνωστή μέθοδο της εξάντλησης όλων των δυνατών συνδυασμών ήταν φαινομενικά αδύνατο για τα δεδομένα της εποχής να εκτελεστούν όλοι οι σχετικοί υπολογισμοί - έπρεπε να γίνουν το πολύ σε διάστημα λίγων ορών πάνω από ένα τρισεκατομμύριο συνδυασμοί.

Στις αρχές του εικοστού αιώνα η Πολωνία αποτελεί μια σπουδαία ανερχόμενη δύναμη στα μαθηματικά, τη λογική και τη φιλοσοφία. Ειδικότερα την περίοδο ανάμεσα στους δύο παγκόσμιους πολέμους η μαθηματική επιστήμη βρίσκεται σε πολύ ψηλό επίπεδο, όπως και η λογική. Μαθηματικοί όπως ο Στεφαν Μπάναχ – σημαντική μορφή στην ανάλυση και ειδικοί στη λογικοί όπως ο Λουκασιέβιτς με τα συστήματα τροπικής λογικής εμπνευσμένα από τον Αριστοτέλη είναι δύο μόνο από τις σπουδαίες προσωπικότητες της Πολωνικής ακαδημαϊκής κοινότητας. Μέσα σε αυτό το κλίμα ολοκλήρωσε τις σπουδές και την έρευνά του ο αλγεβρίστας Μάριαν Ριέφσκι – ειδικός στη μεταθετική θεωρία ομάδων - που μαζί με τους συναδέλφους

του μαθηματικούς – κρυπτολόγους Ροζίσκι και Ζιγκάλτσκι πιστώνονται σήμερα την μελέτη, και την πρώτη αποκρυπτογράφηση για λογαριασμό των Πολωνικών μυστικών υπηρεσιών των μηνυμάτων του Γερμανικού στρατιωτικού Enigma. Η μέθοδος του Ριέφκσι βασίστηκε στις κυκλικές ομάδες και αξιοποίησε ορισμένα ασθενή σημεία της κωδικοποίησης της μηχανής σε συνδυασμό με σχετικές πληροφορίες από συνδέσμους. Η επιτυχία αυτή κατέστη δυνατή στην αρχή της μέσα από πληροφορίες των Γαλλικών μυστικών υπηρεσιών. Πιο συγκεκριμένα, οι Γάλλοι μέσω πρακτόρων τους στις Γερμανικές μυστικές υπηρεσίες είχαν καταφέρει να υποκλέψουν κάποια εγχειρίδια χρήσης καθώς και ένα ενδεικτικό φύλλο ημερήσιας ρύθμισης της συσκευής. Το υλικό αυτό όμως δεν κατάφεραν να το αξιοποιήσουν. Έτσι το μοιράστηκαν με τους Πολωνούς που τελικά κατάφεραν να «σπάσουν» τον κώδικα. Ο Ριέφσκι και η ομάδα του είχαν μάλιστα ανακατασκευάσει το δικό τους Enigma αλλά και μηχανή για το «σπάσιμό» του τις περίφημες Μπόμπες.

Οι Μπόμπες χρησιμοποιούσαν ως πρώτη ύλη κρυπτομηνύματα με περιεχόμενο που μπορούσε εύκολα να εικάσει κανείς τη δομή του. Για παράδειγμα ένα δελτίου καιρού είναι πολύ πιθανό να περιλαμβάνει τη λέξη βροχή, ή τη λέξη άνεμος, ή τη λέξη αίθριος. Στη συνέχεια έκαναν σχετικές δοκιμές και κατέληγαν σε διάφορα σενάρια. Από κει και πέρα τη δουλειά την αναλάμβαναν οι κρυπτολόγοι που έκαναν όλη τη σχετική επεξεργασία χειρονακτικά.

Οι Βρετανοί δεν είχαν καμία γνώση σχετικά με το Enigma μέχρι και το 1939. Τότε, πέντε εβδομάδες πριν ξεκινήσει ο δεύτερος Παγκόσμιος Πόλεμος, με την Γερμανική εισβολή στην Πολωνία, η πολωνική αντικατασκοπεία και η ομάδα του Ριέφσκι οργάνωσαν συνάντηση στη Βαρσοβία, στην οποία και μοιράστηκαν με τους Βρετανούς και Γάλλους συμμάχους τους όλη την γνώση τους σχετικά με το Γερμανικό σύστημα κρυπτογράφησης. Η συνάντηση αυτή που παρέμεινε μυστική για πολλά χρόνια ήταν μια από τις πιο κρίσιμες στην ιστορία του Δευτέρου Παγκοσμίου Πολέμου. Αξίζει να αναφερθεί ότι η ομάδα των Πολωνών κρυπτογράφων ποτέ δεν εργάστηκε για τους Βρετανούς στο Μπλέτσλει Παρκ και ότι η συνεισφορά τους είχε περάσει στη σκιά για χρόνια. Ο Ριέφσκι μετά το τέλος του πολέμου επέστρεψε στην Πολωνία από τη Βρετανία και έζησε το υπόλοιπο της ζωής του ως λογιστής. Μετά και τη δημοσίευση βιβλίου του από το Πολωνικό

Γενικό Επιτελείο σχετικά με το σπάσιμο το κώδικα τη δεκαετία του 1960 αναγνωρίστηκε η προσφορά του από την Πολωνία και όταν πέθανε κηδεύτηκε με τιμές. Μόνο τα τελευταία χρόνια και με τη σημαντική πρωτοβουλία του Σερ Ντερμοντ Τιούριγκ, ανηψιού του Σερ Άλαν, η προσφορά τους άρχισε να παίρνει ευρεία δημοσιότητα και αναγνώριση.

Έχει πάρει ιδιαίτερη δημοσιότητα, και καλώς, η συνεισφορά του σπουδαίου μαθηματικού, ειδικού στη λογική και κρυπταναλυτή Άλαν Τιούριγκ κυρίως μέσα από βιβλία, ταινίες όπως το «Παιχνίδι της μίμησης» αλλά και θεατρικά έργα. Ο Τιούριγκ είχε το χάρισμα ενός πρωτοπόρου θεωρητικού μαθηματικού συνδυασμένο με τις εφαρμογές και τις πρακτικές ικανότητες ενός μηχανικού. Η συνεισφορά του Άλαν Τιούριγκ στο σπάσιμο του Γερμανικού Enigma αλλά και στην επιστημονική δραστηριότητα της Ultra είναι τεράστια. Διαφορετική βέβαια σε πολλά σημεία από όσα περιγράφει η ταινία «Το παιχνίδι της μίμησης» (Imitation game). Πιο συγκεκριμένα, μαζί με μια ομάδα σπουδαίων μαθηματικών και τεχνικών κατάφερε μέσα σε τρεις μήνες, μέχρι τον Δεκέμβριο του 1939, αξιοποιώντας τη γνώση που μοιράστηκαν οι Πολωνοί, να θέσει το σύστημα αποκωδικοποίησης του Enigma σε παραγωγική λειτουργία. Φτιάχτηκαν πολλές μηχανές Bomba και άρχισαν να δίνουν αποτελέσματα. Ο Τιούριγκ έφτιαξε νέα μαθηματικά εργαλεία που επιτάχυναν την ανάγνωση των κρυπτομηνυμάτων, εργαλεία βασισμένα στη στατιστική ανάλυση. Ήταν από τους πρώτους που κατάλαβε τη σημασία της δημιουργίας υπολογιστικών μηχανών που διαθέτουν την απαιτούμενη ταχύτητα για την αποκωδικοποίηση πιο δύσκολων κρυπτομηνυμάτων. Τέλος, η ομάδα του έσπασε το Enigma του Γερμανικού ναυτικού, αξιοποιώντας δύο συσκευές Enigma που είχαν βρεθεί σε Γερμανικά υποβρύχια. Έτσι, οι σύμμαχοι κατάφεραν να κερδίσουν τελικά στη μάχη του Ατλαντικού και να περιοριστούν κατά πολύ οι βυθίσεις των σκαφών τους από τα U-Boats. Κατά τη διάρκεια του πολέμου, ο Τιούριγκ ταξίδεψε στις ΗΠΑ προκειμένου να συνδράμει με την τεχνογνωσία του στα κρυπτοσυστήματα την Αμερικανική αντικατασκοπεία. Μεταξύ άλλων ασχολήθηκε με την κρυπτογράφηση της ανθρώπινης φωνής μέσα από ειδικά συστήματα επικοινωνίας. Έτσι, στήθηκε ένα ολόκληρο σύστημα κωδικοποιημένης φωνητικής επικοινωνίας ανάμεσα στον Τσώρτσιλ και τον Ρούσβελτ.

Το 1941 εμφανίζονται προβλήματα στη λειτουργία του Μπλέτσλει Παρκ λόγω έλλειψης προσωπικού αλλά και άλλων θεμάτων. Στις 21 Οκτωβρίου του 1941 ο Τιούριγκ μαζί με τρις συναδέλφους του, ξεπερνώντας την ιεραρχία της Ultra, απευθύνει επιστολή στον Τσώρτσιλ ζητώντας την με κάθε τρόπο αύξηση της υπολογιστικής ικανότητας των ομάδων στο Μπλετσλει Παρκ. Η επιστολή έγινε δεκτή από τον πρωθυπουργό με την εντολή ΕΝΕΡΓΕΙΑ ΣΗΜΕΡΑ (ACTION THIS DAY Make sure they have all they want on extreme priority and report to me that this had been done). Μετά την προσωπική παρέμβαση του Τσώρτσιλ τα προβλήματα λύθηκαν. Προσλήφθηκαν πολλές γυναίκες χειρίστριες -ας μην ξεχνάμε άλλωστε ότι οι άντρες ήταν στον πόλεμο - και οι ελάχιστοι άνδρες που ήταν απαραίτητοι παρέμειναν εκεί και δεν μετακινήθηκαν στην πρώτη γραμμή. Κατασκευάστηκαν πολλές νέες μηχανές Bomba, τουλάχιστον διακόσιες μηχανές ήταν σε λειτουργία, ενώ το προσωπικό που τις λειτουργούσε και επεξεργαζόταν τα αποτελέσματά τους είχε φτάσει σε κάποιες χιλιάδες άτομα εργαζόμενα όλο το εικοσιτετράωρο. Υπολογίζεται ότι πάνω από οκτώ χιλιάδες ήταν μόνο οι γυναίκες εργαζόμενες ποσοστό άνω του 75% του συνολικού προσωπικού.

Ο Τιούριγκ θεωρείται σήμερα μεταξύ άλλων ένας από τους πατέρες της πληροφορικής και ο πατέρας της τεχνητής νοημοσύνης. Το 1950, ο Alan Turing εκδίδει το άρθρο *Υπολογιστικά Μηχανήματα και Νοημοσύνη (Computing Machinery and Intelligence)* στην επιστημονική επιθεώρηση: *Mind.* Το άρθρο ξεκινάει με "Το Παιχνίδι της Μίμησης" (The Imitation Game), γνωστό ως "Turing Test". Το περίφημο Τεστ του Τιούριγκ είναι αυτό που επιτρέπει να συμπεράνει ένας τρίτος εάν μέσα σε ένα κλειστό θάλαμο βρίσκεται μια μηχανή ή ένας άνθρωπος.

Το αρχικό έργο που τον καθιέρωσε αφορά κυρίως τη λογική. Πιο συγκεκριμένα, στη δεκαετία του 1920, ο διάσημος Γερμανός μαθηματικός Hilbert έθεσε το πρόβλημα αποκρισιμότητας (decidability) της κατηγορηματικής (πρωτοβάθμιας) λογικής (Entscheidungsproblem): *Υπάρχει μηχανική διαδικασία (αλγόριθμος) που να μας επιτρέπει να αποφασίσουμε (σε πεπερασμένο αριθμό βημάτων) εάν μια οποιαδήποτε πρόταση της κατηγορηματικής λογικής είναι αποδείξιμη (ή όχι);* Το 1936, ο Turing – και ανεξάρτητα από αυτόν ο Church - έλυσαν το πρόβλημα αρνητικά με τη βοήθεια μαθηματικών εννοιών που περιέγραψαν - την μέχρι τότε μη τυπικά ορισμένη - έννοια της μηχανικής (αλγοριθμικής) διαδικασίας. Οι εργασίες

και των δύο συγγραφέων έχουν επηρεαστεί από το θεώρημα του Gödel, ειδικά δε από την κωδικοποίηση του συντακτικού με σκοπό την αναγωγή της λογικής στην αριθμητική. Ο Turing όρισε την έννοια της υπολογισιμότητας μέσω αφηρημένων μηχανών (Turing machines) και υποστήριξε πως κάθε αποτελεσματικά υπολογίσιμη αριθμο-θεωρητική συνάρτηση (effectively calculable number-theoretic function) είναι υπολογίσιμη με τη βοήθεια μιας τέτοιας μηχανής. Κάθε πρόγραμμα υπολογιστή μπορεί δηλαδή να περιγραφτεί με τη βοήθεια μιας μηχανής Turing. Ας σημειωθεί ότι όταν δημοσιεύτηκε η εργασία του δεν είχαν κατασκευαστεί οι ηλεκτρονικοί υπολογιστές.

Η κρυπτογραφική μηχανή SZ40 της Γερμανικής εταιρείας Lorenz χρησιμοποιήθηκε για πρώτη φορά το 1940 ως η τελευταία λέξη της τεχνολογίας των κρυπτογραφικών μηχανών της εποχής. Διέθετε 12 κρυπτογραφικούς κυλίνδρους και είχε σημαντικό πλεονέκτημα έναντι του Enigma διότι απαιτούσε μόνο ένα χειριστή – σε αντίθεση με το Enigma που απαιτούσε τρεις (δακτυλογράφο, αντιγραφέα, ασυρματιστή). Η ευκολία χειρισμού αυτής της μηχανής την έκανε ιδιαίτερα δημοφιλή στο Γερμανικό στρατό με αποτέλεσμα ένα μεγάλο μέρος των επικοινωνιών να εκτελούνται από αυτή με το Enigma να χάνει έδαφος. Το σπάσιμο του κώδικά της ήταν λοιπόν ζωτικής σημασίας και έπρεπε να γίνει το συντομότερο δυνατό. Για χάρη χιούμορ/αστειότητας τα σήματα του SZ40 είχαν το ψευδώνυμο Tunny (από το ψάρι τόνος), καθότι όλα τα σχετικά μηνύματα οι Βρετανοί του Μπλέτσι Παρκ τα ονόμαζαν ψάρια (Fish). Ο κώδικας που έπρεπε να σπάσει ήταν πολύ πιο σύνθετος από το Enigma και όπως έδειξε η ιστορία στρατηγικά πολύ πιο σημαντικός. Ο Tunny χρησιμοποιούσε τον κώδικα Baudot και ένα είδος τηλε-εκτυπωτή σε αντίθεση με τον Enigma που χρησιμοποιούσε τον κώδικα Μορς. Ο Χίτλερ θεωρούσε άσπαστο το σύστημα αυτό και γι αυτό εμπιστευόταν τις πιο ευαίσθητες πληροφορίες του. Χρησιμοποιείτο έτσι για τις επικοινωνίες του ίδιου και των ανώτερων διοικητών σε αντίθεση με το Enigma που χρησιμοποιείτο μεταξύ στρατιωτικών σχηματισμών, πλοίων και υποβρυχίων.

Για την επίτευξη του δύσκολου εγχειρήματος της κατανόησης αυτού του κώδικα, μετά και από σύσταση του Turing, προσλήφτηκε στο Μπλέτσει Παρκ ο

μαθηματικός Bill Tutte ο οποίος μαζί με τον περίφημο κρυπταναλυτή συνταγματάρχη Τζον Τιλμαν έσπασαν τον κώδικα. Μετά από μήνες ανεπιτυχώς προσπαθειών το νήμα άρχισε να ξετυλίγεται από τις 30 Αυγούστου του 1941 όταν ένας Γερμανός χειριστής, σε αντίθεση με όλους τους κανονισμούς, έστειλε το ίδιο μήνυμα δύο φορές με τις ίδιες ρυθμίσεις. Για την ακρίβεια, το σώμα του δεύτερου μηνύματος περιείχε συντομογραφίες του πρώτου. Μέσα σε δέκα μέρες ο Τίλμαν είχε καταφέρει να αποκρυπτογραφήσει το συγκεκριμένο μήνυμα χωρίς όμως να προσδιορίσει τον συνολικό μηχανισμό αποκρυπτογράφησης. Αυτό το εξαιρετικά δύσκολο έργο ανατέθηκε στον Μπιλ Τιούτ ο οποίος ολοκλήρωσε επιτυχώς την μαθηματική αναπαράσταση της μηχανής και της λειτουργίας της σε διάστημα λίγων εβδομάδων. Το έργο ήταν εξαιρετικά δύσκολο διότι οι Βρετανοί δεν είχαν στα χέρια τους καμία μηχανή τέτοιου τύπου και έτσι όλα έπρεπε να γίνουν μόνο με διαίσθηση και μαθηματικά. Οι αλγόριθμοι του Τιούτ, όμως, για να είναι χρήσιμοι έπρεπε να εκτελούνται σε σχετικά σύντομο χρονικό διάστημα. Η κρυπτογράφηση αυτή ήταν συμμετρικού κλειδιού και βασιζόταν σε ένα συνδυασμό με τη βοήθεια της Μπουλιανής αποκλειστικής διάζευξης (XOR) του κώδικα Vernam, μέσω του οποίου παραγόταν ένας ψευδοτυχαίος αριθμός, από ένα απλό κείμενο.

Ο κώδικας έπρεπε να σπάει καθημερινά και σε μικρό χρονικό διάστημα για να είναι χρήσιμος και να μπορούν στη συνέχεια οι πληροφορίες να αναλυθούν και να αξιοποιηθούν περεταίρω. Έτσι, η ομάδα του Μπλέτσλει Παρκ, αξιοποιώντας και παλαιότερες προτάσεις του Τιούριγκ προς τον Τσώρτσιλ («χρειαζόμαστε τρόπους ώστε να μπορούμε να κάνουμε πολύ γρήγορα τους υπολογισμούς») σχεδίασε και έθεσε σε λειτουργία τον πρώτο στον κόσμο προγραμματιζόμενο ηλεκτρονικό υπολογιστή τον Colossus. Για την ακρίβεια κατασκεύασε και έθεσε σε λειτουργία δέκα υπολογιστές αυτού του τύπου με τη συνδρομή των Βρετανικών ταχυδρομείων και του μηχανικού τους Τόμι Φλόρενς που ήταν και ο δημιουργός του. Η σημασία της δουλειάς των Τίλμαν και Τιούτ είναι τεράστια καθότι οι σύμμαχοι είχαν πρόσβαση στις πληροφορίες και τις επικοινωνίες σε κορυφαίο επίπεδο. Πολλοί θεωρούν βάσιμα ότι αυτό ήταν σημαντικότερο από το σπάσιμο του Enigma, πολύ πιο δύσκολο και με σημαντικότερες συνέπειες στην τελική έκβαση των μαχών καθότι έδωσε πρόσβαση και στις επικοινωνίες του ίδιου του Χίτλερ και του ανώτατου επιτελείου. Μετά το τέλος του πολέμου ο Bill Tutte πήγε στο Καίμπριτζ

όπου ολοκλήρωσε το διδακτορικό του πάνω στην αλγεβρική θεωρία γραφημάτων, βασικό κλάδο των μαθηματικών πληροφορικής σήμερα, εισάγοντας αυτό που ονομάζεται matroid theory. Διέπρεψε στον Καναδά ως καταξιωμένος ειδικός πάνω στα γραφήματα – άρθρα του πάνω στην κατασκευή μη Χαμιλτονιανών γραφημάτων, αλλά και στον χαρακτηρισμό γραφημάτων θεωρούνται πια κλασσικά.

Η επιχείρηση Ultra σύμφωνα με τους ιστορικούς περιόρισε τη διάρκεια του πολέμου κατά δύο τουλάχιστον χρόνια, άλλοι υποστηρίζουν κατά τέσσερα. Εκατομμύρια άνθρωποι σώθηκαν. Παρότι ο πόλεμος δεν κερδήθηκε αποκλειστικά από την Ultra - πως θα μπορούσε άραγε; - η συμβολή της ήταν αποφασιστικής σημασίας. Χωρίς αυτούς τους αφανείς ήρωες η νίκη δεν ήταν καθόλου δεδομένη. Ήρωες που δεν τιμήθηκαν ποτέ γιατί οι δράσεις τους παρέμειναν μυστικές για πολλά χρόνια. Έχουν όμως ανάγκη από τιμή οι ήρωες; Νομίζω είναι ανάγκη ημών να τους τιμήσουμε και όχι δική τους. Είναι ανάγκη και καθήκον η διατήρηση της μνήμης όσων κέρδισαν την ελευθερία μας από τον Ναζισμό και τον Φασισμό. Και είναι ανάγκη στη μνήμη αυτή να περιληφθούν όχι μόνον οι οπλισμένοι μαχητές αλλά και οι στρατευμένοι επιστήμονες, οι φωτισμένοι μαθηματικοί της εποχής εκείνης. Δεν θυσιάστηκαν μεν οι ίδιοι, έσωσαν όμως τις ζωές πολλών άλλων.