Computação: Enigma

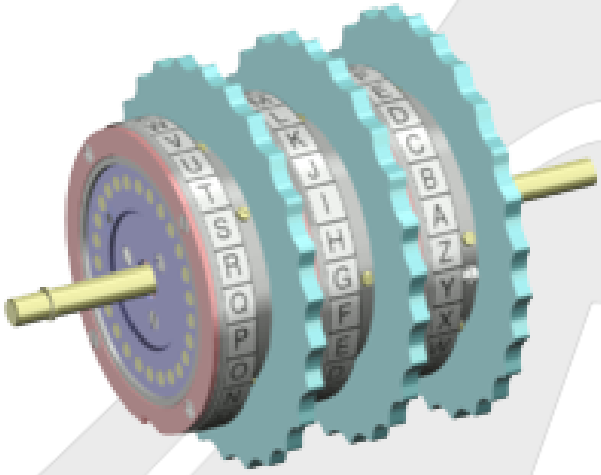
Marcos Santana | marcos_santana@ieee.org
Matheus Carnelutt | matheuschafrao@ieee.org

Computer Society - Tutorial 02

Os alemães continuam avançando contra as nossas linhas de defesa. Foi criada uma força tarefa como última esperança de recurso para que se possa virar a guerra a favor dos Aliados, e que tem uma difícil tarefa: quebrar a máquina nazista, Enigma.

Os nossos amigos poloneses foram os primeiros a estudar a máquina Enigma. Ela foi confiscada pela Alfandega certa vez, quando estava em seus primeiros modelos. A máquina possuía 3 rotores de 26 posições, como mostrado na Figura 1, que permitia incriveis 17.526 configurações diferentes. Todavia, os poloneses com muito esforço conseguiram quebrar a criptografia da máquina.

Figura 1: Rotores da Enigma



Fonte: Google Images.

Com o passar dos anos e com a eminencia da guerra, a máquina Enigma passou por uma série de upgrades para sua versão militar: agora eram 5 rotores de 26 posições(escolhia 3 dos 5 possíveis), que por sua vez implicava em 1.054.560 diferentes configurações iniciais. Como se não bastasse, a máquina possuía ainda um sistema elétrico chamado de "Plugboard"responsável por fazer um ciframento de letras, semelhante a cifra de césar, combinando 10 duplas ordenadas de 26 possíveis letras, o que dava 150.738.274.937.250 de possibilidades. Fazendo o produto dessas possibilidades, a máquina Enigma em sua versão militar possuía **158.962.555.217.826.360.000 (158 quintilhões)** diferentes configurações iniciais, um número assustador. [1]

Figura 2: Máquina Enigma

Fonte: Google Images.

A maquina Enigma é muito semelhante a uma máquina de escrever, como mostrada na Figura 2. Essa é uma das máquinas apreendidas pelos nossos soldados no campo de batalha, e será o objeto de estudo dessa força tarefa.

1 Como os nazistas utilizam a Enigma?

A nossa inteligência intercepta milhares de mensagens de rádio diariamente, que são transmitidos pelos nazistas para suas tropas e vice-versa, por meio de código morse, que é um código muito conhecido. Os alemães estão muito arrogantes com o que criaram, e não tem o mínimo de preocupação que suas mensagens sejam interceptadas, pois não acreditam que é possível quebrar a criptografia da poderosa máquina que criaram.

Descobrimos também que a configuração da máquina muda diariamente quando encontramos um caderno de configurações da Enigma usado por um esquadrão. O caderno possuía instruções de configurações dos próximos 7 dias, depois disso ele fica obsoleto. Esses cadernos são entregues por mensageiros nazistas, que o carregam dentro de uma garrafa que contem um poderoso ácido - caso ele for interceptado durante o seu percurso, bastava quebrar a garrafa para inutilizar o caderno.

A mudança da configuração da Enigma diariamente, dificulta ainda mais o trabalho da nossa força tarefa, pois temos apenas 24 horas para quebrar a criptografia e descobrir as configurações iniciais da Enigma, pois depois disso, toda a configuração muda, e todo o trabalho será perdido e terá sido em vão. Ou seja, temos 24 horas para testar mais de 158 quintilhões de combinações, o que nos dá aproximadamente $5 \cdot 10^{-16}$ segundos para cada tentativa, impossível até mesmo por um grupo constituído por milhares de pessoas.

**Confira o vídeo* `https://www.youtube.com/watch?v=VMJeDLv2suw` *para mais informações.*

2 Como a Engima Funciona?

A Máquina Enigma possui: 1 Teclado, 1 Lightboard, 1 Plugboard, 3 Rotores dinâmicos, 1 Rotor estático e 1 Refletor.

A primeira etapa é configurar a Enigma. Deve-se escolher 3 rotores e colocá-los em suas devidas posições, e após isso, setar o "offset", isto é, a posição em que cada rotor irá começar. Nessa etapa também é necessário encaixar os cabos na Plugboard (geralmente eram feitas de 2 à 10 conexões) para fazer o "ciframento".

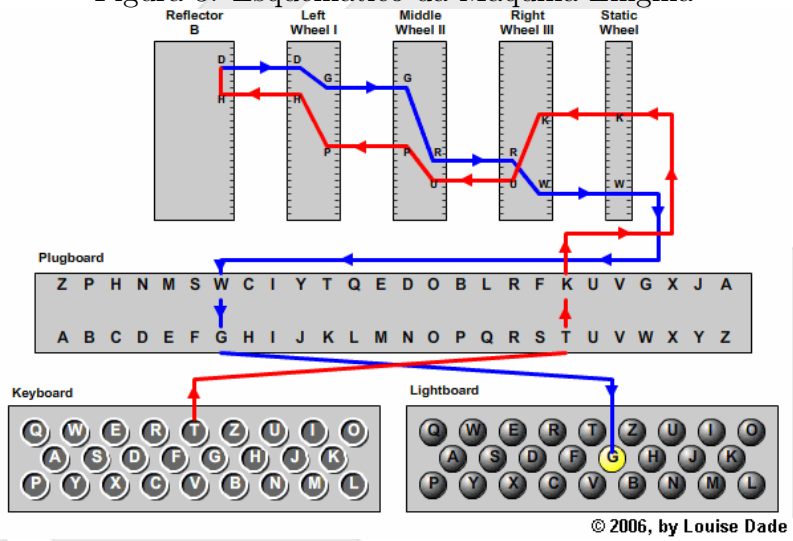
Após a máquina estar configurada, o operador anotava as configurações iniciais feitas, para que posteriormente, a mensagem fosse descriptografada. Ao pressionar uma letra, ela fazia um trajeto passando pelo:

Teclado -> Plugboard -> Rotor Estático -> Terceiro Rotor -> Segundo Rotor -> Primeiro Rotor - > Refletor -> Primeiro Rotor -> Segundo Rotor -> Terceiro Rotor -> Rotor Estátistico -> PlugBoard -> Lightboard

O Rotor estático é um Rotor fixo que continha o alfabeto (A Z) para servir de referência na entrada e saída. Os 3 rotores dinâmicos rotacionavam de acordo com uma condição: o terceiro rotor SEMPRE é rotacionado uma posição quando se pressiona alguma tecla, e quando ele atinge uma pré-determinada posição, ele faz o segundo girar uma posição, e por sua vez, quando o segundo rotor atinge uma pré-determinada posição, o primeiro rotor gira uma posição. O Refletor é um rotor fixo.

Todas as etapas estão descritas na Figura 3 abaixo. O caminho em vermelho é o que sai do teclado até o refletor, e o azul é o que volta do refletor até a Lightboard. Após finalizar o trajeto, a letra criptografada aparecia na Lightboard, e essa era anotada pelo operador. O conjunto dessas era a mensagem cifrada.

Figura 3: Esquemático da Máquina Enigma



Fonte: Google Images.

3 Como a força tarefa enfrentará a Enigma?

Ficou claro para a Força Tarefa que tentar todas as possíveis configurações para quebrar a máquina era impossível, dada o número de possibilidades. Logo, devemos explorar todas as fraquezas da máquina Enigma afim de diminuir o número de possíveis configurações, além de utilizar outros métodos de Criptoanálise já conhecidos.

1. Você conhece algum método de Criptoanálise? Quais? Caso não, pesquise sobre, e pense se ele poderia ser utilizado contra a Enigma (confira o vídeo `https://www.youtube.com/watch?v=_Eeg1LxVWa8`);

2. Pesquise em especial, sobre o método de Frequência para a Criptoanálise;

Depois de um profundo estudo da máquina, bem como testes realizados nas máquinas que possuíamos, conseguimos encontrar a maior falha na Enigma, e que se bem utilizada, pode ser crucial para o nosso sucesso: A letra digitada NUNCA seria representada no texto cifrado por ela mesma! [2]

Além disso, foi conseguido descriptografar algumas mensagens nazistas, e foi possível perceber um padrão. As primeiras mensagens do dia eram geralmente um relatório do clima (*Wetterbericht* em Alemão), e as mensagens sempre terminavam com a saudação nazista *Heil Hitler*.

3. Você conhece o método "crib"de criptoanálise? Pesquise sobre (confira o link: `http://www.ellsbury.com/bombe1.htm`);

A força tarefa enfim consegue achar uma fraqueza a ser explorada na Enigma, além de métodos para fazer ao mesmo. Como sabemos agora "o que procurar", podemos criar uma máquina que diminua as possibilidades através de "contradições", que não são nada mais que configurações impossíveis na máquina para gerar o texto "planejado", fazendo tudo isso através de tentativa e erro (brute force).

Figura 4: Bomba

Fonte: Google Images.

Assim, foi construída a "Bomba", uma máquina eletromecânica, mostrada na figura 4 planeada por Alan Turing - uma máquina de Turing. A máquina ficou responsável por examinar mensagens pelos métodos citados anteriormente, e assim, foi possível quebrar a mensagem!

Por mais incrível que seja a máquina projetada por Turing, precisamos descriptografar as mensagens de maneiras mais rápidas! Você ficou responsável por desenvolver um programa que funcione de forma semelhante a máquina Bomba, que por meio de métodos de criptoanálise citados, decifre as mensagens.

A nossa inteligência estará atualizando diariamente as mensagens interceptadas, e as colocará na seguinte página: `http://ieeeuel.org/enigma`. A página também será atualizadas com mais informações a cada dia a respeito da máquina Enigma, conforme a força tarefa avança, para auxiliar no seu trabalho.

Um dos nossos engenheiros conseguiu criar uma Réplica da Máquina Enigma em C++. Você pode usar ela para aplicar os seus conhecimentos de criptoanálise e decifrar a Enigma! Ele disponibilizou a máquina no seguinte repositório: `https://github.com/sb-uel/CS_Tutorial_02`

Os Aliados contam com você!

Referências

[1] O Enigma nazista e a Bomba de Turing. Disponível em: https://www.maisev.com/forum/off-topic/82401-o-enigma-nazista-e-bomba-de-turing.html. Acesso em 06 de Outubro de 2017

[2] Facts and Myths of Enigma: Breaking Stereotypes. Disponível em: https://link.springer.com/content/pdf/10.1007/3-540-39200-9_7.pdf. Acesso em 06 de Outubro de 2017