Alan Turing : a Bomba, a lógica, a matemática e a cifra

José Maria Fernandes de Almeida

Uma vida dominada pelo segredo, o último dos quais só foi revelado após a NASA — The National Seccurity Agency — dos Estados Unidos da América, em 2 de Abril de 1996, ter desclassificado os documentos referentes à máquina Enigma e processos de cifragem e decifragem utilizados durante a II Guerra Mundial.

Alan Turing nasceu em Paddington, Londres, no dia 23 de Junho de 1912. O seu pai Julius Mathison Turing era funcionário civil do governo inglês em Madastra, India, onde casara com Ethel Stoney pertencente à burguesia colonial. Considerando que o clima de Madrasta não era favorável à saude das crianças entregou Alan e o seu irmão mais velho John aos cuidados de uma família de coronéis do exército britânico. Em Setembro de 1913 Alan e John foram separados dos pais e começaram a ser criados pelos Ward perto de Hastings, Inglaterra.

A família Turing só se reunia de modo intermitente e a senhora Ward educou Alan para ser um verdadeiro homem duro e másculo. No entanto Alan não se adaptava ao modelo preconizado pela senhora Ward assim como também não se adaptou ao modelo victoriano praticado no colégio privado de Sherborne, onde entrou em 1926. Aliás foi neste colégio que Alan se apercebeu da sua atração exclusiva por rapazes. Um seu amigo Christopher Morcon, um ano mais velho que Alan, teve uma influência determinante na sua paixão pelas ciências.

Em 1930 é-lhe atribuída uma bolsa de estudos para o King's College, em Cambridge. No King's College encontra matemáticos notáveis e decide dedicar-se à matemática pura. Dois anos mais tarde apresenta à London Mathematical Society um artigo sob o título *On computable numbers, with an application to the Entscheidungsproblem* [problema da possibilidade de decisão por meios matemáticos, formulado por Hilbert no final da década de 1920]. Neste artigo, que só foi publicado em 1936, Turing descreve uma máquina abstracta muito simples que seria capaz de efectuar, de modo automático, um cálculo desde que a sua configuração fosse definida por uma tabela de instruções. A cada algoritmo corresponde uma tabela de instruções particular. Nada impede a concepção de uma máquina que seja capaz de executar o conjunto das operações realizadas por uma outra determinada máquina. Turing denominou essa máquina "Máquina Universal".

fig. 1 - Alan Turing

Pouco depois de Turing ter submetido o seu artigo à *London Mathematical Society* Alonzo Church, em Princeton, EUA, apresenta uma outra solução para o problema de Hilbert. Max Newman, professor de Turing em Cambridge, Inglaterra, escreve a Church recomendando-lhe o seu aluno. Turing embarca para os EUA em Setembro de 1936 tendo por objectivo frequentar um curso em Princeton como estudante graduado. Enquanto prepara a sua tese de doutoramento, numa tentativa de concretização da sua *Turing machine* utiliza uma máquina de cifra, que usava relays electromagnéticos, para multiplicar números binários.

Em Maio de 1938 Jhon von Neumann convida Turing para ser seu assistente em Priceton, mas Turing recusa esse

convite e regressa a Inglaterra.

Em Setembro de 1939 Turing entra ao serviço da *Government Code and Chypher School*, recém instalada em Bletchley Park. O objectivo prioritário em Bletchley Park é quebrar as chaves da cifra da máquina alemã *Enigma*.

A máquina *Enigma* tinha sido construída pelo alemão Arthur Scherbius em 1923 e era um produto comercial destinado a garantir comunicações que necessitassem de um certo grau de confidencialidade. A *Enigma* original dispunha de um teclado com 26 letras, um painel com 26 letras iluminadas cada uma por uma lâmpada eléctrica e um dispositivo denominado "scrambler". Este dispositivo era constituído por três rotores que giravam num mesmo eixo. Cada rotor possuia dois conjuntos de 26 contactos, um do lado esquerdo e outro do lado direito conectados por condutores eléctricos de tal modo que não existia nunca correspondência directa entre dois contactos idênticos. Cada um dos três rotores era idêntico com excepção da conexão interna dos contactos.

Deste modo, quando uma tecla era premida, a corrente eléctrica proveniente do teclado entrava num contacto direito do primeiro rotor. Através do circuito interno do rotor a corrente eléctrica saía por um contacto do lado esquerdo do rotor que não correspondia à letra afecta ao contacto do lado direito. O primeiro rotor do lado direito denominava-se "rotor rápido", o seguinte "rotor médio" e o da esquerda "rotor lento".

Considerando, por exemplo, que era premida a letra Q no teclado, à saida do "rotor rápido" a letra seria, por exemplo, Y a qual seria transformada, por exemplo, na letra S à saida do "rotor médio" e finalmente, à saida do "rotor lento", obter-se-ia, por exemplo, a letra N que seria iluminada no painel.

O operador anotava a mensagem cifrada a qual era enviada ao destinatário por correio, telégrafo ou telefone. O receptor utilizando uma *Enigma* com configuração idêntica digitava a mensagem cifrada e, tomando nota das letras iluminadas no painel, obtinha a mensagem decifrada.

fig. 2 - *Enigma*

Qualquer um dos rotores podia ser rodado à mão de modo a posicionar-se numa letra inicial diferente. Os rotores eram permutáveis de modo que poderiam ser posicionados em 26 x 26 x 26 (17.576) estados. No entanto, este sistema não era suficientemente seguro para garantir que a chave de cifra não fosse rapidamente identificada. Assim, cada vez que uma tecla era premida o "rotor rápido" avançava uma posição. Quando o "rotor rápido" atingia uma dada posição o "rotor médio" avançava por sua vez uma posição que poderia causar o avanço de uma posição no "rotor lento"; o "scrambler" funcionava de modo semelhante ao odómetro de um automóvel. Este processo reduzia o total de combinações possíveis em 26 x 26 (676), pelo que o quantitativo total de combinações possível era 16.900, na máquina base.

A simplicidade de utilização da *Enigma* e o quantitativo de combinações possível atraiu a atenção das Forças Armadas alemãs que impuseram a sua retirada do mercado e o seu fabrico, sucessivamente aperfeiçoado, para seu uso exclusivo.

Cada rotor passou a poder ser ajustado com um anel de caracteres diferente — "ring setting". A alteração do anel de caracteres provocava dois efeitos: primeiro, a correspondência entre letras num mesmo rotor era alterada; segundo, a posição do grampo de avanço que movia o "rotor médio" e o "rotor lento" passava a corresponder a uma letra diferente. Assim adicionavam-se 676 combinações possíveis dos anéis de caracteres para os "rotores médio e lento". Por outro lado a permutação dos rotores acrescentava seis possibilidades diferentes de posicionamento. Como existia um conjunto de cinco rotores dos quais três podiam ser utilizados o quantitativo de combinações possível era 10 x 6 = 60. Deste modo o quantitativo de combinações inicial seria 17.576 x 60 = 1.054.560. Considerando as combinações possíveis para os anéis de caracteres dos "rotores médio e lento" o conjunto de estados passava a ser de 1.054.560 x 676 = 712.882.560. Considerando agora os 26 estados possíveis para o anel de caracteres do "rotor rápido" o conjunto de estados possível era 26 x 712.882.560 = 18.534.946.560.

Por *encomenda* das Forças Armadas alemãs, foi acrescentado à *Enigma* um quarto rotor denominado "reflecting" que recebia o sinal do "rotor lento", o transformava e reenviava de novo para o "rotor lento" e o processo de cifragem descrito continuava a ser realizado agora em sentido inverso até atingir o "rotor rápido" e era o sinal que saía deste que iluminava a lâmpada no painel. A introdução do reflector produziu a restrição de nenhuma letra poder ser encriptada por ela própria.

As Forças Armadas alemãs acrescentaram ainda à *Enigma* um dispositivo denominado "Stecker" que permitia trocar pares de letras para além das trocas já conseguidas com a utilização dos rotores. Por exemplo se no "Stecker" a letra A fosse trocada com a letra Z, a conversão inversa era também verdadeira, isto é, Z era sempre trocado com A. Este aparente aperfeiçoamento realçava ainda mais uma fraqueza do sistema: nenhuma letra poder ser encriptada por ela própria.

Uma *Enigma* de três rotores, com todos estes aperfeiçamentos, era possível atingir a ordem dos 150.000.000.000.000.000.000 de combinações.

Para complicar ainda mais o sistema de cifra os submarinos alemães (U-boat) utilizavam máquinas *Enigma* com quatro rotores e conjuntos de oito rotores em vez dos cinco utilizados pelos outros ramos das Forças Armadas alemãs.

O quantitativo de combinações possíveis e a sofisticação da *Enigma* convenceu as Forças Armadas alemãs que dispunham de um sistema de chaves de cifra "inquebrável".

No entanto, por engano os alemães enviaram, em 1928, para a sua delegação em Varsóvia uma *Enigma* por correio normal. Detectado o erro, os funcionários da delegação alemã em Varsóvia realizaram rapidamente inquéritos sobre o paradeiro da encomenda. Este procedimento chamou a atenção das autoridades alfandegárias polacas e o resultado foi que o departamento de cifra polaco — BS4 — examinou a máquina *Enigma* durante um fim de semana e só entregou a encomenda, cuidadosamente igual à original, na segunda feira seguinte.

O matemático polaco Marian Rejewski decifrou a chave das *Enigma* alemãs partindo de uma dedução muito simples: para que o receptor da mensagem cifrada a pudesse decifrar tinha que saber exactamente qual era a posição inicial dos rotores na *Enigma* do emissor. Para uma *Enigma* de três rotores a chave era uma sequência de três letras visíveis pelo operador na superfície do tronco de cilindro de cada um dos rotores. O processo utilizado em todos os sistemas de cifragem na época era o de incluir a chave de descodificação no texto da mensagem repetindo-a no início do texto.

Deste modo, o operador emissor da *Enigma* colocava os seus três rotores numa posição conhecida por todos os operadores, por exemplo ZUG, em seguida digitava duas vezes a chave do dia, por exemplo TAGTAG, obtendo uma sequência cifrada de seis letras, por exemplo ARBGMW. Em seguida, colocava os seus três rotores na posição TAG e codificava a mensagem.

O operador receptor colocava os seus três rotores na posição ZUG e em seguida digitava ARBGMW obtendo a chave do dia TAGTAG. Em seguida colocava os seus três rotores na posição TAG e descodificava a mensagem.

Os decifradores polacos desenvolveram um procedimento dedutivo para determinar as chaves de cifragem baseado no pressuposto que os alemães não utlizavam o "Stecker" quando digitavam a chave. Assim, por exemplo, se uma mensagem começasse pela letra A seguida de quatro letras adiante pela letra R, as letras A e R eram o resultado da cifragem da mesma letra. Realizaram a mesma dedução para a segunda e quinta e terceira e sexta. Construiram tabelas a partir de conjuntos de mensagens alemãs e descodificaram todas as mensagens alemãs entre o dia 30 de Abril e 8 de Maio de 1937. O sucesso foi efémero: a partir dessa data todas as *Enigma* passaram a utilizar uma posição inicial escolhida pelo operador ao invés de uma posição fixa.

Quando Turing entra ao serviço da Government Code and Chypher School, em Setembro de 1939 dispõe do conhecimento adquirido pelos decifradores polacos, mas não lhe é possível construir a totalidade das combinações usadas nas novas versões mais complicadas da *Enigma*.

Os decifradores polacos e, posteriormente, os decifradores ingleses tinham verificado que os alemães cometiam algumas falhas nos procedimentos adoptados para cifrar as mensagens. Algumas falhas eram facilmente detectadas.

Uma das falhas detectada era a reutilização dos livros de código para um determinado mês. O livro de código continha a posição inicial em que os rotores da *Enigma* eram posicionados durante um período de 24 horas. Se uma mensagem pudesse ser decifrada num determinado dia, a posição inicial dos rotores era conhecida e todas as outras mensagens cifradas nesse dia eram decifradas.

Outras falhas eram menos óbvias, mas sabia-se que o texto das mensagens alemãs era sempre muito formal. Uma mensagem era sempre iniciada por uma cadeia de caracteres que identificava o destinatário, por exemplo "PARAOGENERALLUIS" (obviamente em alemão). Esta cadeia de caracteres denominava-se crib. Quando os decifradores ingleses pensavam que tinham um crib útil podiam determinar quais as combinações possíveis utilizadas no posicionamento dos rotores da *Enigma*. No entanto o quantitativo de combinações possíveis era da ordem do trilião.

Turing, comparando determinado *scrib* com a respectiva cifra verificou que existiam pares de letras que formavam uma sequência iniciada e terminada pela mesma letra constituindo um loop. Concluiu que existia um quantitativo reduzido de sequências de rotores no scrambler e que seria possível construir uma máquina que pesquisasse estas sequências possíveis de rotores da *Enigma*. Com base nesta descoberta concebeu uma máquina que testasse as combinações possíveis dos rotores de uma *Enigma* usando o método da palavra provável. Deste modo bastaria testar 26 x 26 x 26 x 60 = 1.054.560 sequências de rotores.

Turing e o matemático Gordon Welchman construiram a máquina utilizando *relais* rotativos — idênticos aos usados nos antigos aparelhos telefónicos com marcador circular —, rotores *Enigma*, visores luminosos e quadros eléctricos de conexão de circuitos. A máquina foi denominda *the Bombe*, provavelmente por semelhança com a denominação Bomba atribuida pelos decifradores polacos a uma máquina mecânica construída para apoiar a descriptação das mensagens encriptadas pelos alemães nas máquinas *Enigma*.

A *the Bombe* comportava-se como uma colecção de máquinas *Enigma* trabalhando em conjunto. Segundo Welchman existiam doze conjuntos de rotores *Enigma* na *the Bombe*. No entanto, apesar das onze *the Bombe*, instaladas em Bletchley Park entre

Maio de 1940 e o final da Segunda Guerra Mundial (1939-1945) terem sido destruídas pelos serviços secretos ingleses, há notícia que algumas deveriam dispor de um quantitativo superior a doze rotores *Enigma*.

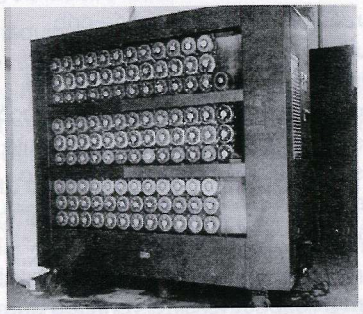

fig. 3 - *the Bombe*

Turing aplicou o processo clássico de "redução ao absurdo" para testar qual a sequência correcta para um determinado crib. Os rotores, na *the Bombe*, eram posicionados segundo uma sequência assumindo que era a correcta para cifrar o *crib*. A máquina começava a trabalhar e tentava provar que não era aquela a sequência correcta. No caso de não ser a sequência correcta a máquina passava automaticamente à segunda sequência que deveria ser testada e tentava provar que esta não era a sequência correcta. Se a máquina não conseguisse provar que a sequência era incorrecta, a sequência era anotada como boa, mas a máquina continuava a trabalhar pesquisando outras sequências correctas possíveis.

A máquina utilizava um sistema binário que podia realizar os testes lógicos muito rapidamente.

Deste modo os decifradores ingleses utilizaram a máquina para determinar qual o conjunto reduzido de combinações possível para um determinado *crib*. Se o *crib* era bom a mensagem era rapidamente decifrada, se não, também rapidamente, seriam encontradas contradições.

No entanto, neste processo não era considerada a utilização do "Stecker" que equipava as *Enigma* e permitia trocar pares de letras. Welchman concebeu então um dispositivo denominado "diagonal board" que fisicamente era construído segundo uma matriz quadrada de 26 x 26 terminais. Cada linha da matriz correspondia aos 26 conectores A a Z do "Stecker". Utilizando as 26 colunas era possível realizar fisicamente, através de conexões eléctricas, todas as trocas de pares de letras. Este aperfeiçoamento eliminava falsas sequências "verdadeiras" e reduzia a pesquisa das sequências de rotores a 26 x 26 x 26 = 17.576.

Com a utilização da *the Bombe*, em finais de 1940 as mensagens de rotina da Luftwaffe eram descriptadas pelos ingleses. A decifragem regular das mensagens dos U-Boat começou a ser realizada nos meados de 1941, mas em 1 de Fevereiro de 1942 as *Enigma* que equipavam os U-boat foram modificadas e perdeu-se a capacidade de decifragem que só foi recuperada no início de 1943.

Em Novembro de 1942 Turing regressa aos EUA, oficialmente como membro de ligação com os aliados, mas efectivamente foi construir, em colaboração com os Bell Laboratories, um sistema electrónico para cifragem das comunicações telefónicas entre Roosevelt e Churchill. Regressa a Inglaterra em Março de 1943 e dedica-se a um projecto de construção de uma máquina para cifrar comunicações telefónicas.

Alan Turing faleceu no dia 7 de Junho de 1954 em Manchester, Inglaterra, e presumivelmente cometeu suicídio.

Uma vida dominada pelo segredo o último dos quais, as suas realizações práticas, só foi revelado após a NSA — The National Seccurity Agency — dos EUA ter desclassificado os documentos referentes à máquina *Enigma* e processos de cifragem e decifragem utilizados durante a Segunda Guerra Mundial em 2 de Abril de 1996.

José Maria Fernandes de Almeida
Univ. Évora

Programação linear (conclusão)

existência de rectas paralelas, expliquei que isso conduzia a que o problema tivesse várias soluções.

No final da aula fiquei com a sensação de que os alunos tinham percebido bastante bem o método de resolução. Aguardei com expectativa as próximas aulas.

Nas duas aulas seguintes trabalharam em grupo com bastante entusiasmo. Levei para estas aulas uma calculadora gráfica TI82, para o caso de quererem comparar gráficos. Entretidos que estavam nos seus trabalhos, ninguém recorreu à máquina.

Pedi-lhes que entregassem os trabalhos feitos e que escrevessem um comentário exprimindo a sua opinião quanto a este tema. A fig. 1 representa a resolução do problema *A papa do bebé* apresentada por um grupo de alunos.

Balanço

Fazendo um balanço destas quatro aulas e principalmente das duas em que trabalharam em grupo, depois de analisar os trabalhos que apresentaram e os comentários que escreveram, acho que este projecto foi inteiramente positivo. Os alunos trabalharam em bom ritmo, três grupos resolveram todos os problemas propostos, dois grupos resolveram três problemas e um grupo apenas resolveu um problema. Todos os grupos expressaram uma opinião positiva sobre estas aulas, consideraram os problemas muito interessantes e motivadores e gostaram sobretudo do facto de terem trabalhado em grupo. Embora em dois grupos a opinião fosse a de que os problemas eram difíceis, nos restantes grupos foram considerados simples e acessíveis.

Referências

Sebastião e Silva, J. (1975). *Guia para a utilização do compêndio de Matemática*. 1º Volume. Lisboa: GEP

Jorge Filipe
Esc. Sec. da Cidade Universitária