كسر شفرة الانجما

استمرت عمليات التقاط الرسائل والاتصالات الألمانية بواسطة إدارة تحليل الشفرة البريطانية (الغرفة ٤٠) وسائر أجهزة المخابرات الغربية فى أوربا بعد انتهاء الحرب العالمية الأولى . وفى ١١٩٢٦ لوحظ التقاط رسائل ألمانية مشفرة بدرجة عالية من الصعوبة وغير قابلة للكسر وكان ذلك نذير وصول الانجما والتوسع فى استخدامها على مستوى الاتصالات الألمانية كافة . واعتبرت الانجما فى ذلك الوقت الآلة الألمانية المعجزة التى يستحيل كسر شفرتها .

وتضافرت جهود عدة دول منها أمريكا وفرنسا وبريطانيا فى محاولات لكسر هذه الشفرة وانتهت كلها باليأس . إلا أن جهود دولة أصغر ولكن أكثر عرضة للخطر كانت أكثر جدية وبالتالى أثمرت عن نتائج مفيدة وهذه الدولة هى بولندا التى كانت واقعة تحت إحساس بالخوف من الغزو الألمانى لها مما دفعها إلى أن تكون أكثر جدية واهتمام من غيرها .

وكان مكتب الشفرة البولندى التابع للدولة Biuro Szyfróws هو المسئول الأول عن هذه الجهود وبدأ النجاح البولندى فى هذا الشأن بعد حصول المكتب على معلومات غاية فى الأهمية وصلت عن طريق التعاون المخابراتى مع فرنسا وكان مصدرها الجاسوس الألمانى هانز شميدت Hans Thilo Schmidt الذى جند بواسطة المخابرات الفرنسية مقابل المال وفى ١٩٣١/١١/٨ سمح شميدت لضابط المخابرات الفرنسى أن يقوم بتصوير تقريرين فى غاية الأهمية عن كيفية تصميم الانجما ومكوناتها وكيفية عملها مقابل عشرة آلاف مارك ألمانى . وقد تمكن شميدت من توفير هذه التقارير من خلال عمله فى إدارة مكتب الاتصالات الألمانية ببرلين وهو الجهة المسئولة عن الانجما .

وقد حاولت المخابرات الفرنسية بعد حصولها على هذين التقريرين أن تقوم ببناء نموذج فعلى لآلة الانجما إلا أن ذلك لم يكن كافياً لفك شفرتها لأن تشغيل هذه الآلة يعتمد على إدخال قيم أولية بدونها لا يمكن التعرف على شفرتها (Setting values) ، لأنه بناء على هذه القيم يتم وضع الآلة فى وضع بداية التشغيل والذى سيترتب عليه كافة حساباتها التالية .

وانتهى الأمر إلى قيام المخابرات الفرنسية وفى إطار التعاون المخابراتى مع بولندا إلى تسليم التقريرين الألمانيين المخابرات البولندية والتى بدأ منهما عملها الجاد فى محاولة التعرف على القيم الأولية لتشغيل الانجما .

وتتكون القيمة الأولية للانجما من ثلاثة عناصر هى :

١ – قيم لوحة مفاتيح الأحرف Plugboard setting .

٢ – ترتيب الخلاطات Scramblers arrangement .

٣ – توجيه الخلاطات Scramblers orientation .

والعنصر الأول يعنى أن لوحة مفاتيح الإدخال يمكن أن تتغير قيمة بعض الأحرف التى بها من خلال توصيلات معينة تتم بالآلة فيمكن مثلا عند ضرب الحرف A يعطى القيمة L والحرف P يعطى القيمة R ، وعليه فإن هذا العنصر الأول يتم وصفه كالتالى :

A/L P/R T/D

والعنصر الثانى قد يأخذ الشكل التالى ٢ – ٣ – ١ ويعنى أن ترتيب الخلاطات الثلاثة داخل الانجما سيكون كالتالى الثانى ثم الثالث ثم الأول . والعنصر الثالث قد يأخذ الشكل CQW ويعنى أن الوضع الأول للخلاط الأول سيكون حرف C والوضع الأول للخلاط الثانى سيكون حرف Q والوضع الأول للخلاط الثالث سيكون حرف W وعليه فإن القيمة الأولية للانجما طبقاً للمثال السابق ستكون :

A/L	P/R	T/D
2	3	1
C	Q	W

وتسمى هذه القيمة بمفتاح اليوم Day - Key مما يعنى أنها تتغير يوميا لمنع أى جهة من التعرف عليها بسهولة وبالطبع يجب أن يكون مفتاح اليوم معروف لدى الراسل والمستقبل بحيث يجب أن تكون الانجما الراسلة والانجما المستقبلة على نفس قيم بدء التشغيل حتى يمكن تحقيق الاتصال السليم .

وقد استطاع عالم الرياضيات البولندى الفز ماريان رويسكى Marian Rejewsi تحليل ترتيب حركة الخلاطات بالانجما واستطاع هو وفريق العمل المصاحب له فى المخابرات البولندية إعداد كتالوج كامل لمختلف أوضاع خلاطات الانجما وبلغ عددها ١٠٥٤٥٦ وضع كما استطاع تصميم آلة تتولى حساب مفتاح اليوم المستخدم فى اتصالات الانجما وسميت هذه الآلة Bombs . إلا أن الجانب الألمانى لم يقف ساكنا وأجرى تعديلات على الانجما وأضاف عليها خلاطات جديدة للأحرف مما زاد من صعوبة كسر شفرتها بدرجة عالية جداً . وعند هذه اللحظة وصلت الجهود البولندية إلى منتهاها وقررت بولندا تسليم ما وصلت إليه من نتائج إلى مخابرات صديقة واختارت جهازى المخابرات الفرنسى والبريطانى ، وكانت احتمالات الخطر تتزايد والحرب العالمية الثانية على الأبواب ، وبعد أسبوعين بالضبط من نجاح تهريب

الجهود البولندية فى فك شفرة الانجما إلى البريطانيين والفرنسيين غزا هتلر بولندا وبدأت الحرب العالمية الثانية .

❁ ❁ ❁

أظهر الإنجاز البولندى فى كسر شفرة الانجما الألمانية للحلفاء الغربيين أهمية إضافة عنص خبراء الرياضيات Mathematicians إلى فريق العمل الموكل لها هذه المهام .

وكانت الغرفة ٤٠ فى بريطانيا مسيطراً عليها بواسطة علماء اللغات إلا أن الأمور تغيرت وبدء تطعيمها بعلماء الرياضة فى حملة كبيرة لتجنيد الأفراد . وبدء تجميع الأفراد الجدد فى مزرعة بلتشلى Beltchley Park خارج لندن فى مقاطعة بكنجهام شاير حيث مقر إدارة الشفرة الحكومية والتى سميت وقتها GC & CS Government Code & Cipher School وتم تقسيم الموقع الجديد لتغطية مختلف الاتصالات التى تلتقطها أجهزة المراقبة البريطانية .

وبدأت مرحلة جديدة من الجهود المضنية فى بلتشلى بارك لفك شفرة الانجما معتمدة على ما حصلت عليه من إنجازات بولندية مع إضافة إمكانات بريطانيا عليها وهى بالطبع أكبر من بولندا فى ذلك الوقت .

وكان العمل اليومى يسير على وتيرة واحدة ففى منتصف كل ليلة يقوم الألمان بتغيير مفتاح اليوم لشفرة الانجما مما يعنى أن مجهودات اليوم السابق أصبحت بلا فائدة بالنسبة لاتصالات اليوم الجديد ويجب البدء فوراً فى محاولة التعرف على مفتاح اليوم الجديد وكان هذا المجهود يستلزم من خمسة إلى ستة ساعات .

وكان من أبرز العاملين فى هذا الفريق عالم الرياضيات آلان تورنج Alan Turing والذى اعتبرت أعماله بداية الطريق نحو إنشاء الحاسب الآلى المبرمج بمفهومه الحاضر .

وقد استطاع تورنج اكتشاف نقاط ضعف الانجما من خلال ربطه لعدة وحدات من آلة الانجما على التوالى واستنبط دائرة كهربائية سميت باسمه Turing Loop. اعتمد عليها فى إدخال حرف من النص الواضح على الآلة الألى من الترتيب التسلسلى لكى تعطيه الآلة الثالثة أو الرابعة الحرف الشفرى المقابل له .

وكان إنجاز فريق مزرعة بلتشلى عظيما لدرجة أن رئيس وزراء بريطانيا فى ذلك الوقت ونستون تشرشل قام بزيارتهم تكريما لهم . وتردد بعض المراجع التاريخية أن إنجاز فريق مزرعة بلتشلى فى كسر شفرة الانجما كان العامل الحاسم فى انتصار

الحلفاء فى الحرب العالمية الثانية وأنه لولا هذا الإنجاز لكانت الحرب ستستمر إلى ١٩٤٨ بدلاً من أن تنتهى فى ١٩٤٥ وما قد يصاحب ذلك من تغيرات .

وبعد انتهاء الحرب تغير اسم الموقع إلى GCHQ Goverment Communications Head Quarter «قيادة الإتصالات الحكومية» وتم نقله إلى شلتنهام .