



# Criptografia de Rotor

E suas falhas



# Máquina de Hebern

---



- O funcionamento da máquina é igual a cifra de Viginere, com tamanho conhecido\*, portanto, basta aplicar a criptoanálise para esse sistema
  - Assumindo que sabe-se a quantidade de rotores
  - A análise é ainda mais fácil que uma análise de Viginere comum, dado que nenhuma letra pode ser repetida na senha
- Mesmo usando mais rotores, como a rotação deles é predeterminada e funciona como um hodômetro, ela pode ser decriptada pelo teste kappa.

# Enigma e suas espertezas (ou quase)

---



- Para facilitar seu uso, a máquina da enigma não tem um carácter mapeado para ele mesmo
  - Reduz imensamente as possibilidades de permutações.
- Senhas de usuários.
- A redundância no envio de senha provou ser uma falha imensa.

# Anatomia de uma mensagem real

---



1035 – 90 – 341 –

PKPJX IGCDS EAHUG WTQGR

KVLFG XUCAL XVYMI GMMNM

FDXTG NVHVR MMEVO UYFZS

LRHDR RXFJW CFHUH MUNZE

FRDIS IKBGP MYVXU Z

# Anatomia de uma mensagem real

---



1035 – 90 – 341 –

PKPJX IGCDS EAHUG WTQGR

KVLFG XUCAL XVYMI GMMNM

FDXTG NVHVR MMEVO UYFZS

LRHDR RXFJW CFHUH MUNZE

FRDIS IKBGP MYVXU Z

Assim, a senha é “facilmente” obtida. O que fazer com ela agora?



# Background matemático

---

- Permutações, notação e operações;

$$H = \begin{pmatrix} \textit{qwertyuiopasdfghjklpxcvbnml} \\ \textit{abcdefghijklmnopqrstuvwxyz} \end{pmatrix}$$

$$AD = (\textit{dvpfkxgzyo})(\textit{eijmunglht})(\textit{bc})(\textit{rw})(\textit{a})(\textit{s})$$

$$BE = (\textit{blfqveoum})(\textit{hjpswizrn})(\textit{axt})(\textit{cgy})(\textit{d})(\textit{k})$$

$$CF = (\textit{abviktjgf cqny})(\textit{duzrehlxwpsmo})$$

# Rejewski's Characteristics

---



- sejam  $A, B, C, D, E, F$  as permutações usadas para encriptar a senha da mensagem. sabemos que:
  - $c1 \cdot A^{-1} = p1 = p4 = c4 \cdot D^{-1} \Rightarrow c1 \cdot A^{-1} \cdot D = c4$
  - $c2 \cdot B^{-1} = p2 = p5 = c5 \cdot E^{-1} \Rightarrow c2 \cdot B^{-1} \cdot E = c5$
  - $c3 \cdot C^{-1} = p3 = p6 = c6 \cdot F^{-1} \Rightarrow c3 \cdot C^{-1} \cdot F = c6$
- Como a Enigma é simétrica:  $AA = I$ , portanto  $A = A^{-1}$ :
  - $c1 \cdot AD = c4$
  - $c2 \cdot BE = c5$
  - $c3 \cdot CF = c6$

Essas equações eram conhecidas como as “características de Rejewski”)



# Exemplo simplificado

---

- As permutações foram calculadas, e a senha RYZOLZ apareceu 5 vezes nas senhas capturadas

$AD = (\text{pjxroquctwzsy})(\text{kvgledmanhfib})$

$BE = (\text{kxtcoigweh})(\text{zvfbsylrnp})(\text{ujd})(\text{mqa})$

$CF = (\text{yvxqtdhpim})(\text{skgrjbcoll})(\text{un})(\text{fa})(\text{e})(\text{z})$

como Z só pode ser trocado por E na permutação CF, podemos testar se a senha eh EEE. Para isso, R+O e Y+L precisam poder ser trocados (estar no mesmo ciclo, e no oposto que o do suposto plain text).



# Exemplo simplificado

- Assim, podemos calcular as seguintes permutações:

$$A = (\text{er})(\text{dx})(\text{jm})(\text{ap})(\text{ny})(\text{hs})(\text{fz})(\text{iw})(\text{bt})(\text{ck})(\text{uv})(\text{gq})(\text{lo})$$
$$D = (\text{eo})(\text{lq})(\text{gu})(\text{cv})(\text{kt})(\text{bw})(\text{iz})(\text{fs})(\text{hy})(\text{np})(\text{ag})(\text{mx})(\text{dr})$$
$$B = (\text{ey})(\text{hs})(\text{kb})(\text{xf})(\text{tv})(\text{cz})(\text{op})(\text{in})(\text{gr})(\text{wl})\dots$$
$$E = (\text{le})(\text{rw})(\text{ng})(\text{pi})(\text{zo})(\text{vc})(\text{ft})(\text{bx})(\text{sk})(\text{yh})\dots$$

que podem ser usadas para traduzir as senhas para plaintext.

# Quebrando as senhas

---



1. Sniffar várias mensagens (no mínimo 60, quanto mais melhor)
2. Acreditar na incapacidade humana de gerar senhas.
3. Gerar as permutações.
4. procurar senhas frequentes para usar o ataque anterior.

# Sistema desconhecido

---



- Como as conexões dos rotores não são conhecidos, as senhas não podem ser usadas na Enigma.

Lembrando do funcionamento interno da Enigma, podemos abrir cada permutação em várias outras. Sejam as permutações:

- S: Plugboard (stecker)
- H: ligação entre o teclado e saída
- R: refletor
- L, M, N: rotores
- P: rotação do rotor



# Sistema desconhecido

$$A = SH(P^1 NP^{-1})LMRM^{-1}L^{-1}(P^1 N^{-1} P^{-1})H^{-1}S^{-1}$$

$$B = SH(P^2 NP^{-2})LMRM^{-1}L^{-1}(P^2 N^{-1} P^{-2})H^{-1}S^{-1}$$

$$C = SH(P^3 NP^{-3})LMRM^{-1}L^{-1}(P^3 N^{-1} P^{-3})H^{-1}S^{-1}$$

$$D = SH(P^4 NP^{-4})LMRM^{-1}L^{-1}(P^4 N^{-1} P^{-4})H^{-1}S^{-1}$$

$$E = SH(P^5 NP^{-5})LMRM^{-1}L^{-1}(P^5 N^{-1} P^{-5})H^{-1}S^{-1}$$

$$F = SH(P^6 NP^{-6})LMRM^{-1}L^{-1}(P^6 N^{-1} P^{-6})H^{-1}S^{-1}$$

L e M (rotores do meio e direita) não rotacionam para a senha. H é fixo e, para a Enigma do exercito, era a identidade.  
Portanto, S, N, L, M, R, e P são desconhecidos



# Sistema desconhecido

$$U = P^{-1} H^{-1} S^{-1} A S H P^1$$

$$= (NP^{-1})Q(P^1 N^{-1})$$

$$V = P^{-2} H^{-1} S^{-1} B S H P^2$$

$$= (NP^{-2})Q(P^2 N^{-1})$$

$$W = P^{-3} H^{-1} S^{-1} C S H P^3$$

$$= (NP^{-3})Q(P^3 N^{-1})$$

$$X = P^{-4} H^{-1} S^{-1} D S H P^4$$

$$= (NP^{-4})Q(P^4 N^{-1})$$

$$Y = P^{-5} H^{-1} S^{-1} E S H P^5$$

$$= (NP^{-5})Q(P^5 N^{-1})$$

$$Z = P^{-6} H^{-1} S^{-1} F S H P^6$$

$$= (NP^{-6})Q(P^6 N^{-1})$$

$$VW = NP^{-1} N^{-1} (UV)NP^1 N^{-1}$$

$$WX = NP^{-1} N^{-1} (VW)NP^1 N^{-1}$$

$$XY = NP^{-1} N^{-1} (WX)NP^1 N^{-1}$$

$$YZ = NP^{-1} N^{-1} (XY)NP^1 N^{-1}$$

Aqui temos apenas  
 $NP^{-1}N^{-1}$  como uma  
permutação desconhecida

$$Q = L M R M^{-1} L^{-1}$$

$$UV = (NP^{-1})Q(P^1 N^{-1})(NP^{-2})Q(P^2 N^{-1}) = NP^{-1}(QP^{-1}QP)P^1 N^{-1}$$

$$VW = (NP^{-2})Q(P^2 N^{-1})(NP^{-3})Q(P^3 N^{-1}) = NP^{-2}(QP^{-1}QP)P^2 N^{-1}$$

$$WX = (NP^{-3})Q(P^3 N^{-1})(NP^{-4})Q(P^4 N^{-1}) = NP^{-3}(QP^{-1}QP)P^3 N^{-1}$$

$$XY = (NP^{-4})Q(P^4 N^{-1})(NP^{-5})Q(P^5 N^{-1}) = NP^{-4}(QP^{-1}QP)P^4 N^{-1}$$

$$YZ = (NP^{-5})Q(P^5 N^{-1})(NP^{-6})Q(P^6 N^{-1}) = NP^{-5}(QP^{-1}QP)P^5 N^{-1}$$

# Sistema desconhecido

---



Tendo as permutações A,B,...,F, podemos derivar U, V, W, X, Y, Z. Depois, multiplicamos elas para obter as permutações compostas.

Como P significa rotacionar o rotor, N e P podem ser derivados a partir do valor composto. Assim, podemos calcular como as letras do rotor estão conectadas, basta escrever todas as permutações N, com diferentes valores de shift. Uma dessas deve estar correta.

# Método da Grelha

---



Com a permutação N conhecida, mas não sua posição inicial, podemos usar as permutações A - F para determinar a posição inicial do rotor.

Para isso, foram escritas 31 permutações de N (26 rotações + repetição das primeiras), e criada uma folha onde pode-se escrever as permutações A - F e comparar com a posição do rotor. Aquela em que todas as permutações estiverem corretas, é a posição certa.

# Método da Grelha

---



Seria simples assim determinar a senha do dia, se não fosse por um pequeno detalhe: a plugboard.

Como as conexões da plugboard são desconhecidas, nenhum valor da grelha vai estar 100% correto. Os criptoanalistas teriam que encontrar aquela que se encaixava melhor.

Uma vez descoberto, no entanto, também se tinha a informação das conexões da plugboard.

# Método da Grelha

---



Por fim, falta determinar a permutação Q. Isso poderia ser feito via brute force, já que havia apenas  $26 \times 26 = 676$  possibilidades de posições iniciais, e 2 maneiras de ordenar os rotores, totalizando 1352 valores a serem testados.



# Segunda guerra mundial

---

Esses esforços acabaram por serem parcialmente desfeitos até a segunda guerra mundial. Em 1938, a Alemanha já havia trocado o método de envio de senhas, criptografando-as usando 2 senhas diárias diferentes (uma para cada vez que fosse encriptado), dificultando a obtenção de A - F.

# Folha de Zygalski

---



Zygalski (outro criptoanalista polonês) percebeu que ainda haviam repetições nas letras, e estas só ocorreriam com senhas e caracteres específicos.

Ao juntar 10 senhas diferentes com repetições de caracteres, podia-se usar uma folha com matrizes de perfurações criada por Zygalski para determinar a senha da mensagem.

# Bomba (Polonesa)

---



Rejewski então criou uma máquina para automatizar a busca por senhas possíveis, fazendo um brute-force na folha de Zygalski.

6 Bombas foram criadas para aumentar a velocidade da busca.

A máquina funcionou até 1938, quando os alemães introduziram 2 novos rotores, o que aumentou a quantidade de máquinas necessárias para 60, sendo infactivel continuar a solução dessa maneira.

# Método do Berço (Crib)

---



Com medo de que, eventualmente, repetições de letras nas senhas fossem proibidas, os ingleses desenvolveram outro método de quebrar a enigma, chamado de método do berço;

Um Crib (berço) seria um plaintext conhecido, ou assumido. Criptoanalistas usariam expressões comuns (ANX, “to” em alemão e X como espaço, por exemplo), procuraram regiões no ciphertext em que nenhuma letra fosse encriptada para ela mesma, e tentariam decifrar a enigma usando esse conhecimento.

# Bomba (Britânica)

---



Inspirado no método do Berço, Alan turing projetou uma máquina que seria capaz de testar todas as quase 18 mil possibilidades de posicionamento de rotores, procurando por falhas (letra encriptada para ela mesma, por exemplo).

Graças a quantidade de restrições forçadas nos operadores de enigmas, várias possibilidades poderiam ser removidas (uma letra conectada via plug board em outra adjacente foi uma regra que acelerou muito o processo).

# Bomba (Britânica)

---



Diferentemente do credo popular, no entanto, a bomba não resolia tudo sozinha. Para decriptar uma mensagem, um criptoanalista geraria um Crib, decidiria quais posições de rotores poderiam ser ignoradas e rodava o teste.

De posse da resposta (múltiplas senhas possíveis), o criptoanalista deveria, então, tentar procurar nesse grupo reduzido, qual senha era correta.