FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Departamento de Informática

Mestrado Integrado em Engenharia Informática

Criptografia

Máquina Enigma

Docente: Isabel Oitavem

Abel Silva nº45872

Rodrigo Cardoso nº45483

Índice

Conteúdo

Introdução

Este trabalho insere-se na cadeira de Criptografia e tem como objetivo apresentar a máquina Enigma, o seu enquadramento histórico, funcionamento e modelo físico, formulação matemática da máquina, quebra da cifra e técnicas criptográficas envolvidas.

A Enigma insere-se nos modelos criptográficos de chave simétrica sendo que a sua cifra é baseada no método de substituição de forma dinâmica.

História da Enigma e seus Protagonistas

Enigma é o nome da marca de uma série de máquinas criptográficas desenvolvidas antes e durante a 2ª guerra mundial.

A história da Enigma começa em meados de 1915 com a invenção das máquinas de cifra baseadas em rotores por parte de dois oficiais da marinha holandesa, nomeadamente Theo A van Hengel (1875-1939) e Rudolf Pieter Cornelis Spengler (1875-1955). As máquinas destinavam-se ao Departamento de guerra holandês.

Imagem 1 – Theo A van Hengel

A máquina foi construída 21 anos antes da 2ª guerra mundial, pelo que a sua concepção não se destinava ao conflito militar. Esta foi criada para uso diplomático e comercial, assim como para impedir a espionagem corporativa.

As Enigmas são máquinas eletromecânicas utilizadas para criptografar e descriptografar mensagens.

A máquina foi patenteada por Arthur Scherbius (1878–1929), um engenheiro de eletricidade, em 1918 e os primeiros modelos (Enigma A) foram exibidos pela primeira vez em 1923.

Imagem 2 – Arthur Scherbius

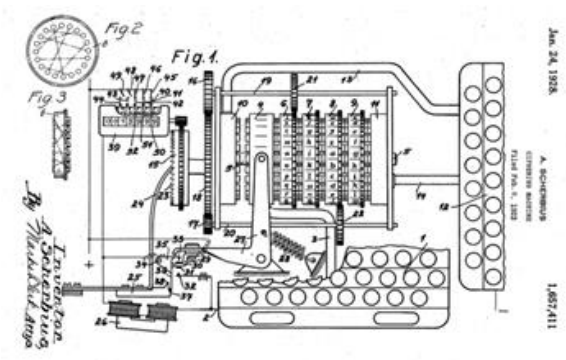

Imagem 3 – Patente da Máquina

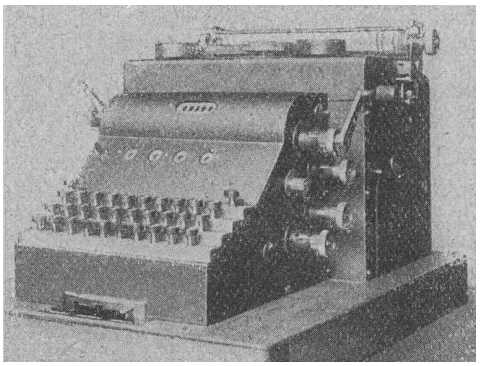

Imagem 4 – Enigma A

A Enigma A assemelhava-se a uma máquina de escrever, pesando cerca de 50kg. Esta versão Esta versão foi rapidamente substituída pela Enigma B devido ao seu custo elevado e aos problemas de fiabilidade associados aos mecanismos de impressão.

Em 1926 é lançada uma versão comercial, a Enigma modelo D, com uma série de melhorias que incluíam a possibilidade de troca entre rotores e um refletor configurável. Esta versão passou a ser o principal produto da marca.

Inicialmente as forças armadas alemãs não mostraram interesse na aquisição da máquina visto que consideravam que não existia tráfego de informação suficiente que justificasse a sua utilização.

Imagem 5 – Enigma D

Imagem 6 – Enigma B

No entanto, ainda no mesmo ano, as forças armadas alemãs decidem requisitar alguns exemplares especiais (diferentes da versão comercial).

Esta variante da Enigma D viria a conter um painel de trocas cujo propósito era aumentar a segurança da encriptação.

O primeiro protótipo desta variante é desenvolvido em 1927 e a versão final encontra-se pronta em 1932 sendo exclusiva para as forças armadas alemãs.

Até essa data todas as versões comerciais da Enigma encontravam-se disponíveis no mercado internacional. A partir do lançamento desta versão as forças armadas reclamam os direitos exclusivos da máquina sendo que daí em diante qualquer venda necessita de aprovação da parte destes.

Imagem 7 – Variante da Enigma D

Em meados de 1930, o departamento polaco de criptografia inicia as primeiras tentativas de quebrar o código da Enigma comercial.

Visto que a Polónia é um país vizinho da Alemanha, o receio de uma invasão (que viria mesmo a ocorrer em 1939) fez com que fossem realizados esforços no sentido de quebrar o código da máquina alemã.

Para tal são chamados 3 matemáticos polacos, nomeadamente:

- Marian Rejwski (16 Agosto 1905 – 13 Fevereiro 1980) era também criptologista e foi responsável por reconstruir a Enigma e deduziu a secreta fiação interna desta juntamente com Jerzy e Henryk.

- Jerzy Rózycki (24 Julho de 1909 - 9 de Janeiro de 1942) era também criptologista e inventou o método do relógio que conseguia por vezes determinar qual dos rotores da máquina era o mais à direita.

- Henryk Zygalski (15 de julho de 1906 - 30 de agosto de 1978) era um criptoanalista e foi responsável por conceber as folhas Zygalski, um dispositivo manual para encontrar as configurações de uma Máquina Enigma.

Imagem 8 – Jerzy Rózycki

Imagem 9 – Marian Rejwski

Imagem 10 – Henryk Zygalski

Os polacos foram os primeiros a quebrar a cifra da Enigma versão militar em 1932. O seu sucesso baseou-se em pura análise matemática, informação de um espião alemão e uma máquina Enigma comercial que foi intercetada pelos serviços de correio polacos.

Após conseguirem comprar uma Enigma comercial, usando toda a informação que reuniram, os matemáticos convertem-na numa Enigma militar e passam a ser capazes de escutar as comunicações alemãs.

Ao longo da história desta máquina os avanços e recuos na quebra da sua cifra foram constantes. Cada vez que os alemães se apercebiam que a confidencialidade das suas comunicações estavam comprometidas implementavam uma alteração na máquina, aumentando o número de combinações possíveis de encriptação de forma exponencial.

Isto fazia com que os matemáticos empenhados no trabalho de quebrar a sua cifra perdessem todo o trabalho efetuado até então e tivessem de recomeçar arranjando formas de fazer face às novas características da máquina.

Uma das máquinas desenhadas pelos polacos ficou conhecida como a bomba criptológica, em resposta às melhorias na Enigma dos alemães. O funcionamento da máquina consistia na análise das letras de controlo enviadas no início de todas as mensagens.

Em 1938 os polacos apercebem-se dum crescente número de mensagens trocadas entre os alemães o que revela que estes estão a preparar-se para a guerra. A Polónia começa então a preparar-se para tirar todo o conhecimento adquirido sobre a Enigma do país antes que fosse demasiado tarde.

Foi realizado um encontro na capital polaca, Varsóvia, onde todos os conhecimentos foram passados aos franceses e aos ingleses juntamente com duas réplicas da Enigma construída pelos polacos.

Imagem 11 – Bomba Criptologica

Imagem 12 - Varsóvia

Após a reunião, o departamento de criptografia polaca destrói todos os documentos e equipamentos e os matemáticos partem para França onde continuam a trabalhar em formas de quebrar a Enigma.

Duas semanas após a reunião, a Polónia é invadida pelos alemães e dois dias depois da invasão, a França e a Inglaterra declaram guerra à Alemanha dando inicio à 2ª guerra mundial.

Inglaterra instala em Bletchley Park o departamento de criptografia, que passou a ser o local onde todos os esforços, para se decifrar a máquina Enigma, foram feitos por Alan Turing e a sua equipa.

Baseado nesse conhecimento passado pelos polacos, Alan Turing desenvolveu uma máquina capaz de recuperar a configuração inicial da Enigma e assim decifrar as mensagens dos alemães.

O nome escolhido para a máquina foi The Bomb, inspirado na bomba criptológica polaca,criada em 1939. O seu funcionamento assumia a existência de um pedaço de texto na mensagem enviada numa determinada posição deste (cribs), visto que os alemães diariamente enviavam comunicações relativas às condições meteorológicas para os submarinos, e estas seguiam sempre o mesmo padrão.

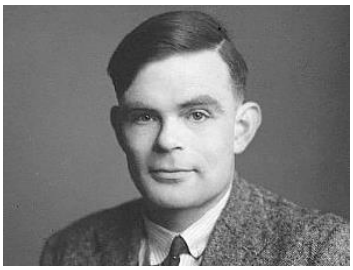

Imagem 13 – Alan Turing

Imagem 14 - Bletchley Park

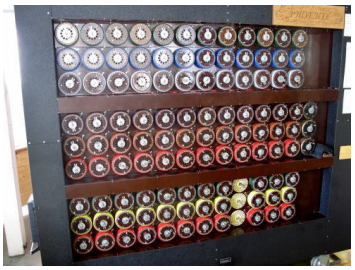

Imagem 15 - The Bomb

Em 1940 os ingleses eram capazes de escutar a maior parte das comunicações da força aérea e alguma relativa ao exercito alemão.

Já as comunicações da marinha alemã eram um problema visto que estes usavam procedimentos distintos e tinham 3 rotores adicionais para poder trocar entre si. Esses rotores extra são exclusivamente utilizados pela marinha e não são partilhados por nenhuma das outras forças armadas.

Em 1941 as forças militares inglesas conseguem capturar um U-boot U-110 (submarino alemão) e consigo uma vasta quantidade de livros de códigos usados pela marinha alemã. Esta descoberta ajuda Turing a conseguir decifrar parte das comunicações da Enigma M3 da marinha.

Imagem 16 – U-boot U-110

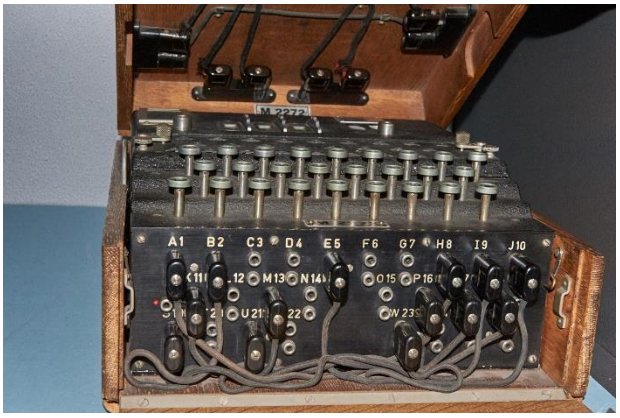

Imagem 17 – Enigma M3

Em 1942 um novo contratempo ocorre, quando a marinha alemã decide mudar as Enigmas M3 para as M4 (de 4 rotores), mudar os livros de código. Essa mudança fez com que os matemáticos ingleses deixassem de conseguir decifrar as mensagens.

O blackout durou 9 meses e durante esse tempo a marinha alemã foi capaz de afundar inúmeros navios que transportavam alimentos, munições e pessoas vindos dos Estados Unidos para a Inglaterra.

Novamente, a sorte faz com que os ingleses sejam capazes de recuperar um submarino alemão naufragado e com ele vários livros de códigos.

Durante os 9 meses de blackout Turing e a sua equipa trabalharam arduamente na fiação que constituía os novos rotores usados pela marinha alemã e os procedimentos únicos que estes usavam. Os livros de códigos capturados vieram completar o puzzle.

Em 1942 os Estados Unidos envolvem-se na guerra, e convencem os ingleses a partilhar os conhecimentos adquiridos sobre a Enigma.

Desta partilha, é iniciada a construção da Bomba americana por Joe Desch, que seria bastante fiável e rápida, permitindo a partir daí decifrar todas as mensagens da marinha alemã e salvar milhões de vidas. Em 1943 a primeira Bomba americana fica pronta.

Imagem 18 – Enigma M4

Imagem 19 – Joe Desch

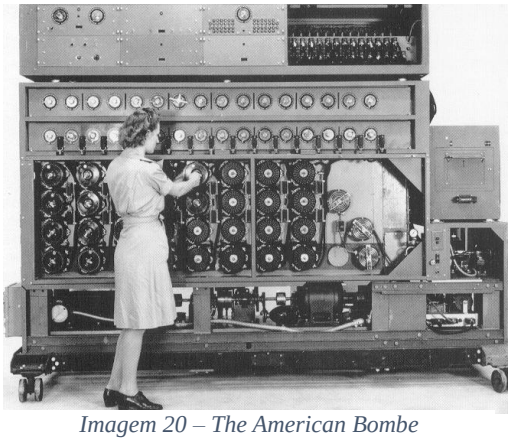

Imagem 20 – The American Bombe

Funcionamento da Máquina

a) A máquina em geral

A máquina Enigma é um dispositivo eletromecânico composto por um teclado, um painel de luz, representando o alfabeto, três ou quatro rotores, um refletor e ainda um painel de trocas.

Cada rotor roda no sentido horário e está orientado de tal forma que as configurações do 1º rotor se alteram a cada carácter que é encriptado variando entre os valores 0 e 25. Na transição entre 25 e 0, o 2º avança uma unidade.

O mesmo acontece para o 3º rotor. Isto garante que se o mesmo carácter for enviado duas vezes seguidas, vai ser provavelmente encriptado como duas letras diferentes sendo que não é possível encriptar uma letra nela própria.

Imagem 21 – Teclado da máquina

Imagem 22 – Painel de luz

Para aumentar o número de permutações possíveis, os rotores são removíveis e podem ser trocados entre si.

O refletor é um dispositivo com 26 contactos na face adjacente ao último rotor, com fios de tal maneira que os contactos estão conectados aos pares. Quando um sinal é enviado para o refletor, este é transmitido através do respetivo fio e regressa ao 3º rotor.

O painel de trocas consiste numa série de tomadas responsável por cifrar um caracter seguindo as seguintes convenções: se uma certa tomada está ligada, o caracter será cifrado caso contrário mantém-se inalterado.

Um sinal elétrico é passado do teclado para os rotores, que estão conectados em série, até este chegar ao refletor. Depois, o sinal é passado para trás desde a placa refletora para os rotores e de volta para o teclado onde um painel em separado é iluminado. Cada lâmpada corresponde a uma letra cifrada.

A máquina tem um compartimento para uma bateria de 4 volts e algumas versões têm um interruptor para selecionar entre a bateria interna e uma fonte de alimentação externa.

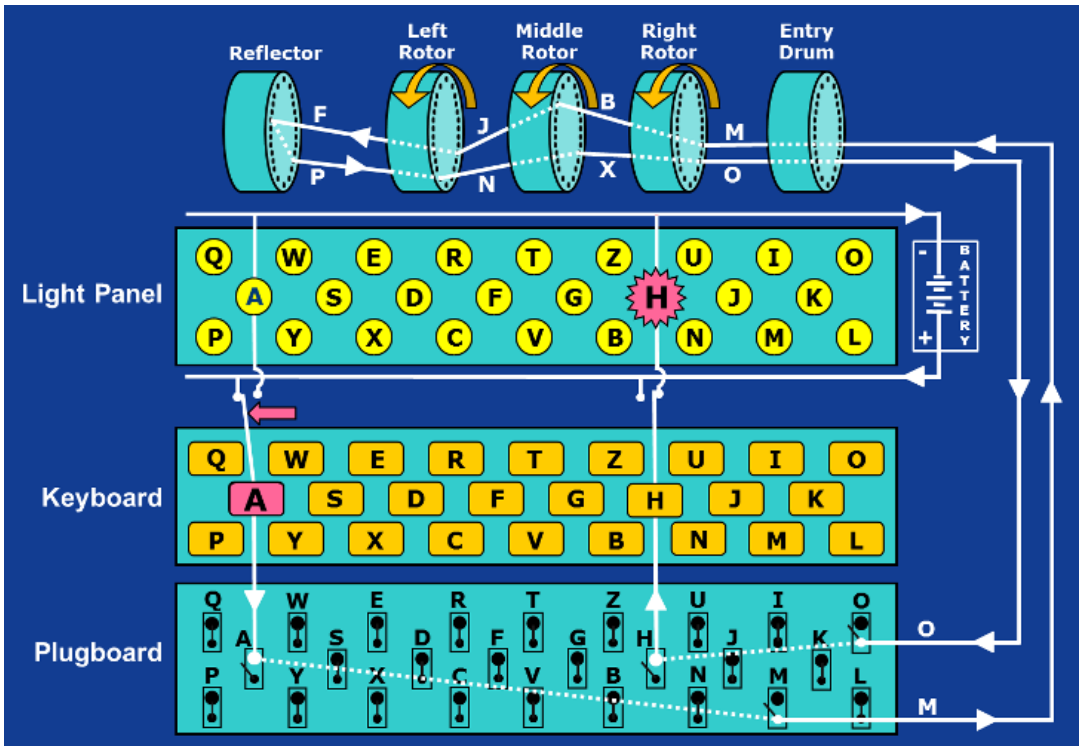

Imagem 23 – Caminho seguido pelo sinal elétrico

Imagem 24 – Bateria restaurada da máquina

b) Os rotores

Os rotores são o elemento mais importante da máquina. Estes discos redondos têm um núcleo com 26 pinos do lado direito e 26 contactos do lado esquerdo, ligados entre si por um conjunto de fios, e com um eixo oco ao centro.

Fora do núcleo da fiação existe um anel móvel com 26 números ou letras e uma cavilha. Este anel é rotativo e é bloqueado com um pino de mola.

Alterar a posição do anel alterará a posição da cavilha e do alfabeto, em relação à fiação interna. Esta configuração é chamada de ajuste de anel ou Ringstellung e a sua posição é visível por uma marcação de pontos.

Imagem 25 - Lado esquerdo do rotor

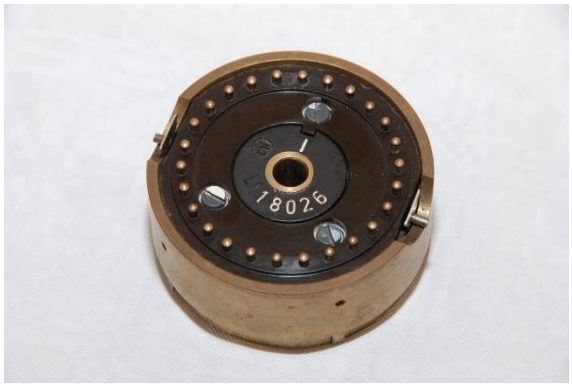

Imagem 26 – Lado direto do rotor

Imagem 27 – Anel

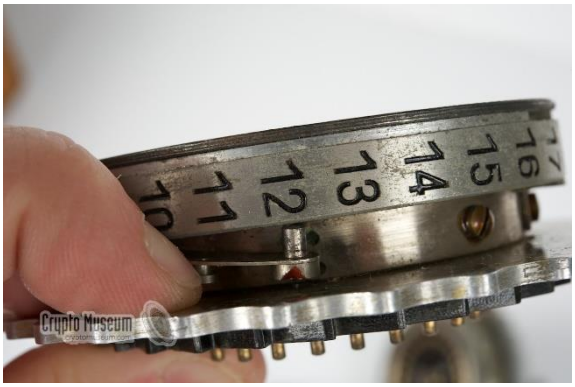

Imagem 28 - Cavilha

c) O refletor

O refletor, Umkehrwalze ou UKW em Alemão, é uma característica única da máquina Enigma. Na fiação interna de todos os rotores móveis, cada letra pode ser ligada a qualquer outra.

No refletor, as conexões são feitas aos pares. Deste modo, é possível encriptar e desencriptar utilizando a mesma máquina e a mesma configuração.

Imagem 29 - Refletor

Imagem 30 – Interior do refletor

d) O painel de trocas:

Em 1930, o painel de trocas foi introduzido na primeira versão da Wehrmacht Enigma.

O painel de trocas está situado na parte frontal da máquina. Sem qualquer ligação inserida, a corrente flui para os interruptores, controlados pelo teclado, diretamente para a entrada do rotor.

A inserção de um cabo no painel resulta numa troca de duas letras envolvidas antes de prosseguir para a entrada do rotor.

Cada máquina estava equipada por norma com um conjunto de 10 cabos. A adição deste elemento resultou num aumento exponencial do número de combinações induzidas pela máquina, melhorando a sua capacidade de encriptação.

Imagem 31 – Painel de trocas

e) Os operadores

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:

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. A discriminante (for exemplo, QXT) — este era usado para o operador identificar, aos destinatários pretendidos, a chave que estava a usar.

O operador começa por configurar todos os rotores rodando o anel exterior por forma a que os números da lista se alinhem com uma marca no rotor, fixando o anel nessa posição com a cavilha. Depois este tem de ordenar os rotores ao longo do eixo também de acordo com o pré-definido. De seguida faz as ligações indicadas no painel de trocas.

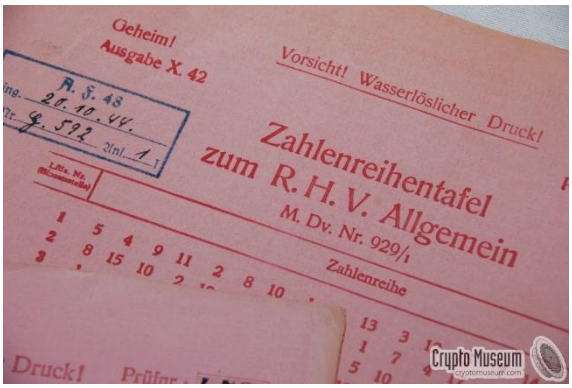

Imagem 32 – Lista de códigos (chaves)

f) A segurança matemática da Enigma

Para selecionar 3 rotores de um conjunto de 5, existem 60 combinações (5 * 4 * 3)

Cada rotor, ou seja, a sua fiação interna, pode ser ajustado em qualquer uma das 26 posições. Portanto, com 3 rotores há 17.576 diferentes posições do rotor (26 * 26 * 26).

O anel em cada rotor detém a sua rotação (que não importa aqui) e uma cavilha que afeta o avanço do próximo rotor esquerdo introduzindo mais 676 combinações.

Já o painel de trocas com o padrão de 10 cabos temos 150.738.274.937.250 combinações diferentes.

No total, isto dá: 60 * 17.576 * 676 * 150.738.274.937.250 = 107.458 687.327.250.619.360.000 ou $1{,}07 * 10^{23}$

g) As fraquezas da Enigma

1. *Uma letra nunca pode ser codificada nela própria:*

   Uma das propriedades chave do design da Enigma é o facto de uma letra nunca poder ser codificada nela própria o que acaba por permitir aos criptoanalistas reduzir o número possível de combinações.

2. *Avanço duplo do rotor do meio:*

   Sobre certas circunstâncias, o rotor do meio pode provocar um avanço duplo após duas teclas premidas de seguida. Isto reduz efetivamente para metade o período da cifra. Este fenómeno é descrito em um artigo de David Hamer.

3. *O girar regular dos rotores:*

   Na maior parte das máquinas Enigma, o rotor mais à direita necessita de uma volta completa antes de o rotor à sua esquerda avançar uma posição. O resultado disto é que o segundo rotor só avança a cada 26 caracteres e o terceiro quase nunca se move. Isto faz com que a Enigma seja mais previsível.

4. *O quarto rotor não se movia:*

   Na Enigma M4 naval, o rotor extra (Zusatswalze) pode ser definido para qualquer uma das 26 posições no inicio de uma mensagem. Durante a encriptação, contudo, esse rotor nunca se move. Juntamente com o refletor, este rotor pode ser considerado como uma seleção entre 26 refletores diferentes.

5. *Número fixo de cabos no painel de trocas:*

   O painel de trocas possuía 26 tomadas, uma para cada letra do alfabeto. Os cabos era usados para trocar pares de letras. Se um cabo era omitido, essa letra não podia ser trocada. Em teoria, qualquer número de cabos entre 0 e 13 seria assim possível, sendo que com 11 cabos se produzia o maior número de combinações. Na prática, os procedimentos obrigavam o uso de um número fixo de cabos (10 na maior parte dos casos), o que reduzia consideravelmente o número máximo de possibilidades.

A Enigma e a sua Matemática

Cada rotor é representado por um conjunto de permutações contendo todos os valores de letras entre 0 e 25.

Cada um dos rotores possui um conjunto de permutações único que denominaremos α_1, α_2, α_3 em que cada α_i representa as possíveis transições entre letras efetuada no interior do rotor.

Visto que cada rotor pode ser configurado manualmente, rodando a sua posição inicial, introduziremos as variáveis r_1, r_2 e r_3 que representam a configuração inicial de cada rotor (representam a letra apresentada no topo do rotor).

Para o propósito desta demonstração não teremos em conta o painel de trocas (como já vimos, este painel só consta nas versões militares da Enigma).

Por fim o refletor é matematicamente modelado como um conjunto de permutações entre pares de letras que denotaremos por β.

O objetivo será seguirmos o sinal elétrico desde que este deixa o teclado e atravessa todos os rotores ate ao refletor e volta para o teclado iluminado.

Para sermos capazes de calcular a letra cifrada para cada input dado vamos calcular a rotação em cada rotor, a permutação efetuada pelo refletor e todas as permutações no caminho de volta ao teclado iluminado.

Consideremos então os seguintes conjuntos de permutações:

α_1 = (0 15 6 10 14 8 19 17 22 18 11) (1 2 9 13 21 25) (3 4 23 5 24 7 12 16 20)
α_2 = (0 7 9 4 6 18 23 25 8) (1 17 19) (2 20 10) (3 12) (5 11 13 21) (14 22 15 16 24)
α_3 = (0 2 4 7 16 17 19 5) (1 6 3 8 21 24 11 13 9 10 25 12 14 15) (18 23 20 22)
β = (0 4) (1 7) (2 9) (3 16) (5 20) (6 8) (10 19) (11 17) (12 25) (13 18) (14 24) (15 22) (21 23)

Desta forma, no rotor 1 por exemplo, 0 é transformado em 15, 15 é transformado em 6 e 11 é transformado em 0 etc…

Cada conjunto de permutações possui um inverso, que desfaz a ação da permutação. Os conjuntos inversos são os seguintes:

α^{-1} = (11 18 22 17 19 8 14 10 6 15 0) (25 21 13 9 2 1) (20 16 12 7 24 5 23 4 3)
α^{-2} = (8 25 23 18 6 4 9 7 0) (19 17 1) (10 20 2) (12 3) (21 13 11 5) (24 16 15 22 14)
α^{-3} = (5 19 17 16 7 4 2 0) (15 14 12 25 10 9 3 11 24 21 8 3 6 1) (22 20 23 18)

Ao chegar ao refletor, que permuta entre pares de letras, obtemos:
(Output do rotor 3)$^{\beta}$ = output do refletor (agora em sentido inverso).
Ao seguirmos o sinal elétrico de volta ao teclado iluminado passando pelos rotores 3,2 e 1 respetivamente obtemos:

Rem[output refletor$^{\alpha 3 \wedge (-1)}$ - r3,26] = output rotor 3
Rem[output rotor 3$^{\alpha 2 \wedge (-1)}$ – r2,26] = output rotor 2
Rem[output rotor 2$^{\alpha 1 \wedge (-1)}$ – r1,26] = output rotor 1

Após completar a cifragem de uma letra e esta ser mostrada no painel iluminado, é necessário atualizar as posições dos rotores.

O rotor r1 (rotor rápido que é atualizado a cada letra premida) comporta-se matematicamente:

Rem[r1 + 1,26] e caso r1 = 25 ao adicionar 1, o novo valor de r1 será 0 e o rotor 2 (rotor médio) avança uma unidade e assim sucessivamente (ou seja a cada revolução completa de um rotor, o rotor à sua esquerda avança uma unidade).

Conclusão

Com a realização deste trabalho foi possível conhecer um dos marcos históricos da criptografia e a sua importância na codificação de mensagens secretas nos conflitos militares.

O trabalho permitiu aos alunos consolidar os conhecimentos no modelo de criptografia de chave simétrica e agilizar a utilização de aritmética modular.

Se por um lado foi possível constatar a capacidade impressionante da máquina Enigma, relativamente ao número de combinações possíveis que esta incluía na sua cifra, o trabalho realizado pela criptoanálise revelou-se crucial para o desfecho da segunda guerra mundial.

Bibliografia

Imagens:

Imagem 0: http://www.cryptomuseum.com/crypto/Enigma/d/img/301443/038/full.jpg

Imagem 1: https://upload.wikimedia.org/wikipedia/commons/3/31/Theo_A._van_Hengel.jpg

Imagem 2: http://cs-exhibitions.uni-klu.ac.at/uploads/pics/scherbius_02.jpg

Imagem 3: https://upload.wikimedia.org/wikipedia/commons/thumb/b/b3/Scherbius-1928-patent.png/440px-Scherbius-1928-patent.png

Imagem 4: http://cryptomuseum.com/crypto/Enigma/a/img/etz1f.jpg

Imagem 5: http://www.cryptomuseum.com/crypto/Enigma/d/img/301443/039/full.jpg

Imagem 6: http://www.cryptomuseum.com/crypto/Enigma/b/img/b_003_full.jpg

Imagem 7: http://www.cryptomuseum.com/crypto/Enigma/i/img/300002/018/full.jpg

Imagem 8: https://upload.wikimedia.org/wikipedia/commons/6/6c/Jerzy_Rozycki.jpg

Imagem 9: http://www.cryptomuseum.com/people/img/rejewski.jpg

Imagem 10: https://upload.wikimedia.org/wikipedia/commons/7/7d/Henryk_Zygalski.jpg

Imagem 11: http://www.cryptomuseum.com/crypto/bombe/img/bomba_3_full.jpg

Imagem 12: http://img-fotki.yandex.ru/get/9303/141128800.210/0_b4a3a_a2eebb97_orig.jpg

Imagem 13: http://www.cryptomuseum.com/people/img/turing_2s.jpg

Imagem 14: https://ichef.bbci.co.uk/news/624/media/images/75472000/jpg/_75472096_bp2.jpg

Imagem 15: https://upload.wikimedia.org/wikipedia/commons/thumb/b/b1/RebuiltBombeFrontView.jpg/300px-RebuiltBombeFrontView.jpg

Imagem 16: http://www.uboatarchive.net/U-110A/U-110INT-D.jpg

Imagem 17: http://www.cryptomuseum.com/crypto/Enigma/m3/img/m3_m2272_000_large.jpg

Imagem 18: http://www.cryptomuseum.com/crypto/Enigma/m4/img/300012/081/full.jpg

Imagem 19: http://www.thecorememory.com/assets/images/Joseph_R_Desch_NCR_194002.jpg

Imagem 20: http://www.cryptomuseum.com/crypto/bombe/img/us_bombe_full.jpg

Imagem 21: http://www.ilord.com/images/Enigma/Enigma-keyboard.jpg

Imagem 22: https://media2.s-nbcnews.com/j/newscms/2015_29/1121466/Enigma_3_d3482a08eb68df1d7162656018353265.nbcnews-ux-2880-1000.jpg

Imagem 24: http://www.cryptomuseum.com/crypto/Enigma/img/300684/010/full.jpg

Imagem 25: http://www.cryptomuseum.com/crypto/Enigma/img/300698/001/full.jpg

Imagem 26: http://www.cryptomuseum.com/crypto/Enigma/img/300698/002/full.jpg

Imagem 27: http://www.cryptomuseum.com/crypto/Enigma/img/300698/009/full.jpg

Imagem 28:
http://www.cryptomuseum.com/crypto/Enigma/i/img/300002/056/full.jpg

Imagem 29:
http://www.cryptomuseum.com/crypto/Enigma/img/300017/001/full.jpg

Imagem 30:
http://www.cryptomuseum.com/crypto/Enigma/img/300017/013/full.jpg

Imagem 31:
http://cryptomuseum.com/crypto/Enigma/i/img/300002/046/full.jpg

Imagem 32:
http://www.cryptomuseum.com/crypto/codebook/img/300357/000/full.jpg

Informação:

http://www.cryptomuseum.com/

Material didático fornecido pela docente.