Cifras de rotor

A evolução da criptografia mecânica

Introdução e história

Introdução e história

- A cifra de Vigenère foi considerada indecifrável por 3 séculos

Introdução e história

- A cifra de Vigenère foi considerada indecifrável por 3 séculos
- Mesmo após ter sido quebrada, a dificuldade na decriptação era diretamente proporcional ao tamanho da chave
  - Chaves muito grandes tornavam difícil o processo de criptoanálise

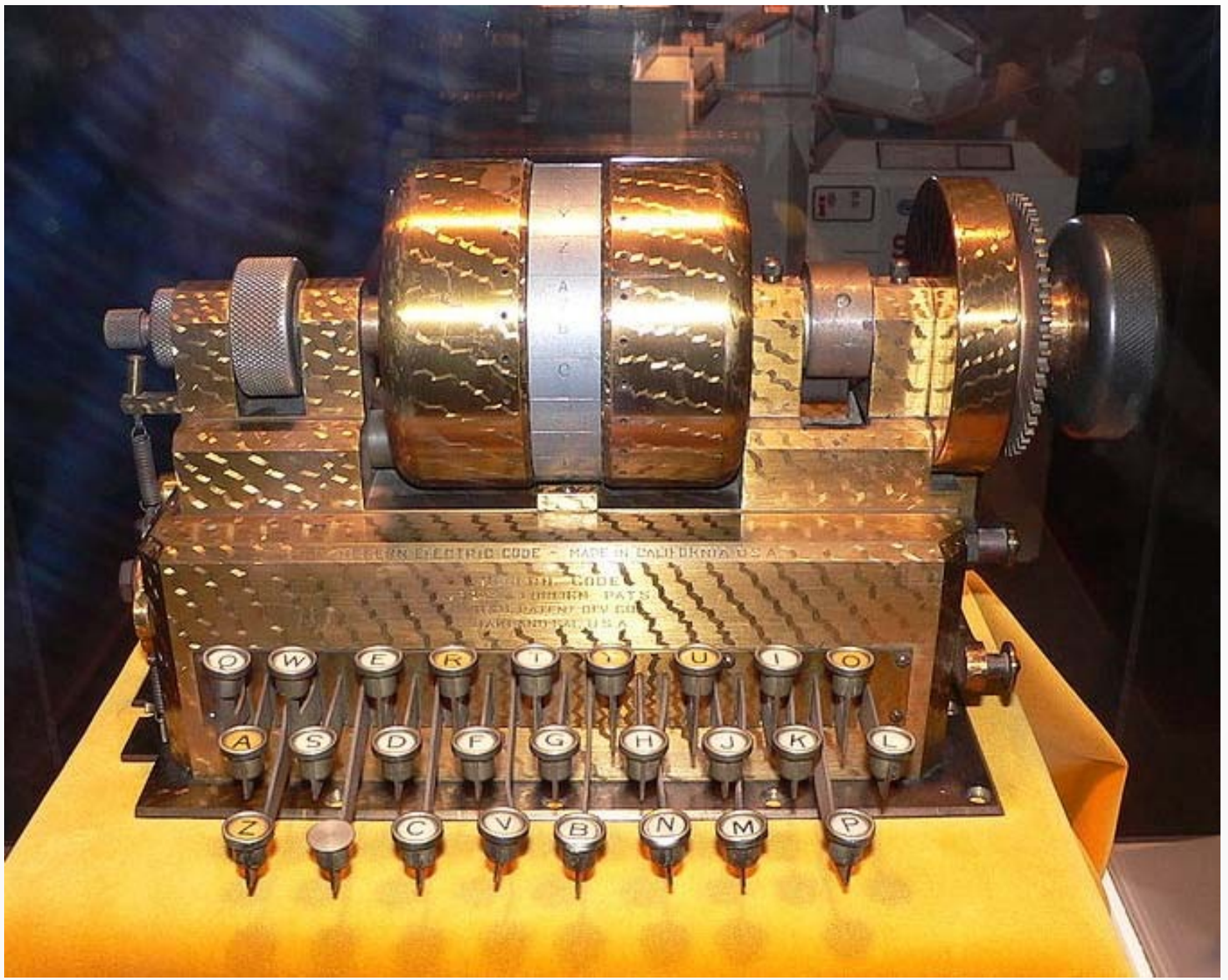
Introdução e história

- A cifra de Vigenère foi considerada indecifrável por 3 séculos
- Mesmo após ter sido quebrada, a dificuldade na decriptação era diretamente proporcional ao tamanho da chave
  - Chaves muito grandes tornavam difícil o processo de criptoanálise
- Objetivo: criar uma cifra de substituição com chave grande o suficiente mas de fácil utilização

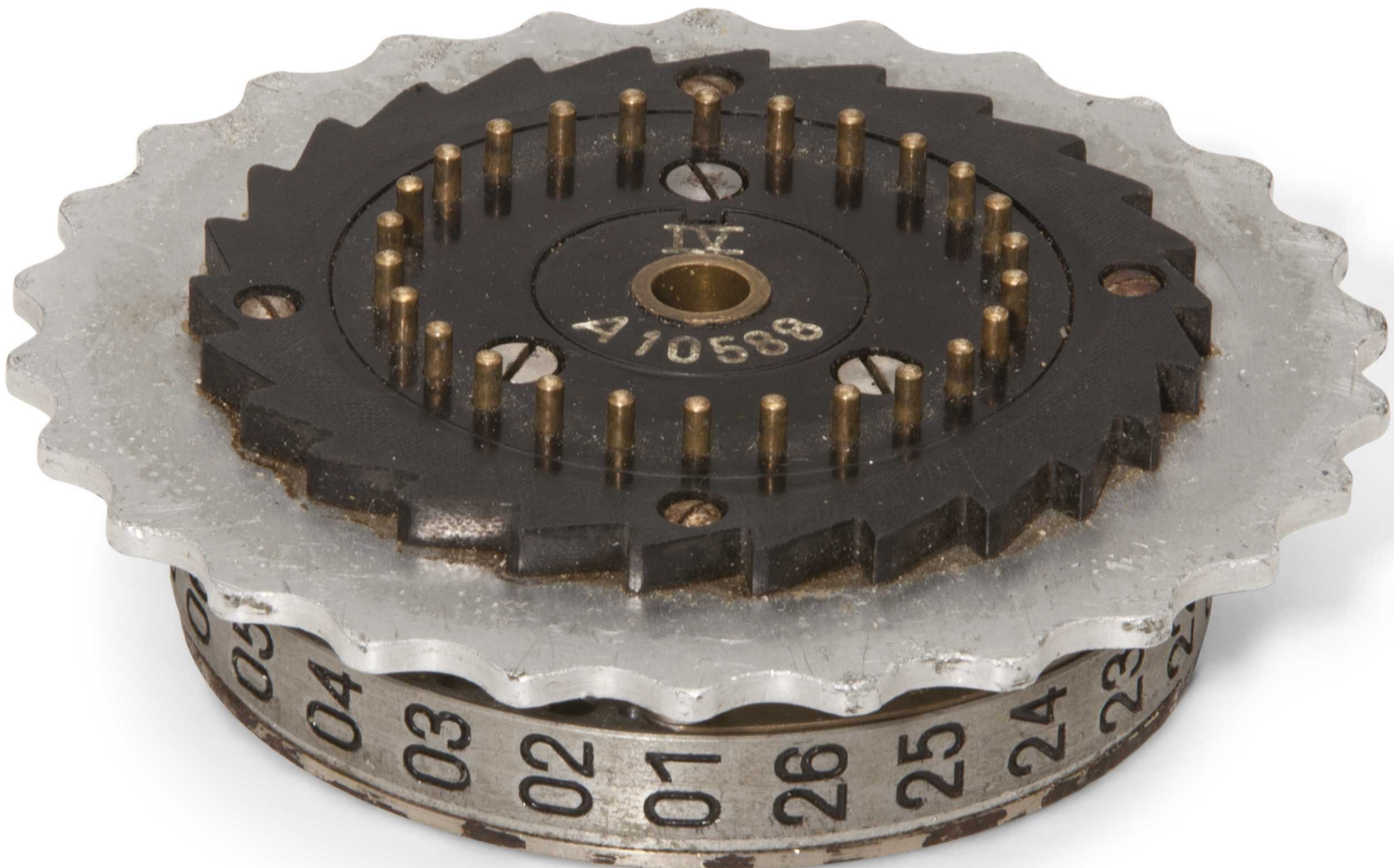
Introdução e história

- A cifra de Vigenère foi considerada indecifrável por 3 séculos
- Mesmo após ter sido quebrada, a dificuldade na decriptação era diretamente proporcional ao tamanho da chave
  - Chaves muito grandes tornavam difícil o processo de criptoanálise
- Objetivo: criar uma cifra de substituição com chave grande o suficiente mas de fácil utilização
  - Máquinas de rotor

Máquina de Hebern



Rotor simples



Funcionamento

Funcionamento

- Segue o mesmo princípio da cifra de Vigenère

Funcionamento

- Segue o mesmo princípio da cifra de Vigenère
  - O rotor é uma “chave”
    - As conexões entre o contato interno e externo determinam o mapeamento entre pares de letras

Funcionamento

- Segue o mesmo princípio da cifra de Vigenère
  - O rotor é uma “chave”
    - As conexões entre o contato interno e externo determinam o mapeamento entre pares de letras
  - Cada letra da mensagem original é cifrada de forma diferente, a depender da posição do rotor
    - Ao digitar, o rotor gira automaticamente, criando um novo mapeamento

Funcionamento

- Segue o mesmo princípio da cifra de Vigenère
  - O rotor é uma “chave”
    - As conexões entre o contato interno e externo determinam o mapeamento entre pares de letras
  - Cada letra da mensagem original é cifrada de forma diferente, a depender da posição do rotor
    - Ao digitar, o rotor gira automaticamente, criando um novo mapeamento
- Para decriptar uma mensagem encriptada, basta colocar o rotor na posição inversa

Problemas

- Um rotor possui um tamanho fixo e relativamente pequeno de mapeamentos
  - Em textos grandes, torna-se **menos** seguro que a cifra de Vigenère

Problemas

- Um rotor possui um tamanho fixo e relativamente pequeno de mapeamentos
  - Em textos grandes, torna-se **menos** seguro que a cifra de Vigenère
- O único fator desconhecido é a posição inicial do rotor
  - Escolher 1 entre n (pequeno) rotores não melhoraria significativamente a segurança

Problemas

- Um rotor possui um tamanho fixo e relativamente pequeno de mapeamentos
  - Em textos grandes, torna-se **menos** seguro que a cifra de Vigenère
- O único fator desconhecido é a posição inicial do rotor
  - Escolher 1 entre n (pequeno) rotores não melhoraria significativamente a segurança
- Como consequência, foi quebrado logo que se tornou comercial

Problemas

- Um rotor possui um tamanho fixo e relativamente pequeno de mapeamentos
  - Em textos grandes, torna-se **menos** seguro que a cifra de Vigenère
- O único fator desconhecido é a posição inicial do rotor
  - Escolher 1 entre n (pequeno) rotores não melhoraria significativamente a segurança
- Como consequência, foi quebrado logo que se tornou comercial
- Além disso, a decriptação de um texto não era facilitada

Aumentando a segurança

Aumentando a segurança

- Utilizar vários rotores interligados
  - A saída do rotor à direita é a entrada do rotor à esquerda
  - Aumenta drasticamente o tamanho da chave

Aumentando a segurança

- Utilizar vários rotores interligados
  - A saída do rotor à direita é a entrada do rotor à esquerda
  - Aumenta drasticamente o tamanho da chave
- Definir a posição inicial do rotor para cada mensagem
  - Posição da “chave” é alterada

Aumentando a segurança

- Utilizar vários rotores interligados
  - A saída do rotor à direita é a entrada do rotor à esquerda
  - Aumenta drasticamente o tamanho da chave
- Definir a posição inicial do rotor para cada mensagem
  - Posição da “chave” é alterada
- Rotacioná-los sobre seu próprio eixo, alterando as conexões internas do rotor
  - Produz um “shift” no mapeamento

Aumentando a segurança

- Se a posição relativa entre os rotores for fixa, não é difícil descobrir a chave por força bruta

Aumentando a segurança

- Se a posição relativa entre os rotores for fixa, não é difícil descobrir a chave por força bruta
  - Solução: trocar a ordem dos rotores dentro da máquina

Aumentando a segurança

- Se a posição relativa entre os rotores for fixa, não é difícil descobrir a chave por força bruta
  - Solução: trocar a ordem dos rotores dentro da máquina
- Escolher n entre N possibilidades de rotores

Aumentando a segurança

- Se a posição relativa entre os rotores for fixa, não é difícil descobrir a chave por força bruta
  - Solução: trocar a ordem dos rotores dentro da máquina
- Escolher n entre N possibilidades de rotores
- Fazer uma substituição das letras
  - Utilizando pares de plugues, é possível redirecionar o sinal elétrico de uma tecla para outra

Os números impressionam...

- Em uma máquina de 3 rotores com 5 disponíveis:

Os números impressionam...

- Em uma máquina de 3 rotores com 5 disponíveis:
  - 5x4x3 = 60 possibilidades de rotores

Os números impressionam...

- Em uma máquina de 3 rotores com 5 disponíveis:
  - 5x4x3 = 60 possibilidades de rotores
  - 3x2x1 = 6 possibilidades de permutação

Os números impressionam...

- Em uma máquina de 3 rotores com 5 disponíveis:
  - 5x4x3 = 60 possibilidades de rotores
  - 3x2x1 = 6 possibilidades de permutação
  - 26x26x26 = 17576 possibilidades de definir a posição inicial dos rotores

Os números impressionam...

- Em uma máquina de 3 rotores com 5 disponíveis:
  - 5x4x3 = 60 possibilidades de rotores
  - 3x2x1 = 6 possibilidades de permutação
  - 26x26x26 = 17576 possibilidades de definir a posição inicial dos rotores
  - 26x26x26 = 17576 mapeamentos entre as conexões internas dos rotores

Os números impressionam...

- Em uma máquina de 3 rotores com 5 disponíveis:
  - 5x4x3 = 60 possibilidades de rotores
  - 3x2x1 = 6 possibilidades de permutação
  - 26x26x26 = 17576 possibilidades de definir a posição inicial dos rotores
  - 26x26x26 = 17576 mapeamentos entre as conexões internas dos rotores
  - $\frac{26!}{13!*2^{13}} = 7{,}9*10^{12}$ substituições de letras

Os números impressionam...

- Em uma máquina de 3 rotores com 5 disponíveis:
  - 5x4x3 = 60 possibilidades de rotores
  - 3x2x1 = 6 possibilidades de permutação
  - 26x26x26 = 17576 possibilidades de definir a posição inicial dos rotores
  - 26x26x26 = 17576 mapeamentos entre as conexões internas dos rotores
  - $\frac{26!}{13!*2^{13}} = 7{,}9*10^{12}$ substituições de letras
  - Total: $8{,}8*10^{23}$ possibilidades de encriptação

Enigma – muito mais robusta

- Eventualmente implementou todas as soluções discutidas anteriormente

Enigma – muito mais robusta

- Eventualmente implementou todas as soluções discutidas anteriormente
  - Em suas primeiras versões, havia apenas 3 rotores disponíveis, sendo 3 suportadas

Enigma – muito mais robusta

- Eventualmente implementou todas as soluções discutidas anteriormente
  - Em suas primeiras versões, havia apenas 3 rotores disponíveis, sendo 3 suportadas
  - Posteriormente passou-se a utilizar 5 rotores, com exceção da marinha, que utilizava 8

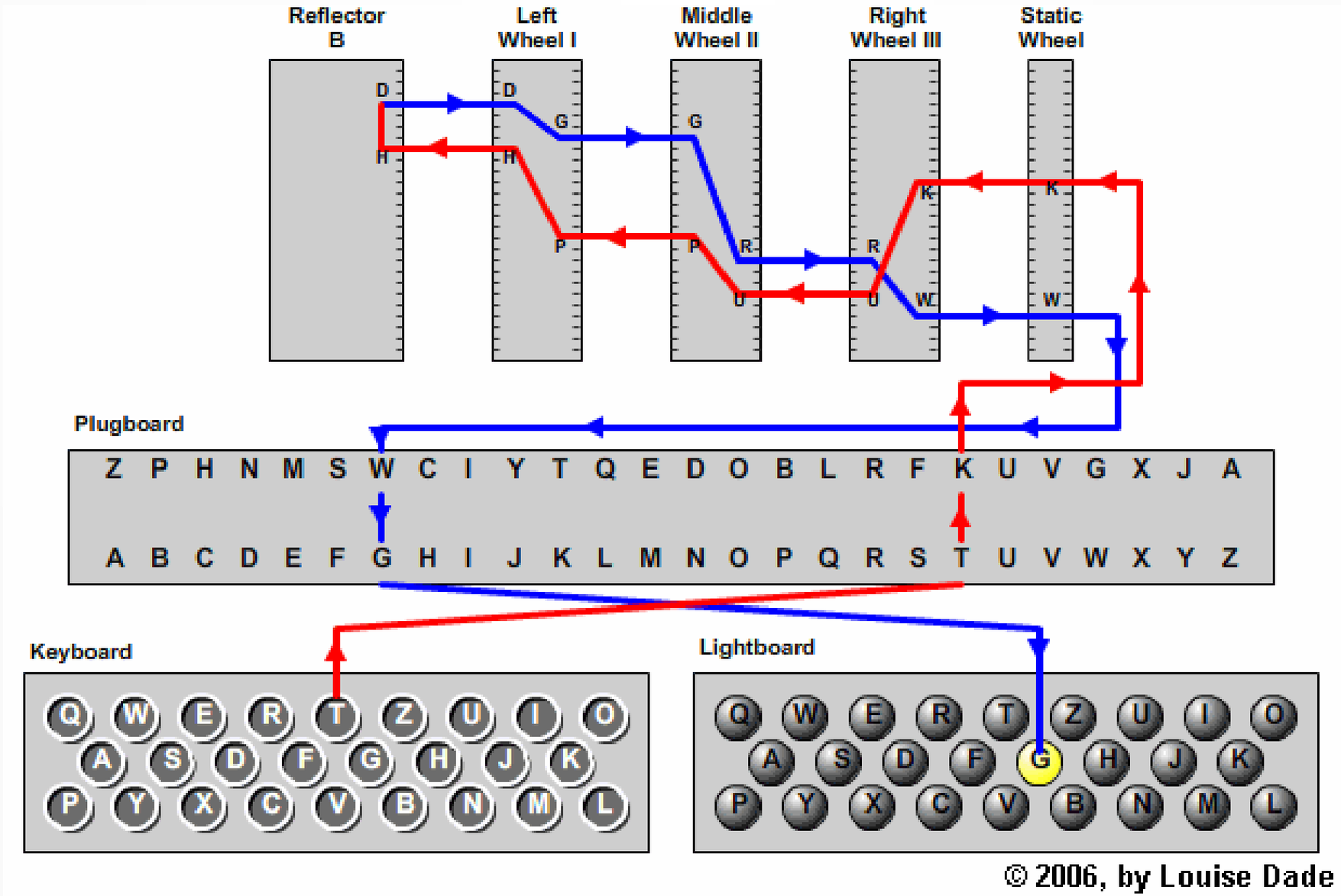
Enigma – muito mais robusta

- Eventualmente implementou todas as soluções discutidas anteriormente
  - Em suas primeiras versões, havia apenas 3 rotores disponíveis, sendo 3 suportadas
  - Posteriormente passou-se a utilizar 5 rotores, com exceção da marinha, que utilizava 8
  - Inicialmente não havia o *plug-board*, o qual passou a ser utilizado durante a guerra

Enigma – muito mais robusta

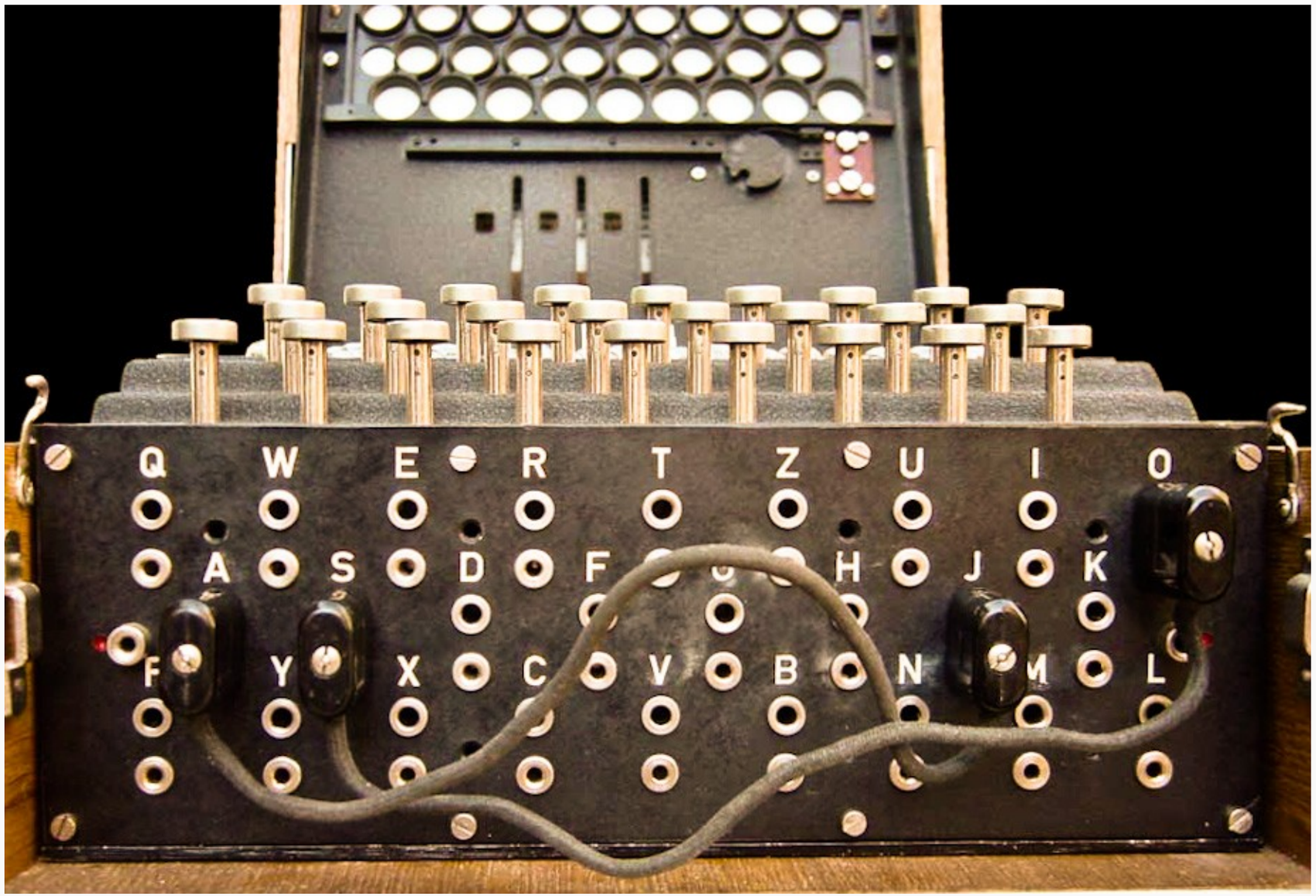
- Eventualmente implementou todas as soluções discutidas anteriormente
  - Em suas primeiras versões, havia apenas 3 rotores disponíveis, sendo 3 suportadas
  - Posteriormente passou-se a utilizar 5 rotores, com exceção da marinha, que utilizava 8
  - Inicialmente não havia o *plug-board*, o qual passou a ser utilizado durante a guerra
- Incluiu um refletor após o último rotor
  - Permitia simetria entre a encriptação e a decriptação

Enigma - encriptação



Enigma

Enigma - plugboard



Decifrando a Enigma

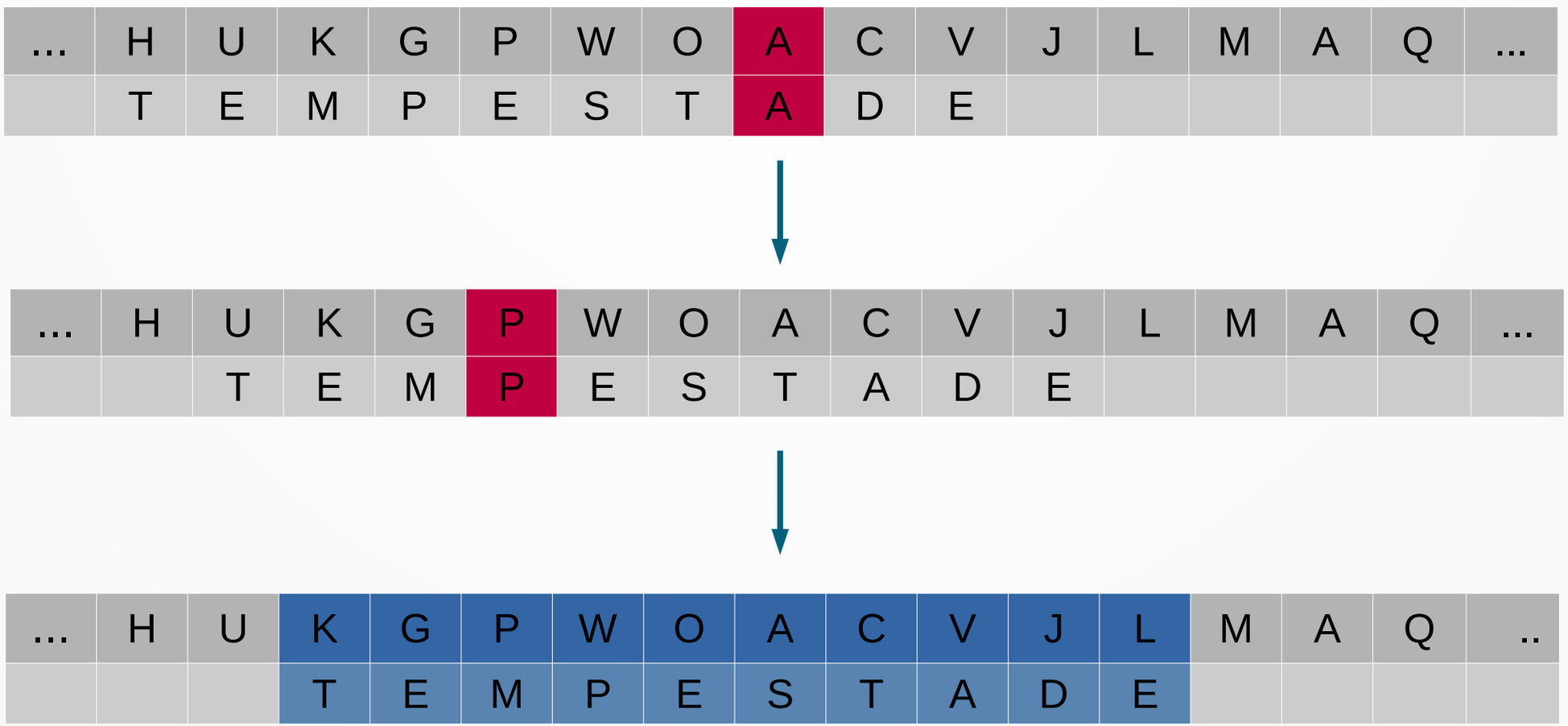
Decifrando a Enigma

- Devido ao funcionamento da Enigma e do seu refletor, uma letra nunca era mapeada para ela mesma
  - Grande falha de segurança: reduzia drasticamente as possibilidades de força bruta

Decifrando a Enigma

- Devido ao funcionamento da Enigma e do seu refletor, uma letra nunca era mapeada para ela mesma
  - Grande falha de segurança: reduzia drasticamente as possibilidades de força bruta
- Durante a Segunda Guerra mundial, os alemães utilizavam padrões conhecidos de escrita e muitas palavras repetidas
  - Permitia comparar a mensagem cifrada com palavras mais prováveis de estarem no texto original

Decifrando a Enigma - exemplo



Decifrando a Enigma – passo a passo

1) Configure os rotores para uma posição inicial qualquer
2) Para a primeira letra da mensagem original, chute uma letra qualquer para ser seu par no *plug-board*
3) Tecle a letra obtida no passo 2 na Enigma e anote o resultado
4) Com a letra obtida no passo 3 e a sua letra correspondente na mensagem encriptada, deduzimos um novo par no *plug-board*
5) Utilizando apenas pares já conhecidos, utilize o mesmo procedimento anterior para obter novos pares
    1) Se houver conflito entre dois pares, o par chutado inicialmente está errado e deve ser refeito
        1) Se todas as suposições resultarem em conflito, a posição inicial dos rotores está errada
    2) Se não houver conflito, uma possível configuração foi descoberta

Erros cometidos

Erros cometidos

- Padronização das mensagens
  - “Previsão do tempo” e palavras relacionadas
  - “Heil Hitler” no final de cada mensagem
  - Começar certas mensagens com “continuação”

Erros cometidos

- Padronização das mensagens
  - “Previsão do tempo” e palavras relacionadas
  - “Heil Hitler” no final de cada mensagem
  - Começar certas mensagens com “continuação”
- Regras para a escolha de rotores
  - Nenhum rotor poderia ser colocado na mesma posição que foi utilizado na configuração anterior

Erros cometidos

- Utilização da mesma configuração para enviar múltiplas mensagens seguidas

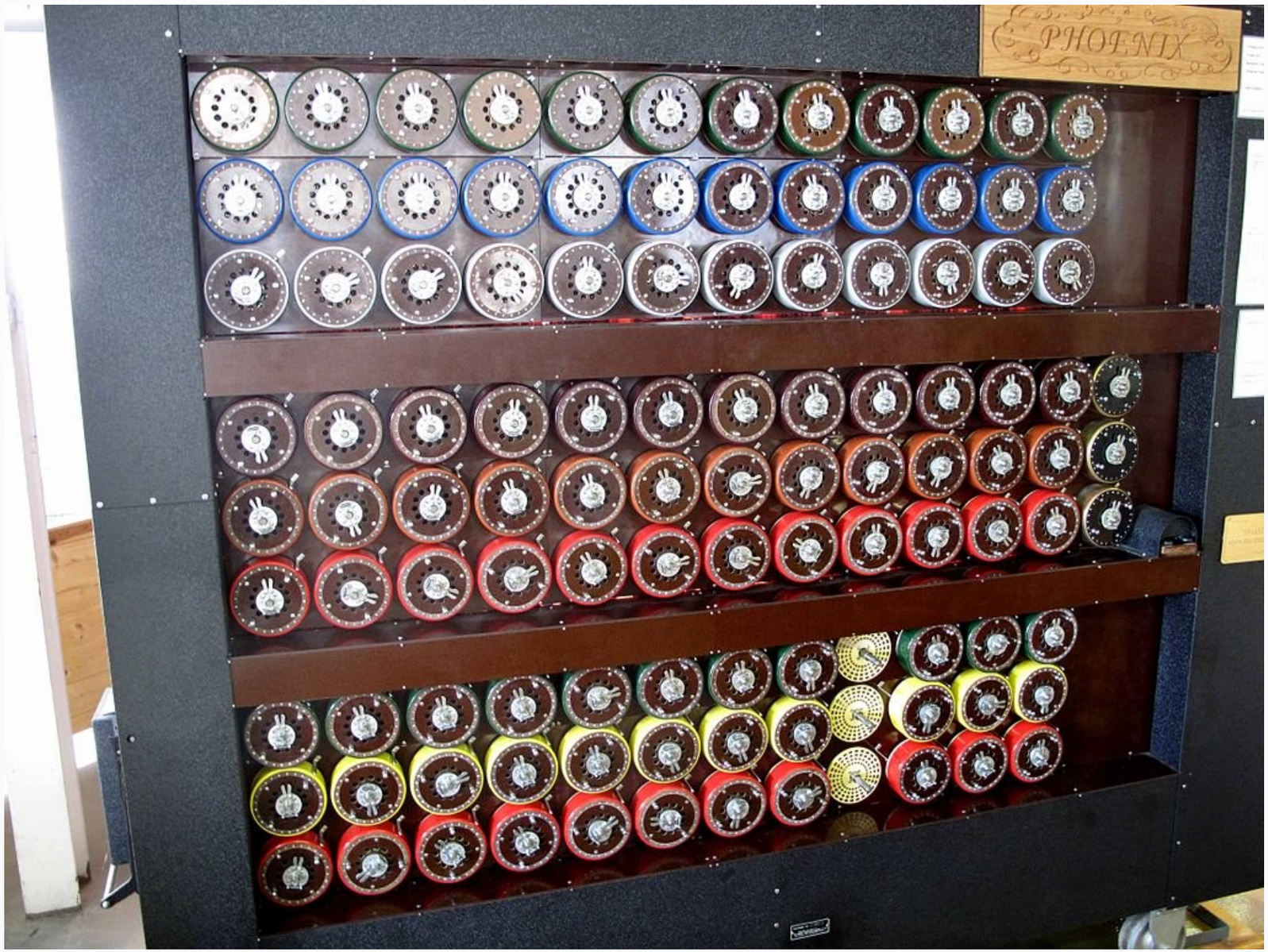
Erros cometidos

- Utilização da mesma configuração para enviar múltiplas mensagens seguidas
  - Alta probabilidade de existirem duas mensagens com a mesma posição inicial dos rotores ou que diferem apenas no mais lento

Erros cometidos

- Utilização da mesma configuração para enviar múltiplas mensagens seguidas
  - Alta probabilidade de existirem duas mensagens com a mesma posição inicial dos rotores ou que diferem apenas no mais lento
  - “Banburismus”: processo criptoanalítico desenvolvido por Turing para explorar essa falha
    - Permitiu selecionar as opções mais prováveis para os dois rotores da direita
    - Diminuiu drasticamente o tempo necessário para quebrar as configurações utilizadas diariamente

Réplica da “Bombe”



Typex - “Enigma britânico”

Typex - melhorias

- Utilizava 5 rotores ao invés de 3 ou 4 da Enigma
  - Cada rotor possuía diferentes *turn-points*
  - Adicionalmente, 2 rotores eram fixos e simulavam o *plug-board* da Enigma

Typex - melhorias

- Utilizava 5 rotores ao invés de 3 ou 4 da Enigma
  - Cada rotor possuía diferentes *turn-points*
  - Adicionalmente, 2 rotores eram fixos e simulavam o *plug-board* da Enigma
- Permitia que letras fossem substituídas por elas mesmas

Typex - melhorias

- Utilizava 5 rotores ao invés de 3 ou 4 da Enigma
  - Cada rotor possuía diferentes *turn-points*
  - Adicionalmente, 2 rotores eram fixos e simulavam o *plug-board* da Enigma
- Permitia que letras fossem substituídas por elas mesmas
- O texto cifrado era impresso, excluindo a possibilidade de erros

Typex - melhorias

- Utilizava 5 rotores ao invés de 3 ou 4 da Enigma
  - Cada rotor possuía diferentes *turn-points*
  - Adicionalmente, 2 rotores eram fixos e simulavam o *plug-board* da Enigma
- Permitia que letras fossem substituídas por elas mesmas
- O texto cifrado era impresso, excluindo a possibilidade de erros
- Como resultado, as tentativas de ataque ao Typex não tiveram o mesmo sucesso da Enigma

Fim