Turing e a Enigma

António Machiavelo e Rogério Reis
Departamentos de Matemática e de Ciência dos Computadores
Faculdade de Ciências da Universidade do Porto
e-mails: ajmachia@fc.up.pt e rvr@dcc.fc.up.pt

Resumo: Neste artigo, depois de fazer uma descrição da máquina criptográfica Enigma usada pelas tropas alemãs na segunda guerra mundial, apresenta-se alguma da história sua criptanálise, que envolve ideias atribuídas a Alan Turing.

Abstract: After describing the cryptographic machine known as Enigma, which was used by the Germans in the second world war, some of its cryptanalysis is presented, which include ideas attributed to Alan Turing.

palavras-chave: Alan Turing; Enigma; criptanálise.

1 Introdução

A figura de Alan Turing (1912–1954), um dos matemáticos mais brilhantes e originais do século XX, está inegavelmente associada ao ataque à cifra usada pelos militares alemães durante a segunda guerra mundial. Mas o trabalho desenvolvido por toda uma equipa de criptanalistas que incluía Turing e que foi reunida em Bletchley Park, uma propriedade em Milton Keynes, continua, mesmo 65 anos após o fim dessa guerra, debaixo de uma cortina de silêncio imposta pelo governo inglês. Este exacerbado secretismo alimenta as contradições e confusões sobre esse trabalho — mesmo por aqueles que lá estiveram —, impedindo de conhecer o contributo concreto, que se suspeita ser enorme, de Turing, de quem este ano se comemora o centenário.

Neste contexto, pareceu-nos que a homenagem possível nesta área da criptografia, onde o papel de Turing é inegável, seria a da divulgação da história da quebra dos sucessivos modos de utilização da Enigma.

Assim, depois de uns breves rudimentos de criptografia clássica, descrevemos o dispositivo da máquina Enigma e o seu funcionamento, assim com um pouco da sua história. Seguidamente, são expostos os ataques à correspondente cifra durante a guerra civil espanhola; o contributo polaco e a importância do envolvimento da matemática na criptanálise; e por fim alguns dos métodos desenvolvidos em Bletchley Park, onde certamente Turing desempenhou um papel central.

2 Brevíssima introdução à Criptografia

As cifras mono-alfabéticas. O objectivo de uma cifra é o de transformar um texto num outro que não seja fácil de entender sem o acesso a um pedaço de informação a que normalmente chamamos **chave**. Esta transformação pode ir ao ponto de transformar o alfabeto usado na mensagem original num outro, apesar de, pelas evidentes razões práticas, na maioria das vezes se optar por utilizar o mesmo alfabeto em ambos os textos, original e cifrado. A mais simples família de cifras é formada por funções que fazem corresponder a cada carácter de um alfabeto um outro carácter do mesmo conjunto de símbolos. Como o objectivo, para além de esconder o texto original, cifrando-o, é também poder decifrá-lo por aqueles que conheçam o "segredo", estas transformações têm que ser injectivas, ou seja permutações. As cifras mono-alfabéticas são, portanto, permutações do alfabeto.

Às primeiras cifras correspondiam permutações simples: deslocamentos circulares do alfabeto de um dado número de posições. É a chamada cifra de César. A tabela que segue exemplifica uma destas cifras.

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
d e f g h i j k l m n o p q r s t u v w x y z a b c
```

O acto de cifrar corresponde a substituir cada letra do texto original usando a correspondente na segunda linha da tabela acima. É fácil de ver que o esforço necessário para quebrar uma mensagem assim cifrada é muito pequeno. Bastam, no máximo, 25 tentativas para recuperarmos o texto original. Neste caso o ataque a esta cifra a que normalmente chamamos de ataque de "força bruta" consiste em testar sucessivamente **todas** as chaves possíveis, que, no caso, são os 25 possíveis deslocamentos do segundo alfabeto.

Uma solução para esta "fraqueza" intrínseca da cifra será aumentar significativamente o número de chaves. Podemos para isso tomar uma ordem qualquer, para o segundo alfabeto, e não somente uma permutação circular do primeiro.

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
m f u r j k q a x d y p v z t c e l n i w b g h o s
```

Um ataque de "força bruta" a esta cifra envolve agora $26! - 1 = 403291461126605635583999999 \approx 4 \times 10^{26}$ tentativas, o que parece ser suficientemente seguro. Mas aqui entra em campo a Criptanálise. Um criptograma (mensagem cifrada) com esta cifra, parece-nos uma sequência aleatória de caracteres. Mas será mesmo assim? Como observou o matemático

árabe do século IX, al-Kindi[1], ao longo de todo o criptograma cada letra do texto original é sempre cifrada da mesma forma. Por exemplo, e com a chave acima, a letra `A` é sempre transformada num `m`, e a letra `X` num `h`. Como a letra `A` ocorre muito mais vezes, nas mensagens escritas em português, do que a letra `X`, isso vai significar que a letra `m` vai ocorrer muito mais frequentemente que a letra `h` nos criptogramas correspondentes. Esta observação, permite uma criptanálise muito eficiente a este tipo de cifras. Dado um criptograma, construímos a tabela de frequências relativas dos caracteres da língua em que a mensagem foi escrita. Agora dirigimos a pesquisa da chave fazendo corresponder as frequências encontradas no criptograma com as frequências médias de cada carácter na língua original, no português por exemplo. Ainda que a semelhança das frequências de cada carácter no criptograma e da respectiva frequência média possa conter algumas variações significativas, em especial se o criptograma for pouco extenso, este método permite reduzir drasticamente o espaço de procura de chaves, tornando o ataque a este tipo de cifra relativamente fácil.

As cifras poli-alfabéticas. A solução para dificultar este tipo de ataques baseados no estudo das frequências de ocorrência dos caracteres nos criptogramas, passa por encontrar cifras que não cifrem sempre da mesma forma cada uma das letras do texto original. Começou-se por utilizar duas cifras mono-alfabéticas, e cifrar cada uma das letras, alternadamente, com uma e outra cifra. Esta é a solução de B. Alberti (1404–1472). Mas é fácil perceber que se calcularmos independentemente, as frequências relativas dos caracteres em posições de ordem ímpar e os caracteres em posições de ordem par, voltamos a ter frequências que devem ser aproximações das frequências médias dos caracteres na língua original. O processo apenas duplica o trabalho necessário para um ataque, o que é muito pouco.

Levando mais longe esta tentativa de complicar estas cifras, a chamada cifra de Vigenère[2], em vez de duas cifras mono-alfabéticas, usa ciclicamente cifras de uma sequência de cifras de César. Esta nova cifra, que foi entusiasticamente denominada como "le chiffre indéchiffrable", vem, apesar disso, a ser quebrada no século XIX por C. Babbage (1791–1871). O que ele observa é que o período da cifra, o tamanho da sequência de cifras de César

[1] Abu Yūsuf Ya'qūb ibn 'Isḥāq aṣ-Ṣabbāḥ al-Kindī (c. 801–873), de facto
أبو يوسف يعقوب بن إسحاق الصباح الكندي

[2] Que se deve aos trabalhos de J. Trithemius (1462–1516), G. Porta (1535–1615) e B. Vigenère (1523–1596).

usadas, pode ser facilmente determinado, e portanto, é possível proceder-se a um ataque estatístico, inteiramente análogo ao que se fez para a cifra de Alberti, apesar de com um esforço proporcional ao tamanho do referido período.

Os dispositivos criptográficos. Claro que outras soluções podem ser aplicadas para resolver as debilidades das cifras mono-alfabéticas, assim como das cifras poli-alfabéticas, mas o resultado será sempre a adopção de cifras cada vez mais complicadas e portanto susceptíveis de erros de operação. Outras soluções foram propostas, como a cifra poligráfica Playfair, que imediatamente foram descartadas pela alegada dificuldade de treinar operadores de cifra que as pudessem utilizar. A utilização militar com sucesso de uma cifra pressupõe que se possam treinar rapidamente operadores, não necessitando de dar grandes pormenores de como a cifra funciona[3], para que no campo de operações as mensagens possam ser transmitidas de forma (relativamente) célere e sem grandes taxas de erro. É desta necessidade, de automatizar a "complicação" da cifra, que nascem os dispositivos criptográficos electromecânicos no início do século XX. De qualquer forma é importante notar que estes dispositivos, ainda que constituam uma parte fundamental das cifras que neles se baseiam, **não são em si mesmo a cifra**. Desta faz parte integrante a forma como é gerada a chave, e o processo de sincronização da chave entre o emissor e o receptor de cada mensagem então cifrada.

3 A Enigma

Em 1918, o engenheiro electrotécnico alemão Arthur Scherbius (1878–1929) inventa um dispositivo electromecânico de cifra, que só virá a ser comercializado a partir de 1923, com o nome de «Enigma». A máquina irá ser remodelada por diversas vezes[4], vindo a sua versão D a ser usada, a partir de 1927, para fins comerciais, diplomáticos e militares. Em particular, a Enigma D foi usada na guerra civil espanhola e versões um pouco mais sofisticadas foram usadas por várias unidades do exército, da força aérea e da marinha alemãs durante a segunda guerra mundial.

[3]Como se verá a seguir, pode ser elevado o preço a pagar por este pressuposto, que é mais seguro treinar operadores mais ou menos ignorantes em criptografia, em vez os formar (ainda que rudimentarmente) na cifra que estão a usar.

[4]Ver `http://www.cryptomuseum.com/crypto/enigma`.

Nas versões militares alemãs, a máquina Enigma tinha um teclado, um quadro luminoso de letras dispostas pela mesma ordem que nas teclas, um painel de trocas (*plugboard*) e uma unidade de permutação do texto. Esta unidade de permutação consistia de terminais de entrada e saída, de três ou quatro rotores e de um reflector — ver Figura 1, uma fotografia[5] de uma máquina Enigma com a tampa superior aberta. Os rotores, componentes

Figura 1: Máquina Enigma, versão militar

fundamentais da Enigma, eram cilindros contendo 26 contactos eléctricos em cada face e um conjunto de ligações internas que ligam cada contacto de uma face a um outro contacto da face oposta. Se nomearmos cada um desses contactos em cada face como `A`, `B`,..., `Z`, cada rotor corresponde à materialização de uma cifra mono-alfabética, ou seja corresponde a uma permutação do alfabeto $\{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Y}, \mathtt{Z}\}$. Por sua vez, o reflector era um cilindro contendo contactos eléctricos numa só face, ligados aos pares, de modo que a permutação por ele induzida se pode escrever como um produto de 13 transposições disjuntas.

Por exemplo, as permutações induzidas pelos 5 rotores usados pelo exér-

[5]Retirada de `http://www.ieeeghn.org/wiki/images/7/72/Enigma00.jpg`).

cito alemão eram, quando escritas como produto de ciclos disjuntos[6]:

$$\begin{aligned}
\text{rotor I} &= (\texttt{AELTPHQXRU})(\texttt{BKNW})(\texttt{CMOY})(\texttt{DFG})(\texttt{IV})(\texttt{JZ})(\texttt{S})\\
\text{rotor II} &= (\texttt{A})(\texttt{BJ})(\texttt{CDKLHUP})(\texttt{ESZ})(\texttt{FIXVYOMW})(\texttt{GR})(\texttt{NT})(\texttt{Q})\\
\text{rotor III} &= (\texttt{ABDHPEJT})(\texttt{CFLVMZOYQIRWUKXSG})(\texttt{N})\\
\text{rotor IV} &= (\texttt{AEPLIYWCOXMRFZBSTGJQNH})(\texttt{DV})(\texttt{KU})\\
\text{rotor V} &= (\texttt{AVOLDRWFIUQ})(\texttt{BZKSMNHYC})(\texttt{EGTJPX}).
\end{aligned}$$

Dois reflectores comuns eram os seugintes:

$$\begin{aligned}
\text{reflector B} &= (\texttt{AY})(\texttt{BR})(\texttt{CU})(\texttt{DH})(\texttt{EQ})(\texttt{FS})(\texttt{GL})(\texttt{IP})(\texttt{JX})(\texttt{KN})(\texttt{MO})(\texttt{TZ})(\texttt{VW})\\
\text{reflector C} &= (\texttt{AF})(\texttt{BV})(\texttt{CP})(\texttt{DJ})(\texttt{EI})(\texttt{GO})(\texttt{HY})(\texttt{KR})(\texttt{LZ})(\texttt{MX})(\texttt{NW})(\texttt{TQ})(\texttt{SU}).
\end{aligned}$$

Quando uma tecla da Enigma é pressionada, o primeiro rotor (que ficava do lado direito da máquina) avança uma posição e, de seguida, o circuito eléctrico é accionado, passando a corrente sucessivamente pelo painel de trocas, depois pelos rotores, da direita para a esquerda, após o que passa pelo reflector, regressando depois novamente pelos rotores, mas agora da esquerda para a direita, após o que vai novamente ao painel de trocas, e finalmente ao quadro luminoso onde se acende a lâmpada correspondente à letra que, nessa configuração específica da Enigma, cifra a letra cuja tecla foi pressionada. O facto de o reflector efectuar uma permutação que é involutiva[7], resulta do modo como a Enigma funciona que a permutação final, ou seja a permutação induzida pela Enigma, é também uma involução. Isto é importante, pois para decifrar uma mensagem basta então fazer passar o criptograma pela Enigma, começando exactamente com a mesma configuração dos rotores e painel de trocas com que se iniciou a cifração da respectiva mensagem.

Convém realçar que para decifrar uma mensagem cifrada pela Enigma não basta ter uma máquina. É necessário saber a configuração inicial com que a mensagem foi cifrada! A chave da cifra dada por uma máquina Enigma consiste assim nessa configuração inicial, a saber: quais os rotores, qual a sua posição inicial e quais as ligações do painel de trocas. Observe-se que os rotores eram intermutáveis e, no caso do exército, chegaram a ser 3 de um

[6]Relembramos que qualquer permutação se pode decompor como um produto de ciclos disjuntos de uma só maneira (a menos da ordem, que é irrelevante pois ciclos disjuntos comutam) — ver capítulo VI de [1] —, e que a notação $(abc\ldots)$ denota uma permutação que envia a em b, envia b em c, etc...

[7]Uma aplicação μ diz-se uma involução quando satisfaz $\mu^2 = I$, onde $\mu^2 = \mu \circ \mu$, e I denota a identidade, ou seja quando, sendo uma permutação sobre um conjunto finito, a sua decomposição em ciclos disjuntos contém apenas ciclos de tamanho 1 e 2.

conjunto de 5 (os que acima ficaram descritos), enquanto que na marinha chegaram a ser 3 de um total de 8. A partir de 1 de Fevereiro de 1942, a marinha introduz uma Enigma com 4 rotores para as comunicações com os submarinos.

O movimento dos rotores funciona quase como o odómetro de um automóvel. Quando o rotor da direita dá uma volta completa, contada a partir de um certo ponto, o segundo rotor avança uma posição e quando este dá uma volta completa, então o terceiro avança uma posição. Mas, contrariamente ao que acontece num odómetro, o ponto em que um dado rotor avança pode ser alterado, pois cada rotor contém um anel exterior que pode ser rodado livremente, sendo depois fixado com uma cavilha (ver a figura 2)[8]. Estes

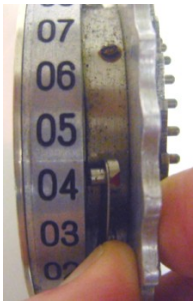


Figura 2: Cavilha de fixação do anel exterior

anéis continham, na sua superfície exterior, os números de 01 a 26, ou as letras de `A` a `Z`, e tinham um entalhe que era mecanicamente responsável pelo avanço do rotor. Em particular, a posição destes anéis relativamente ao cilindro central do rotor é também um dos elementos da chave que é necessário saber para decifrar uma mensagem.

Portanto a "chave" que tem que ser "partilhada" pelo emissor e o receptor, por forma que uma mensagem possa ser transmitida e depois lida, consiste na escolha dos rotores a colocar na máquina (caso o conjunto de rotores disponível seja maior que o número de rotores usado no dispositivo), a ordenação destes rotores, o posicionamento de cada anel externo (que tem inscritos os símbolos que identificam a posição do rotor assim como o ponto de avanço do rotor seguinte) relativamente ao núcleo do mesmo rotor, a posição inicial dos rotores e finalmente a configuração do painel de trocas (caso este exista). Estas são todas as configurações que têm que coincidir

[8]Há uma outra diferença, o chamado *avanço-duplo*, que aqui ignoramos — ver `http://users.telenet.be/d.rijmenants/en/enigmatech.htm#rotors` para uma descrição detalhada acompanhada de excelentes imagens, e de onde a da Figura 2 foi retirada.

nos dispositivos do emissor e do receptor. Se todos eles constam das instruções fixadas para o dia, ou se alguns são arbitrados pelo operador-emissor e de alguma forma enviados com a mensagem, constituí o que se costuma chamar *o modo de operação* do dispositivo.

Durante uma boa parte da segunda guerra mundial (as coisas eram mais simples na guerra civil espanhola, como adiante veremos, e mais complicadas em finais da segunda guerra mundial), a cada operador da Enigma no exército alemão era fornecida uma lista de chaves para um certo período (e.g. um mês). Cada chave era utilizada durante um dia, das 00h00 às 24h00. Esta lista continha cinco parâmetros de inicialização da Enigma[9]:

1. a data;
2. a ordem dos rotores (por exemplo: V, IV, I);
3. a posição dos anéis exteriores relativamente ao cilindro central dos rotores, ou seja, a posição das cavilhas (por exemplo, 19, 05, 23);
4. as ligações no painel de trocas (por exemplo, `BZ DT EG FJ HI KP LT MX OY QR`);
5. o discriminante (for exemplo, `QXT`) — este era usado para o operador identificar, aos destinatários pretendidos, a chave que estava a usar. Os discriminantes não terão nenhum papel na discussão que se segue.

No exemplo dado, o operador pegaria no rotor V e rodaria o seu anel exterior por forma a que o número 19 (letra `S`) ficasse alinhado com uma certa na marca no rotor, fixando o anel nessa posição com a cavilha. O mesmo seria feito para o rotor IV e II, colocando os respectivos anéis nas posições 5 (letra `E`) e 23 (letra W). Depois o operador colocaria os rotores no eixo em torno do qual se movem, de modo a que o rotor V ficasse à esquerda, o rotor IV no meio e o I na direita. Poderia agora fechar a tampa da máquina. De seguida, faria as ligações indicadas no painel de trocas, ligando o `B` ao `Z`, o `D` ao `T`, etc.

Num dos modos de operação usado durante a segunda guerra, o operador tinha agora de escolher três letras aleatoriamente (de preferência!), digamos `QAY`, que constituem o que aqui chamaremos **primeiro indicador** (*indicator setting*). Rodaria os rotores de modo a essas letras serem visíveis nas respectivas ranhuras. Finalmente, o operador teria de escolher outras três letras ao acaso (de preferência!), por exemplo `MPR`, a que chamaremos **segundo indicador** (*text setting*), carregar nas respectivas teclas

[9] Ver `http://users.telenet.be/d.rijmenants/en/enigmaproc.htm` para mais detalhes e alguns exemplos reais.

(até certa altura este segundo indicador era repetido e cifrado, ou seja, no nosso exemplo, cifrava-se `MPRMPR`) e anotar as três letras (respectivamente, seis) que se acendiam, digamos `WSX`. Finalmente, voltava a colocar os rotores nas posições `MPR`.

Só após todo este procedimento é que a Enigma ficava pronta a cifrar. A mensagem desejada seria então dactilografada, registando-se o respectivo criptograma, que ia aparecendo no quadro luminoso.

No nosso exemplo, as três letras `QAY` seriam enviadas em claro, seguidas das letras `WSX` e do criptograma. O operador destinatário da mensagem teria de efectuar o mesmo procedimento acima descrito para colocar a Enigma na configuração diária. Depois colocaria os rotores nas posições `QAY`, cifrando de seguida `WSX`. Obteria então `MPR`. Colocava então os rotores nas posições `MPR`, dactilografando de seguida o criptograma. Graças ao facto da máquina Enigma ser involutiva, como acima observamos, obteria então a mensagem original.

Deixamos aqui um exemplo, descrito em [14] (p. 36), da forma como uma mensagem Enigma chegaria aos criptanalistas de Bletchley Park, depois de interceptada e tratada pelo serviço britânico de escuta das comunicações alemãs:

Informação dada pelo Operador de Intercepção

a. Frequência: 4760 Quilociclos (KHz)
b. Hora de intercepção: 11:10

Preâmbulo não Cifrado

1. Sinais de chamada: P7J a SF9 e 5KQ
2. Hora de origem: 10:30
3. Número de letras: 114
4. Única ou parte: parte 2 de 4
5. Discriminante: QXT
6. Primeiro indicador: VIN

Texto Cifrado

WQ S EU	PMP I Z	TL J J U	WQEHG	L R B I D
F EWBO	J I EP D	J AZHT	T B J RO	A H HYO
J Y G S F	HYKT N	TDBPH	U LKOH	U N T I M
O F A R L	B P A P M	XKZZX	D T S X L	QWHV L
R A G U Z	Z T S G G	Y I J V		

4 Na Guerra Civil espanhola

Durante a Guerra Civil em Espanha (1938–1939), a Enigma foi utilizada por todas as partes envolvidas no conflito: o governo de Espanha, a Alemanha e Itália que intervieram directamente no derrube da República, assim como a Inglaterra, demasiado preocupada com o rearmamento alemão. Com todos estes intervenientes com dispositivos similares, houve um grande esforço para que fossem descobertos métodos de ataque a estas cifras. Deste esforço resultou que todas as partes conseguiam, regularmente, ler as mensagens cifradas pelos adversários. A versão da Enigma então usada por todos as partes era a mais próxima da versão comercial de Scherbius. Portanto, os dispositivos usados eram compostos por 3 rotores intermutáveis, cujos anéis exteriores se podiam recolocar, mas não há lugar a nenhum painel de trocas, assim como os rotores IV e V ainda não haviam sido introduzidos.

O ataque que passamos a descrever assenta no seguinte conjunto de pressupostos:

- As permutações de cada um dos rotores utilizados são conhecidas. Num conflito deste tipo, a perda e captura de equipamento de comunicações é muito frequente, pelo que tal pressuposto é perfeitamente natural.

- É possível "prever", com alguma certeza, algumas palavras que constam do início da mensagem. Esta é uma premissa que parece mais difícil de garantir para quem não conheça bem as comunicações militares. Mas estas são extremamente formais, contendo sempre a especificação do remetente e destinatário, a data da emissão da mensagem (por extenso) assim como, na maioria das vezes, um conjunto de tratamentos formais mais ou menos constantes. Esta fraqueza das comunicações militares ir-se-á revelar fatal na maioria das cifras usadas no conflito mundial que se seguiu. Estes segmentos de texto cuja existência e localização podemos prever, chamam-se normalmente «cábulas» (em inglês, *cribs*).

Para o que se segue, vamos supor que os dois rotores mais à esquerda, o segundo e o terceiro, não se movem durante a cifra de uma dada cábula. Dado que o segundo rotor só se move uma vez em cada 26 letras, e o terceiro uma vez em cada 26 movimentos do segundo rotor, esta suposição não é assim tão irrealista quanto possa parecer (havendo também métodos para lidar com situações em que ela não se verifica). Então o efeito de transformação destes dois rotores, mais o reflector, durante toda a cifra da cábula é

o de uma cifra mono-alfabética simples. Seja Ψ tal cifra. Como o reflector é uma involução sem pontos fixos (composto somente por pares), Ψ é também uma permutação desse tipo.

O facto de conhecermos uma cábula, digamos $[\varepsilon_i]_i$, e conhecermos a sua posição, suponhamos para simplificar que se encontra na primeira posição, então possuimos um conjunto de pares $(\varepsilon_i, \sigma_i)_i$ em que $\sigma_i = \Sigma_i(\varepsilon_i)$, onde Σ_i representa a cifra mono-alfabética da Enigma na posição i do texto.

Observemos o que acontece com o primeiro carácter, representando por α a permutação induzida pelo primeiro rotor (o da direita) numa dada posição inicial que estamos a testar. A permutação Σ pode ser decomposta explicitando o primeiro rotor e a permutação constante Ψ. Tem-se

$$\begin{aligned} \Sigma_0(\varepsilon_0) &= \sigma_0 \\ \alpha^{-1} \circ \Psi \circ \alpha(\varepsilon_0) &= \sigma_0. \end{aligned}$$

Podemos escrever esta equação de uma forma mais conveniente, compondo α à esquerda de cada um dos membros da equação, e obtemos:

$$\Psi \circ \alpha(\varepsilon_0) = \alpha(\sigma_0).$$

Ou seja, se aplicarmos a permutação do primeiro rotor tanto ao primeiro carácter da cábula como à sua imagem cifrada, obtemos um dos pares que constituem a permutação Ψ. Em geral, para uma qualquer posição i da cábula, temos

$$\Psi \circ \rho^i \circ \alpha \circ \rho^{-i}(\varepsilon_i) = \rho^i \circ \alpha \circ \rho^{-i}(\sigma_i), \tag{1}$$

onde ρ é a permutação correspondente a uma "rotação" do alfabeto de uma letra, ou seja,

$$\rho = (\texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ}).$$

Como sabemos que Ψ é constituída somente por pares, podemos eliminar qualquer posição inicial que conduza a ciclos em Ψ que não tenham este tamanho, ou que conduza a contradições, ou seja, que impliquem que Ψ não é sequer uma função. Só necessitamos de testar 26 posições possíveis para saber qual a posição inicial do primeiro rotor. Caso não saibamos qual é o rotor que foi colocado na primeira posição, este processo tem que ser tentado para cada possível rotor.

Considere-se, por exemplo, que se sabia que numa determinada mensagem o segmento `BOMBARDEODEGUERNICA` foi cifrado em `FYHTRDIMDUXYBSZFZKX`, ou seja que é conhecida a cábula:

```
BOMBARDEODEGUERNICA
FYHTRDIMDUXYBSZFZKX
```

Suponhamos ainda que a mensagem em causa foi cifrada por uma Enigma em que as sucessivas permutações geradas pelo rotor de entrada são:

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

Alguém que interceptasse a mensagem, conhecendo a cábula mas desconhecendo a posição inicial do rotor de entrada, e supondo que a posição inicial desse rotor era a posição 3, usando a equação (1), obteria das primeiras letras da cábula os seguintes pares para a permutação Ψ: (LH) e (WL). Concluiu-se imediatamente que essa não poderia ser a posição inicial desse rotor.

Analogamente, na posição 4 obteria os pares (FP), (RE), (VR); na posição 1, os pares (FM), (QD), (OC), (VL), (ND). Ambas estas posições não poderiam pois corresponder à chave procurada. Repare-se que na posição 0 se obtêm os pares (KG), (XS), (IP), (FA), (FA), $\cdots$, não se obtendo nenhuma contradição, o que indicaria que esta poderia ser a posição inicial em que foi cifrada a mensagem.

Com este método ficamos a saber qual o rotor que está na primeira posição e qual a sua posição inicial. Se tivermos pré-catalogado todas as permutações com dois rotores, podemos agora extrair a configuração inicial e ler a mensagem.

5 Matemáticos polacos

Depois da experiência da utilização da Enigma na guerra civil espanhola, era evidente para todas as partes que esta utilização não era de todo segura. Os criptólogos alemães encontraram um "remendo" para o dispositivo original que os convenceu que este dispositivo poderia passar a ser usado com elevada segurança. Desenharam uma variante da Enigma original, em que cada

circuito correspondente a cada letra podia ser "baralhado" por um *painel de trocas* (*plugboard*), antes e depois do circuito dos rotores ser accionado. Este painel de trocas permite permutar, através da utilização de um cabo duplo, pares de letras. Como se trata de uma permutação contendo somente ciclos de ordem dois (para além das letras que permanecem inalteradas), estamos em presença de mais uma involução. Se a cifra da Enigma sem este painel de trocas for designada por Γ e π a transformação operada por este painel, passamos a ter a seguinte equação de cifra para esta nova Enigma:

$$\sigma = \Sigma(\varepsilon) = \pi \circ \Gamma \circ \pi(\varepsilon).$$

O número de pares permutados pelo painel de trocas variou muito ao longo da sua utilização. Mas se supusermos que o número de cabos a utilizar é fixo, o maior número de combinações é atingido com 11 pares. Para a Enigma sem painel de trocas, as diferentes combinações possíveis correspondem ao número de formas de ordenar os 3 rotores, vezes as diferentes possíveis posições iniciais desses três rotores. Ou seja, $6 \times 26^3 = 105456$. Com a introdução deste painel de trocas, este número ascende para umas exorbitantes 21 676 712 075 158 140 000 diferentes configurações iniciais. Mesmo com a tecnologia digital actual, e supondo que poderíamos testar um milhão de configurações por segundo, seriam necessários mais de meio milhão de anos para testar todas as configurações deste novo dispositivo. Dada a dimensão combinatória envolvida, é natural que os criptólogos alemães tivessem ficado convencidos da robustez deste novo dispositivo, e por isso mesmo tivessem relaxado, de alguma forma, o cuidado na concepção do seu novo modo de operação.

As circunstâncias exactas que levaram o governo polaco a envolver um conjunto de matemáticos nas tarefas de criptanálise nos anos que precederam a invasão da Polónia pelo exército alemão não são completamente claras. Alguns defendem que foi o facto de não haver criptanalistas treinados disponíveis, que os levaram a escolher aqueles que lhes parecia terem as melhores capacidades para rapidamente dominar uma nova área de conhecimento. A verdade é que esta opção, tomada de forma consciente ou não, teve uma imensa importância no desenrolar do ataque à Enigma e consequentemente no desenrolar da própria guerra. Se Marian Rejewski (1905–1980) e os seus companheiros não fossem matemáticos, com natural propensão para ver as cifras da Enigma como permutações, e como tal manipuláveis com todo o arsenal que a Teoria de Grupos lhes fornecia, não seria provável que os criptanalistas polacos pudessem perceber que, apesar da explosão combinatória por si induzida, o painel de trocas não consegue esconder muitas das características da Enigma anterior à sua introdução.

Quando o governo polaco começa a tentar quebrar as mensagens alemãs, o modo de utilização da Enigma é o seguinte: a configuração dos rotores, e a sua ordenação, é fixada por um livro de operação e fica inalterada por 3 meses. O livro de operação estabelece para cada dia qual a posição inicial dos rotores assim como a configuração do painel de trocas. Quando uma nova mensagem deve ser transmitida, o operador escolhe uma nova chave com 3 letras (o que acima se chamou "segundo indicador") e cifra esta nova chave, **duas vezes**, usando a chave do dia (que nesta altura desempenha o papel de primeiro indicador). Depois, usando esta nova chave que acaba de escolher, cifra a mensagem propriamente dita.

Seja $\varepsilon_1\varepsilon_2\varepsilon_3$ a chave escolhida pelo operador para esta mensagem. A messagem cifrada irá então começar pelos seguintes caracteres,

$$\Sigma_1(\varepsilon_1)\Sigma_2(\varepsilon_2)\Sigma_3(\varepsilon_3)\Sigma_4(\varepsilon_1)\Sigma_5(\varepsilon_2)\Sigma_6(\varepsilon_3) = \sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6,$$

em que Σ_i representam as consecutivas permutações da Enigma quando inicializada com a chave do dia. Como a Enigma é, em cada momento, uma involução, sabemos que $\Sigma_1(\varepsilon_1) = \sigma_1$ é o mesmo que $\Sigma_1(\sigma_1) = \varepsilon_1$. Não podemos directamente usar este facto porque não conhecemos ε_1, mas podemos concluir que

$$\sigma_4 = \Sigma_4(\varepsilon_1) = \Sigma_4(\Sigma_1(\sigma_1)) = \Sigma_4 \circ \Sigma_1(\sigma_1).$$

Coligindo um número suficiente de mensagens durante o dia (algumas dezenas) podemos assim reconstruir os ciclos que caracterizam a permutação $\Sigma_4 \circ \Sigma_1$, e proceder da mesma forma para $\Sigma_5 \circ \Sigma_2$ e $\Sigma_6 \circ \Sigma_3$.

Rejewski observou os seguintes factos, que são de demonstração trivial. Se α e β são duas involuções constituídas somente por pares, e se $\gamma = \beta \circ \alpha$, então

R1 γ tem uma decomposição em ciclos constituída por pares de ciclos de igual tamanho;

R2 Se $(\sigma_1\sigma_2)$ é um par de α, então σ_1 e σ_2 ocorrerem em ciclos distintos de γ que têm o mesmo tamanho;

R3 Se $(\sigma_1\sigma_2)$ é um par de α, então o par $(\gamma(\sigma_1)\gamma^{-1}(\sigma_2))$ é também um par de α.

Quando coligido um número significativo de mensagens, era muito usual aparecerem diversos indicadores repetidos. Estes indicadores repetidos correspondiam, quase sempre, às piores escolhas de chaves que os operadores

podiam fazer. Chaves constituídas pela repetição da mesma letra, AAA, por exemplo. Vejamos um exemplo de como o ataque se poderia então desenrolar. Suponhamos que já coligimos os ciclos das permutações compostas:

$$\begin{aligned}\Sigma_4 \circ \Sigma_1 &: (\texttt{DP})(\texttt{SY})(\texttt{ABQHZUIWOXL})(\texttt{MNJRVTGCKEF})\\ \Sigma_5 \circ \Sigma_2 &: (\texttt{AJV})(\texttt{HNY})(\texttt{BFZSWGCIMO})(\texttt{DKTLRXEQUP})\\ \Sigma_6 \circ \Sigma_3 &: (\texttt{AXJBLREONDZCS})(\texttt{IUYHWQVMFTPGK}),\end{aligned}$$

e seja YSGSWK um dos indicadores do dia que aparecem repetidos, e que portanto suspeitamos que deva ser a repetição de um símbolo, digamos ε. Por R2, e por a Enigma induzir uma permutação sem pontos fixos, sabemos que os únicos valores possíveis de ε só podem ser D ou P, pois (DP) é o único outro ciclo de tamanho 2 de $\Sigma_4 \circ \Sigma_1$. Mas não pode ser P, porque na permutação $\Sigma_6 \circ \Sigma_3$ a letra P ocorre no mesmo ciclo que G e K. Portanto $\varepsilon = \texttt{D}$. Logo (DY) é um par de Σ_1, assim como (PS). Portanto Σ_4 contém (DS) e (YP). Por outro lado, como (DS) é um par de Σ_2, podemos usar R3, para sucessivamente concluir que (KZ), (TF), (LB), (RO), (XM), (EI), (QC), (VG) e (PW) também são pares dessa permutação. Da mesma forma poderíamos prosseguir e deduzir informação sobre Σ_3, Σ_5 e Σ_6. Se agora procedermos da mesma forma para um outro indicador que suspeitemos repetido, a informação que se extrai é, muito provavelmente, suficiente para reconstruir por completo as permutações Σ_i $(i = 1, \ldots, 6)$. Com isto podemos recuperar as chaves de todas as mensagens desse dia. Resta saber qual a configuração do painel de trocas. Mas com a chave da mensagem conhecida, não é difícil, examinando as mensagens que vão de forma incompleta sendo decifradas, deduzir os pares activados no dito painel. Nesta simplificada exposição[10] foi omitida a descrição de como era possível deduzir a ordem dos rotores. Essa dedução é bastante mais morosa e envolve o recurso a um catálogo ordenado de todas as possíveis permutações de rotores, que havia sido feita antecipadamente para utilização diária.

Em 15 de Setembro de 1939, o modo de operação da Enigma muda. No livro de operação passa a estar a ordenação dos rotores e configuração dos seus anéis exteriores, assim como a configuração do painel de trocas, que mudam todos os dias. Para além disso, para enviar uma mensagem, o operador passa a ter que escolher duas chaves (ou indicadores). A primeira é enviada sem qualquer cifra, e a segunda cifrada com a primeira, **repetidas duas vezes**. É esta segunda chave que vai ser usada para cifrar o texto da mensagem. Como a chave com que a segunda chave é cifrada muda

[10] Para mais detalhes, consultar [12].

com cada mensagem, o ataque anteriormente descrito não pode efectuado. Apesar disso, o painel de trocas, mais uma vez, não esconde algumas características da composição dos rotores. Por vezes, no indicador da mensagem, ocorre $\Sigma_1(\varepsilon_1) = \Sigma_4(\varepsilon_1)$, $\Sigma_2(\varepsilon_2) = \Sigma_5(\varepsilon_2)$ ou $\Sigma_3(\varepsilon_3) = \Sigma_6(\varepsilon_3)$, ocorrência que os polacos chamavam uma "fêmea". Ou seja, a permutação $\Sigma_4 \circ \Sigma_1$ (ou $\Sigma_5 \circ \Sigma_2$, ou $\Sigma_6 \circ \Sigma_3$, respectivamente) tem um ciclo de ordem 1. Como o tamanho dos ciclos destas permutações compostas são preservados pelo painel de trocas, estes pontos fixos destas permutações também o são. A ocorrência de fêmeas é bastante frequente nos indicadores das mensagens, pelo que não era costume demorar muito tempo até aparecerem três mensagens com fêmeas formadas pela mesma letra, respectivamente para $\Sigma_4 \circ \Sigma_1$, $\Sigma_5 \circ \Sigma_2$ e $\Sigma_6 \circ \Sigma_3$. A este conjunto de 3 mensagens chamava-se uma "fêmea tripla". Com esta informação necessitamos descobrir, supondo que tal letra não é afectada pelo painel de trocas[11], qual das configurações (ordem dos rotores e posicionamento dos anéis dos rotores), admite esta fêmea tripla. Mais, sabemos também qual é a posição relativa dos rotores para estas posições iniciais destas configurações, pois as chaves com que foram cifradas cada uma das fêmeas é transmitida, de forma não cifrada em cada mensagem.[12] Para verificar qual das $26^3 \times 6$ configurações possíveis da Enigma satisfazem estas condições, foi construído um dispositivo que fazia a codificação de duas máquinas Enigma separadas por um avanço de 3 passos (o que corresponde à composição $\Sigma_{i+3} \circ \Sigma_i$) e que percorria todas as 26^3 configurações. Para saber qual a ordem dos rotores tinham-se 6, em vez de um só, destes dispositivos a funcionar. Este dispositivo, que ficou conhecido como "bomba" (ou "bomba polaca" para não ser confundida com um dispositivo distinto usado mais tarde em Bletchley Park), conseguia descobrir a configuração pretendida em cerca de 30 minutos.

O notável trabalho dos criptanalistas polacos consistiu essencialmente em, ao olhar para a cifra da Enigma à luz da Teoria de Grupos, evidenciar que o obstáculo intransponível que o painel de trocas parecia constituir, afinal, por ser uma simples conjugação da cifra original, não escondia muitas das propriedades dessa cifra.

Quando o exército nazi invade a Polónia, todo este trabalho não se perde.

[11] Como nesta altura o painel de trocas tinha somente 6 cabos, esta suposição tem uma probabilidade de um pouco mais de $\frac{1}{2}$ de se verificar.

[12] Esta chave não pode ser utilizada directamente, por serem desconhecidas as posições dos anéis externos de cada rotor, pelo que os símbolos indicativos da chave não podem ser usados. Mas as chaves das diversas mensagens, ainda que não indiquem uma posição absoluta dos rotores, estabelecem posições relativas para as posições iniciais dos rotores em cada una das mensagens.

Num encontro secreto em 25 de Julho de 1939, os polacos passam aos representantes dos governos francês e inglês todo o conhecimento que foram coligindo sobre a Enigma e o seu ataque, assim como dois protótipos de Enigmas reconstruídas. Os ataques então descritos só puderam ser utilizados durante menos de um ano, altura em que o modo de operação da Enigma voltou a ser alterado, mas este acto de partilha de informação tem uma importância indesmentível para o que viria a ser o esforço britânico de criptanálise da Enigma. Apesar do imenso potencial destes ensinamentos ter sido em parte desperdiçado[13] pelas medidas de segurança e secretismo ingleses, o simples facto de um punhado de matemáticos empenhados numa tarefa de criptanálise ter tido este sucesso não pode ter deixado de influenciar as decisões fundadoras de Bletchley Park.

A propósito do envolvimento de matemáticos na Criptografia, transcrevemos aqui duas curiosas passagens, a primeira escrita por Gordon Welchman, e a outra por Peter Hilton, ambos matemáticos que trabalharam em Blethcley Park:

> *A good deal of importance has been attached to the fact that first the Poles and than the British brought in mathematicians to work on Enigma. Like Rejewski and Turing, I was a mathematician but, whereas they were both at home with deep problems of mathematical analysis, my principal interest lay in a descriptive approach to algebraic geometry, now out of fashion. However, soon after reinventing the Zygalski sheets, I came up with an abstract idea — the principle of the diagonal board — which greatly increased the power of the Turing bombe. My wartime associate, Pat Bayly, maintains that this idea can be attributed to my pre-war habit of thinking in abstract multi-dimensional space. (Welchman [14, p. 199]).*

> [...] *despite the genius of Turing and his unique contribution, it must be understood that we could not have been sucessful without the effective cooperation of each member of the team of mathematicians brought to Bletchley Park for the purpose of analysing German signals enciphered on their highest grade codes. Why were we so successful?*

[13] Gordon Welchman, no seu livro de memórias sobre o ataque à Enigma em Bletchley Park [14, pag. 196], afirma desconhecer toda a teoria desenvolvida por Rejewski até à década de 1980, e por isso mesmo ter que voltar a deduzir parte das técnicas de ataque que os polacos tinham criado e comunicado ao governo inglês.

> *The relevant facts are these. Gathered together at Bletchley Park was a group of mathematicians, each of whom would be described as quintessentially "pure". (Peter Hilton [5, p. 299]).*

Não cabe aqui transcrever toda a passagem deste curioso texto de Peter Hilton, cuja leitura recomendamos ao leitor.

6 Uma contribuição de Turing

A 10 de Maio de 1940 os alemães abandonaram a cifra dupla daquilo que acima chamamos o segundo indicador, ou seja a chave escolhida pelo operador ([14], p. 97). Felizmente, por essa altura os criptanalistas de Bletchley Park tinham já acumulado muita informação sobre a tipologia de certas mensagens e os hábitos pessoais de alguns operadores alemães da Enigma, o que lhes permitia prever um número considerável de cábulas.

São de Turing as ideias essenciais de como usar uma cábula para determinar a configuração inicial dos rotores e as ligações do painel de trocas da máquina que cifrou a mensagem correspondente. Para as descrever, denote-se, como acima, por π a permutação dada pelo painel de trocas, por ρ a permutação correspondente a uma "rotação" do alfabeto de uma letra, e sejam α, β, γ, as permutações efectuadas pelo primeiro (o de entrada, e saída quando a informação regressa do reflector), segundo (o do meio) e terceiro (o que fica junto ao reflector) rotores, respectivamente, numa dada configuração inicial de uma Enigma. Finalmente, seja μ a permutação dada pelo reflector. A permutação Σ_k ($k \in \mathbb{N}$) efectuada pela Enigma, quando esta cifra a k-ésima letra da mensagem, pode então ser descrita do seguinte modo, supondo, para simplificar, que apenas o rotor de entrada se move aquando da cifração do segmento de mensagem que será analisado:

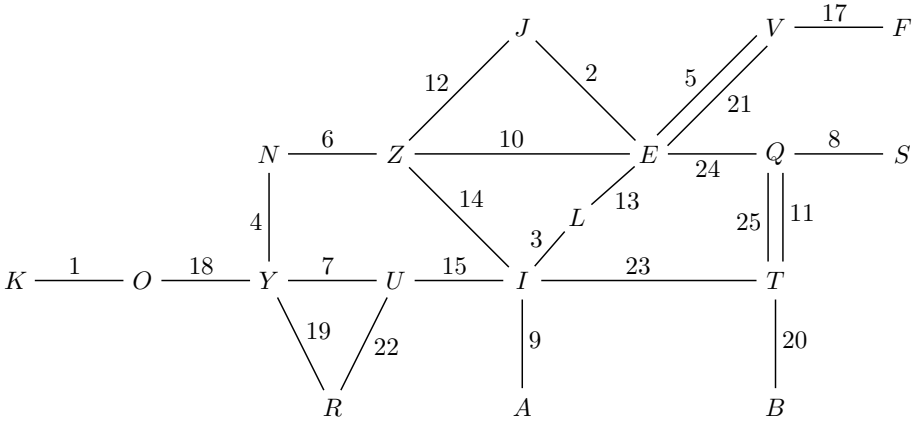
$$\Sigma_k = \pi \circ \rho^k \circ \alpha^{-1} \circ \rho^{-k} \circ \beta^{-1} \circ \gamma^{-1} \circ \mu \circ \gamma \circ \beta \circ \rho^k \circ \alpha \circ \rho^{-k} \circ \pi$$

Finalmente, seja $\Gamma_k = \pi \circ \Sigma_k \circ \pi$, a permutação correspondende a uma Enigma sem painel de trocas.

Suponhamos agora que sabíamos que, numa certa mensagem, o segmento `KEINEZUSAETZEZUMVORBERIQT`, de "keine zusaetze zum vorbericht", com `CH` substituído por `Q` para ter apenas 25 letras, correspondia a `OJLYVNYQIZQJLIIWFYYTVUTEQ` no criptograma. A informação contida nesta cábula, que para mais fácil leitura dispomos do seguinte modo

```
KEINEZUSAETZEZUMVORBERIQT
OJLYVNYQIZQJLIIWFYYTVUTEQ,
```

pode ser sumariada no diagrama seguinte, que era conhecido em Bletchley como um "menu" (de facto, um menu é um subdiagrama escolhido de um modo apropriado para ser testado numa "Bomba"), onde duas letras estão ligadas por uma aresta quando uma delas foi, em certa posição, cifrada na outra e onde cada aresta está etiquetada com a posição correspondente.



Ou seja, por exemplo, $\Sigma_6(\mathtt{Z}) = \mathtt{N}$. Dada a natureza involutiva da máquina Enigma, é claro que se tem também $\Sigma_6(\mathtt{N}) = \mathtt{Z}$.

Um ciclo $X_1 \xrightarrow{n_1} X_2 \xrightarrow{n_2} X_3 \xrightarrow{n_3} \cdots \xrightarrow{n_{t-1}} X_{t-1} \xrightarrow{n_t} X_1$ de um diagrama de uma cábula fornece equações

$$\Sigma_{n_{j-1}} \circ \cdots \circ \Sigma_{n_1} \circ \Sigma_{n_t} \circ \cdots \circ \Sigma_{n_{j+1}} \circ \Sigma_{n_j}(X_j) = X_j, \qquad j = 1, \ldots, t,$$

que, por se ter $\pi^2 = I$, são equivalentes a

$$\Gamma_{n_{j-1}} \circ \cdots \circ \Gamma_{n_1} \circ \Gamma_{n_t} \circ \cdots \circ \Gamma_{n_{j+1}} \circ \Gamma_{n_j}(\pi(X_j)) = \pi(X_j), \quad j = 1, \ldots, t.$$

Como veremos, isto pode ser usado para fornecer informação sobre a localização dos rotores, a sua posição inicial e a configuração do painel de trocas, efectuando um número de tentativas de, no máximo, 60×26^3, ou seja, retirando efectivamente a complexidade introduzida pelo painel de trocas.

As permutações da Enigma, sem o painel de trocas, que produziram o criptograma relativo ao segmento `KEINEZUSAETZEZUMVORBERIQT` foram as seguintes (i.e. Γ_i é a permutação dada pela i-ésima linha, tendo-se que $\Sigma_i(p_i) = c_i$):

i	p_i	p_i?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	c_i	c_i?
1	K	?	E	N	V	W	A	G	F	I	H	Q	O	P	X	B	K	L	J	T	U	R	S	C	D	M	Z	Y	O	?
2	E	?	L	F	Q	V	J	B	I	S	G	E	U	A	T	R	Z	Y	C	N	H	M	K	D	X	W	P	O	J	?
3	I	?	P	S	U	W	Z	K	M	O	L	R	F	I	G	V	H	A	X	J	B	Y	C	N	D	Q	T	E	L	?
4	N	K	S	U	L	O	H	K	Q	E	T	M	F	C	J	Y	D	Z	G	W	A	I	B	X	R	V	N	P	Y	O
5	E	E	K	Q	U	I	V	J	T	S	D	F	A	W	N	M	R	Z	B	O	H	G	C	E	L	Y	X	P	V	J
6	Z	I	J	R	Q	P	U	T	V	K	L	A	H	I	Y	Z	W	D	C	B	X	F	E	G	O	S	M	N	N	L
7	U	N	P	H	J	R	F	E	I	B	G	C	L	K	S	V	W	A	X	D	M	Z	Y	N	O	Q	U	T	Y	Y
8	S	E	I	W	D	C	O	M	H	G	A	L	P	J	F	R	E	K	S	N	Q	U	T	Z	B	Y	X	V	Q	V
9	A	Z	I	Y	P	W	R	Z	J	X	A	G	O	T	Q	S	K	C	M	E	N	L	V	U	D	H	B	F	I	N
10	E	U	M	R	V	I	Z	O	Y	X	D	U	N	W	A	K	F	T	S	B	Q	P	J	C	L	H	G	E	Z	Y
11	T	S	M	I	U	S	V	W	L	O	B	Z	P	G	A	Y	H	K	T	X	D	Q	C	E	F	R	N	J	Q	Q
12	Z	A	K	N	W	F	P	D	R	Y	U	Z	A	M	L	B	X	E	T	G	V	Q	I	S	C	O	H	J	J	I
13	E	E	V	C	B	S	L	N	K	O	X	P	G	E	U	F	H	J	R	Q	D	Z	M	A	Y	I	W	T	L	Z
14	Z	T	S	H	Y	J	W	T	Q	B	Z	D	U	M	L	X	V	R	G	P	A	F	K	O	E	N	C	I	I	Q
15	U	Z	H	X	S	V	L	M	T	A	U	Y	R	E	F	P	W	N	Z	K	C	G	I	D	O	B	J	Q	I	J
16	M	E	R	I	P	K	N	J	O	Z	B	F	D	U	W	E	G	C	Y	A	X	V	L	T	M	S	Q	H	W	L
17	V	Z	T	O	M	U	P	V	W	K	Q	Z	H	Y	C	X	B	E	I	S	R	A	D	F	G	N	L	J	F	I
18	O	U	V	J	R	L	P	H	T	F	U	B	Z	D	S	X	Y	E	W	C	M	G	I	A	Q	N	O	K	Y	I
19	R	M	I	W	H	N	Q	L	X	C	A	Z	P	F	U	D	S	K	E	Y	O	V	M	T	B	G	R	J	Y	W
20	B	V	P	T	R	S	N	G	F	M	K	U	I	X	H	E	Q	A	O	C	D	B	J	Y	Z	L	V	W	T	F
21	E	O	X	J	F	H	V	C	Q	D	K	B	I	M	L	O	N	R	G	P	W	U	T	E	S	A	Z	Y	V	Y
22	R	R	N	H	D	C	M	O	L	B	W	T	S	G	E	A	F	Z	V	U	K	J	R	Q	I	Y	X	P	U	Y
23	I	B	H	M	F	K	L	C	Y	A	T	W	D	E	B	O	N	Z	R	Q	V	I	X	S	J	U	G	P	T	T
24	Q	E	O	Z	T	U	Q	S	X	M	J	I	N	Y	H	K	A	R	E	P	F	C	D	W	V	G	L	B	E	V
25	T	R	V	S	M	Y	F	E	O	W	L	R	P	I	C	X	G	K	T	J	B	Q	Z	A	H	N	D	U	Q	U

É claro que o criptanalista não tem acesso a esta informação específica, sendo o seu plano de ataque percorrer todas as permutações da Enigma sem o painel de trocas, para cada possível escolha dos três rotores e para cada uma das suas posições iniciais, deduzindo todas as consequências de se supor uma ligação particular entre duas letras no painel de trocas. No exemplo dado, da suposição $\mathtt{A} \leftrightarrow \mathtt{Y}$, ou seja $\pi(\mathtt{A}) = \mathtt{Y}$, resultaria (ver diagrama acima) $\Gamma_{19} \circ \Gamma_{22} \circ \Gamma_7(\mathtt{A}) = \mathtt{A}$. Observe-se que aqui Γ_7 significa a sétima permutação quando se começa a contagem na inicial (que é desconhecida). Supondo agora que a máquina Enigma tinha começado a cifrar a mensagem na posição 4 (uma das muitas tentativas a serem feitas), o que significa que Γ_7, por exemplo, deve ser lida na posição 10, vê-se então que

$$\Gamma_{19} \circ \Gamma_{22} \circ \Gamma_7(\mathtt{A}) = \Gamma_{19} \circ \Gamma_{22}(\mathtt{M}) = \Gamma_{19}(\mathtt{C}) = \mathtt{D},$$

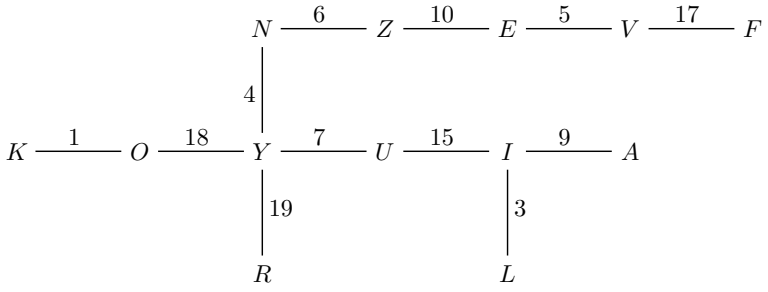
o que mostra que uma das suposições está errada: ou a mensagem não foi cifrada com início na posição 4, ou $\mathtt{A} \not\leftrightarrow \mathtt{Y}$. Ter-se-ia agora de testar todas as possibilidades $\mathtt{B} \leftrightarrow \mathtt{Y}$, $\mathtt{C} \leftrightarrow \mathtt{Y}$, $\mathtt{D} \leftrightarrow \mathtt{Y}$, etc... Se todas elas conduzirem a uma contradição, concluímos que 4 não é a posição inicial em que a mensagem foi cifrada; caso contrário, teríamos uma possível posição inicial, assim como uma ligação do painel de trocas.

Uma observação importante feita por Turing é que uma suposição de ligação no painel de trocas é equivalente a muitas outras, que portanto não são necessárias verificar. Por exemplo, como

$$\begin{array}{ccc} \mathtt{Y} & \xrightarrow{\Sigma_7} & \mathtt{U} \\ \downarrow \pi & & \downarrow \pi \\ A & \xrightarrow{\Gamma_7} & I \end{array}$$

a suposição $\mathtt{A} \leftrightarrow \mathtt{Y}$ é equivalente à suposição $\mathtt{I} \leftrightarrow \mathtt{U}$. O passo crucial dado em Bletchley Park foi o de se desenhar um dispositivo eléctrico cujos circuitos implementavam automaticamente a dedução das consequências de uma suposição. Tal dispositivo ficou a ser conhecido como a "Bomba" [14].

Na sua concepção inicial, o dispositivo eléctrico da Bomba explorava o *feedback* fornecido pelos ciclos contidos numa cábula. Mas é claro que o processo de tentativa de obtenção de contradições acima descrito pode ser usado mesmo quando o menu obtido de uma cábula não contém ciclos. Considere-se, por exemplo, o menu:



Suponhamos novamente que a mensagem foi cifrada com início na quarta permutação da tabela dada acima. Da suposição $\mathtt{K} \leftrightarrow \mathtt{A}$ deduzir-se-iam agora, sucessivamente: $\mathtt{O} \leftrightarrow \mathtt{S}$, $\mathtt{Y} \leftrightarrow \mathtt{W}$ e $\mathtt{N} \leftrightarrow \mathtt{O}$, obtendo-se a contradição de a letra $\mathtt{O}$ estar simultaneamente ligada a $\mathtt{S}$ e a $\mathtt{N}$ no painel de trocas. É Gordon Welchman que tem a ideia de acrescentar à Bomba um "quadro

[14] Que não deve ser confundido com a "bomba" polaca...

diagonal", que consiste num certo número de ligações extra e que implementa automaticamente o facto de, se `X` $\leftrightarrow$ `Y`, então `Y` $\leftrightarrow$ `X`, retirando assim mais consequências de uma dada suposição, o que permitia reduzir o número de testes.

O leitor interessado que queira perceber como foram desenhados os circuitos eléctricos que implementam estas observações deve consultar [14]. Para saber como adaptar este procedimento ao caso em que o rotor do meio se move durante a cábula, ver a p. 98 (p. 105 do documento digital) do documento escrito por Turing conhecido pelo nome *The Prof's Book*, disponível nos arquivos nacionais britânicos[15].

7 Observações finais

Para além de todo o trabalho na Enigma, Turing trabalhou num método de assegurar confidencialidade em transmissões de voz [14, p. 176][16], mas nada parece ser publicamente conhecido sobre os detalhes deste trabalho.

Relativamente ao papel que Turing terá ou não tido na criptanálise da cifra conhecida em Bletchley pelo nome de *Fish*, usada para comunicações entre o alto comando alemão, e no subsequente desenho e construção do *Colossus*, um dispositivo que foi usado para a quebrar, a confusão é enorme. Por exemplo, o seu biógrafo, Andrew Hodges escreve[17]:

> *Alan Turing did not become the chief figure in the Fish work, and in particular did not design or build the Colossus, as is so often incorrectly stated. Note also that the Colossus did not work on the Enigma ciphers! However, it depended on the statistical theory that Alan Turing had developed for breaking the naval Enigma. It was also very important that Turing knew all about the success of the Colossus, because this was the first large-scale application of digital electronics, and showed that this technology was reliable and practical. Turing's acquaintance with this work allowed him to plan with confidence for the computer of the future.*

[15] No *site* `http://www.nationalarchives.gov.uk`, mais precisamente na página `http://www.nationalarchives.gov.uk/documentsonline/details-result.asp?queryType=1&resultcount=1&Edoc_Id=2772131`, por 3.36 libras. Uma cópia tinha já sido disponibilizada pela NSA em Abril de 1996: ver `http://www.turingarchive.org/browse.php/C/30`. Para um resumo, consultar `http://www.turing.org.uk/publications/profsbook.html`.

[16] Ver também `http://www.turing.org.uk/sources/delilah.html`

[17] `http://www.turing.org.uk/turing/scrapbook/electronic.html`

E em [3, pag. xix–xx], o jornalista e escritor Paul Gannon, afirma:

> *Turing was only one of the people who worked on the cipher problem for which Colossus was built and his role was tangential at best (indeed, Turing developed a hand or manual method of breaking the relevant cipher, not the machine method for which Colossus was invented).*

Mas, em [5, pag. 293], Peter Hilton, que trabalhou directamente com Turing em Bletchley Park, diz peremptoriamente:

> *It was Alan Turing who first appreciate the essential role which could be played in the elimination phase of the process by high-speed electronic machines, and who was, in fact, — and quite consciously and deliberately — inventing the computer as he designed first the "Bombe" and then the "Colossus" for our cryptanalytical purposes.*

É lamentável que esta celebração centenária do nascimento de uma das figuras inglesas mais extraordinárias e brilhantes do século XX não tenha sido aproveitada pelas autoridades britânicas para deixar claro qual foi exactamente o papel de Turing na notável critanálise das várias cifras usadas pelas tropas nazis na segunda guerra mundial. Nem a omissão, ou falta de esclarecimento, do seu papel no esforço criptanalítico britânico, nem, no extremo oposto, o quase endeusamento do seu papel, ofuscando as contribuições dos muitos outros brilhantes matemáticos que com ele trabalharam, faz jus à sua memória.

Referências

[1] G. Birkhoff e S. MacLane, *A Survey of Modern Algebra*, Macmillan Co., 1941.

[2] Martin Davis, *Engines of Logic*, W.W Norton & Co., 2000.

[3] Paul Gannon, *Colossus: Bletchley Park's Greatest Secret*, Atlantic Books, 2006.

[4] I. J. Good, "Early work on computers at Bletchley", *Annals of the History of Computing*, Vol. 1, No. 1 (1979), pp. 38–48.

[5] Peter Hilton, "Reminiscences of Bletchley Park, 1942–1945", in Peter Duren (ed.), *A Century of Mathematics in America*, Vol. I, American Mathematical Society, 1988, pp. 291–301.

[6] Peter Hilton, "Working with Alan Turing", *The Mathematical Intelligencer*, Vol. 13, No. 4 (1991), pp. 22–25.

[7] Peter Hilton, "Reminiscences and Reflections of a Codebreaker", in W. D. Joyner (ed.), *Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory*, Springer, 2000, pp. 1–8.

[8] F. H. Hinsley and Alan Stripp, *Code Breakers*, Oxford University Press, 1993.

[9] David Kahn, *The Codebreakers: the story of secret writing*, The Macmillian Company, 1967.

[10] David Kahn, *Seizing the Enigma. The Race to Break the German U-Boat Codes*, Barnes & Noble, 1998.

[11] T. W. Körner, *The Pleasures of Counting*, Cambridge University Press, 1998.

[12] Bruno Ribeiro, *A Criptanálise da ENIGMA: 1932–1939*, Tese do Mestrado de Engenharia Matemática, Faculdade de Ciências da Universidade do Porto, 2007.

[13] Simon Singh, *O Livro dos Códigos*, Temas & Debates, 1999.

[14] Gordon Welchman, *The Hut Six Story: breaking the Enigma codes*, M & M Baldwin, 1998.