ICMC USP
SÃO CARLOS

GANESH

Criptografias de rotor

Introdução

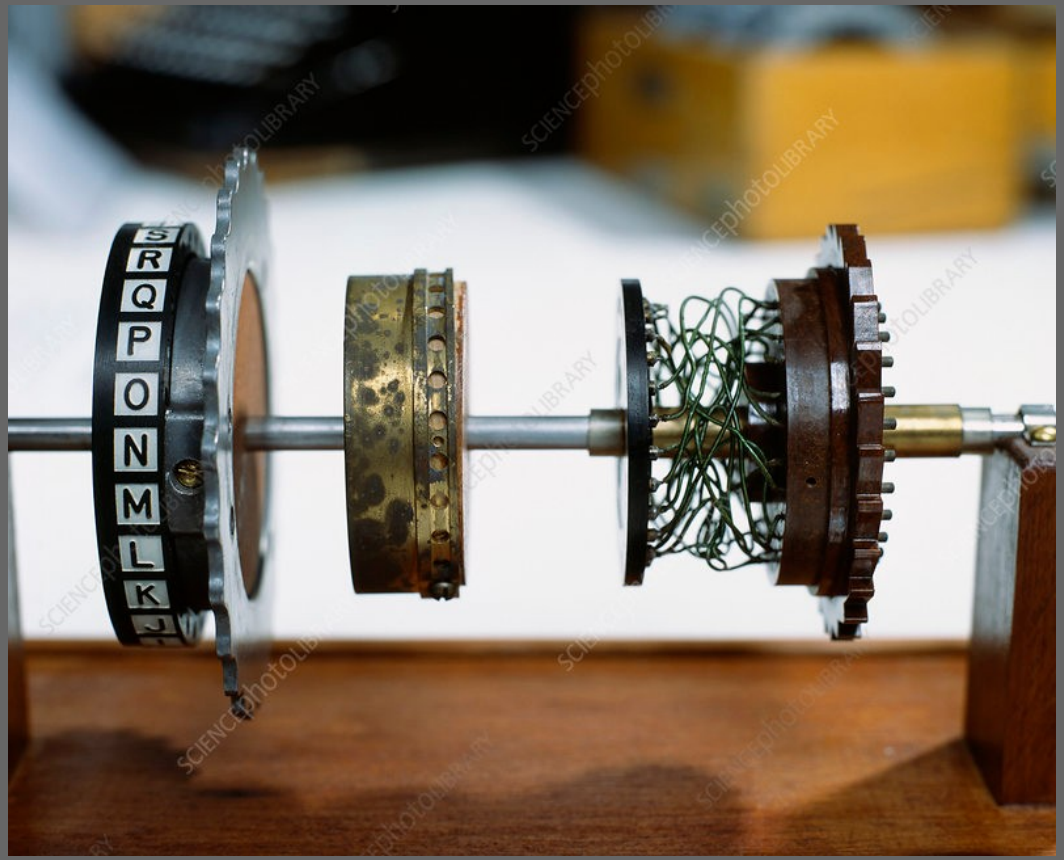
- Criptografias pré-rotor → métodos manuais de encriptação e decriptação
  - Sujeito a erros humanos
  - Processo trabalhoso e dispendioso
- Máquinas de rotor
  - Encriptação e decriptação feitas de forma automática
  - Processo rápido e íntegro
  - Maior segurança devido à imensa quantidade de combinações dos rotores

Enigma

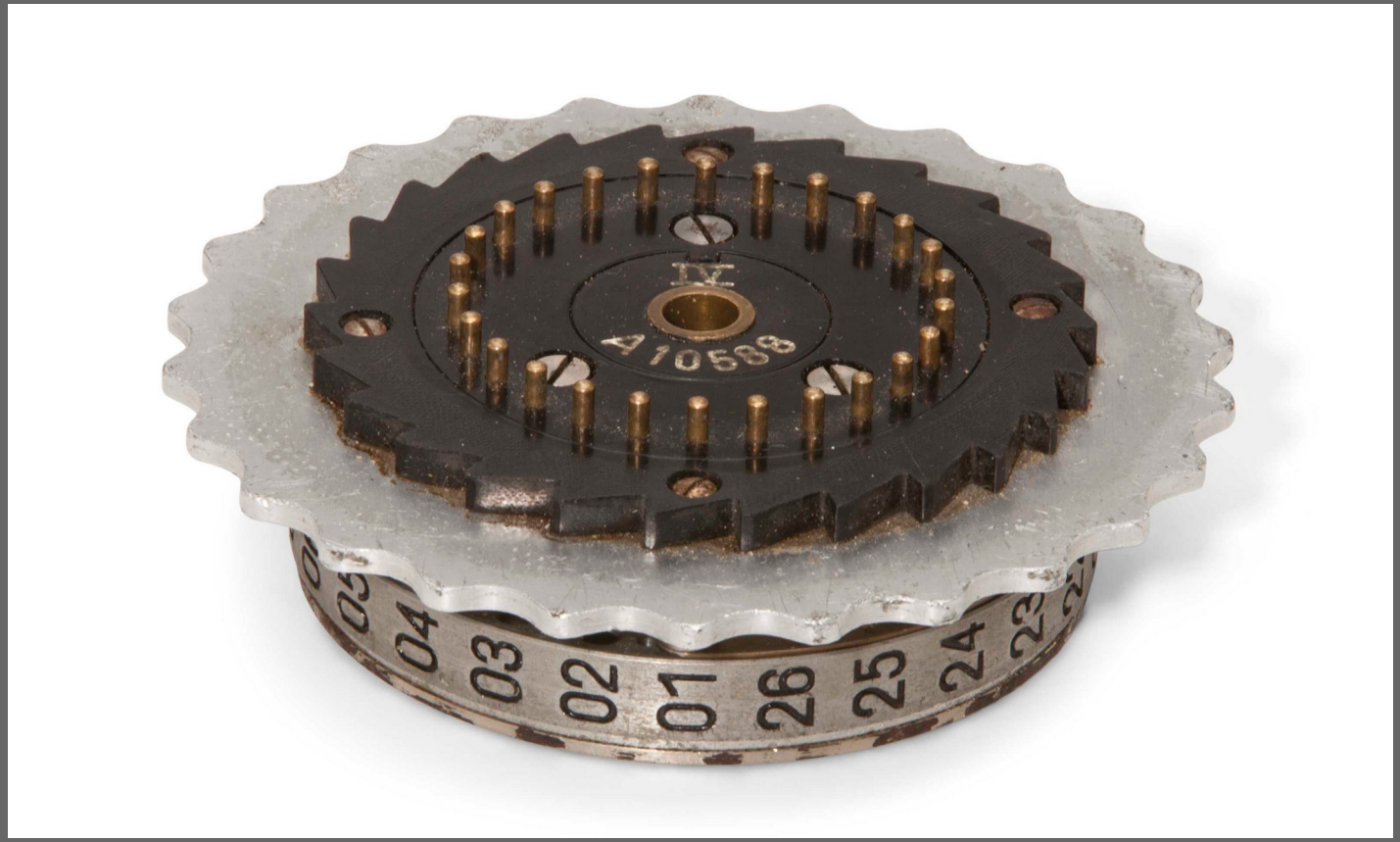
Rotor

- Mapeamento entre *plaintext* e *ciphertext* é feito através das conexões internas do rotor
- Pressionar uma tecla faz o rotor girar, alterando o mapeamento (alfabeto)
- Após 26 rotações ele começa a se repetir
  - Semelhante a uma chave de Vigenère de 26 caracteres
- Para encriptar e decriptar mensagens, uma posição inicial deve ser combinada
- A decriptação (inicialmente) exige que o rotor seja invertido

Rotor por dentro



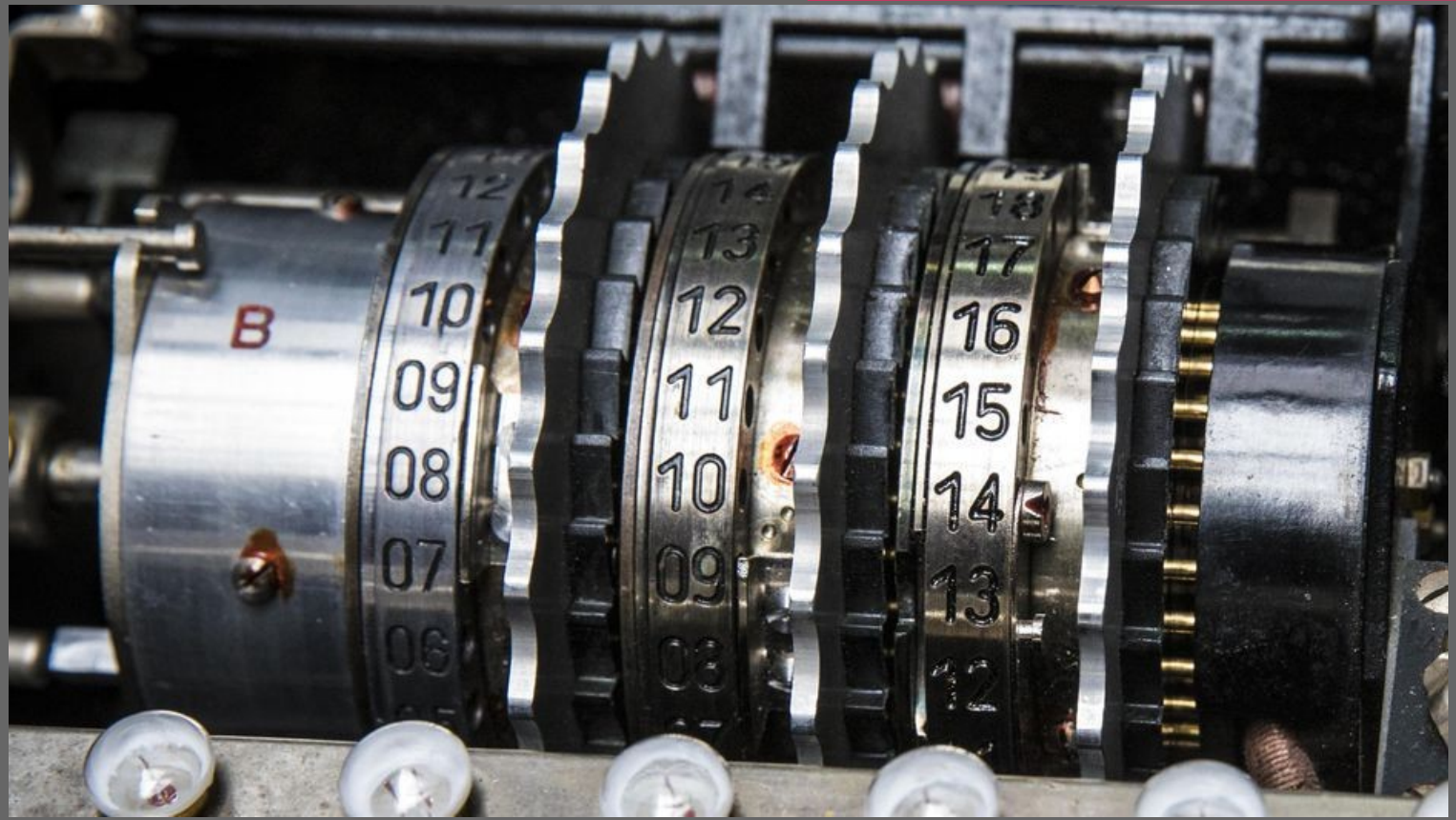
Rotor da Enigma



Múltiplos rotores

- Utilizar somente 1 rotor não produz a segurança necessária
  - Solução: conectar múltiplos rotores serialmente
- *n* mapeamentos sequenciais e *n* posições iniciais
  - *n* = quantidade de rotores
- 26^n possibilidades de encriptação
- 26 rotações do rotor à esquerda → 1 rotação do rotor à direita
- Também era possível alternar o uso com rotores “reservas” disponíveis

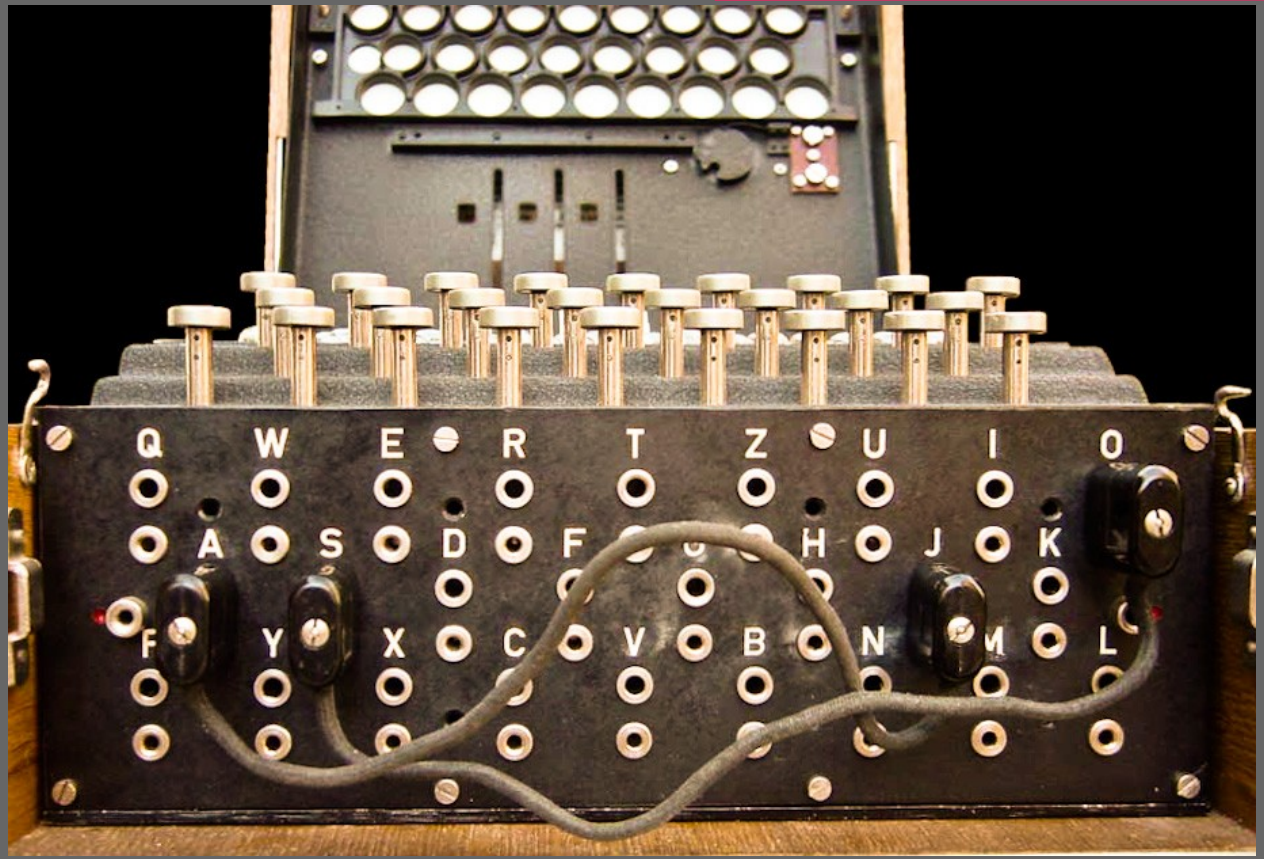
Múltiplos rotores



Plugboard (Enigma)

- Conectando pares de letras entre si, trocamos o sinal que é enviado ao primeiro rotor
  - Digitar uma dessas letras produzia um resultado diferente
- Em um alfabeto com 26 letras e 13 conexões possíveis:
  - $26! / (13! * 2^{13}) = 7,9 * 10^{12}$ possibilidades de conexões
- Dificulta o ataque por força bruta

Plugboard (Enigma)

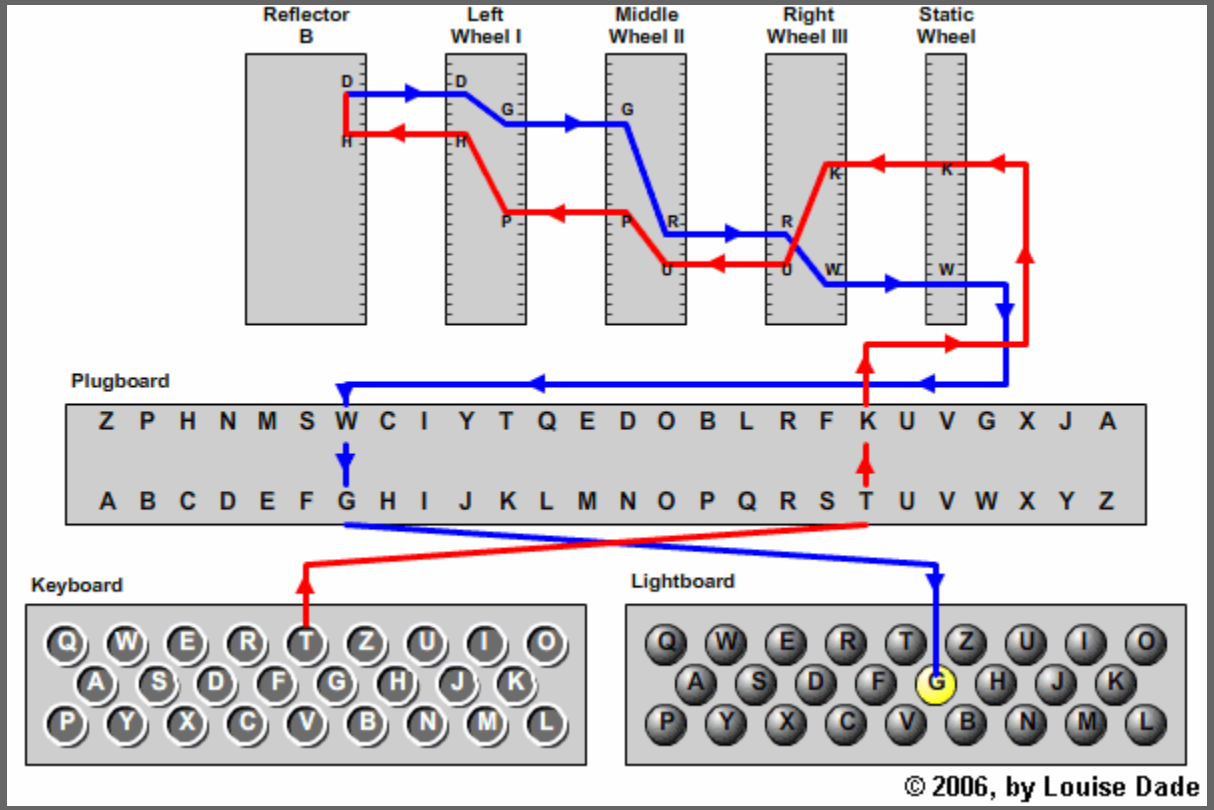


Refletor (Enigma)

- Inicialmente, a decriptação exigia inverter o sentido dos rotores
- A Enigma resolveu essa dificuldade com o uso do refletor
- Conexões fixas entre pares de letras
- Permitiu decriptar mensagens mantendo os mesmos rotores na posição inicial
- No caso da Enigma, não possibilitava que uma letra fosse mapeada para ela mesma
    - Vulnerabilidade crítica que permitiu aos aliados quebrar a criptografia da Enigma

Refletor (Enigma)

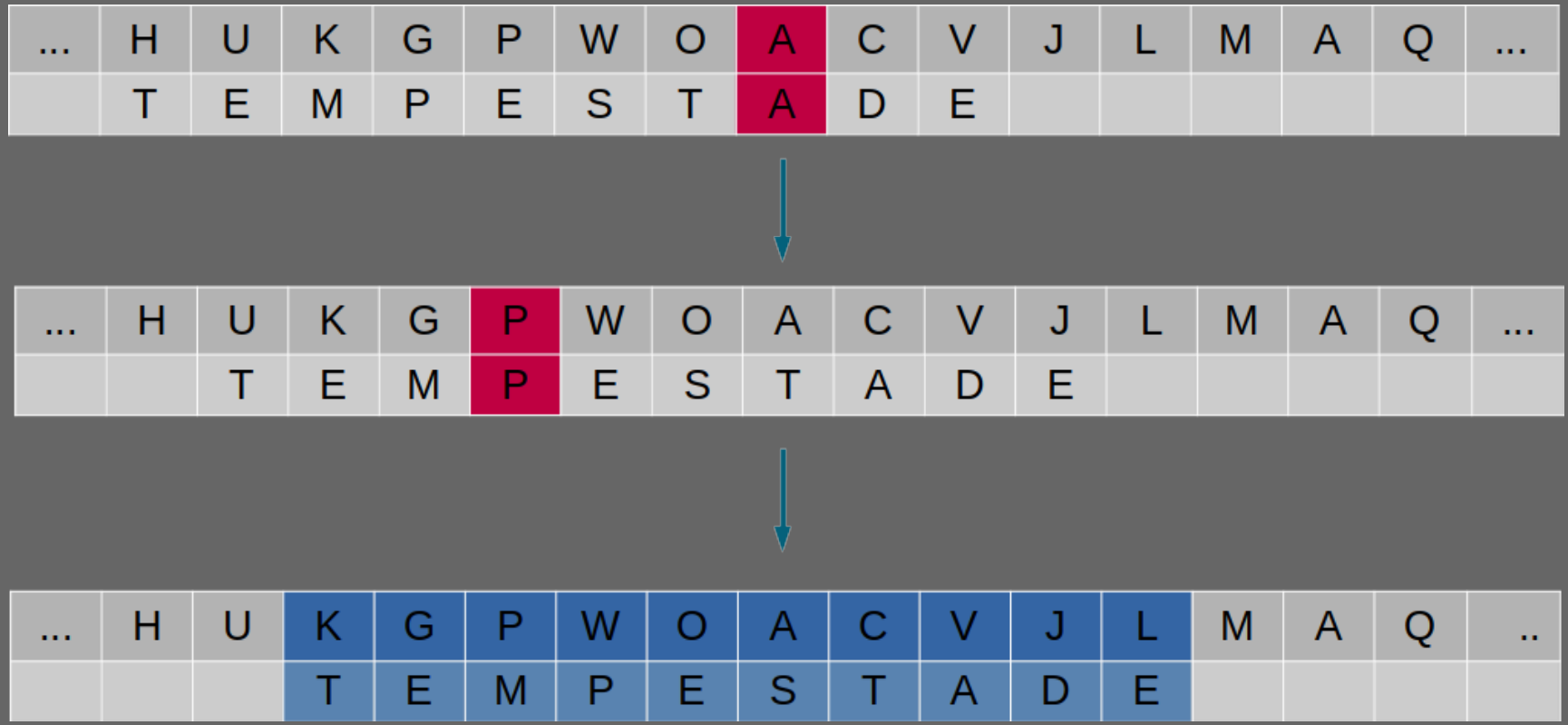
Enigma - funcionamento



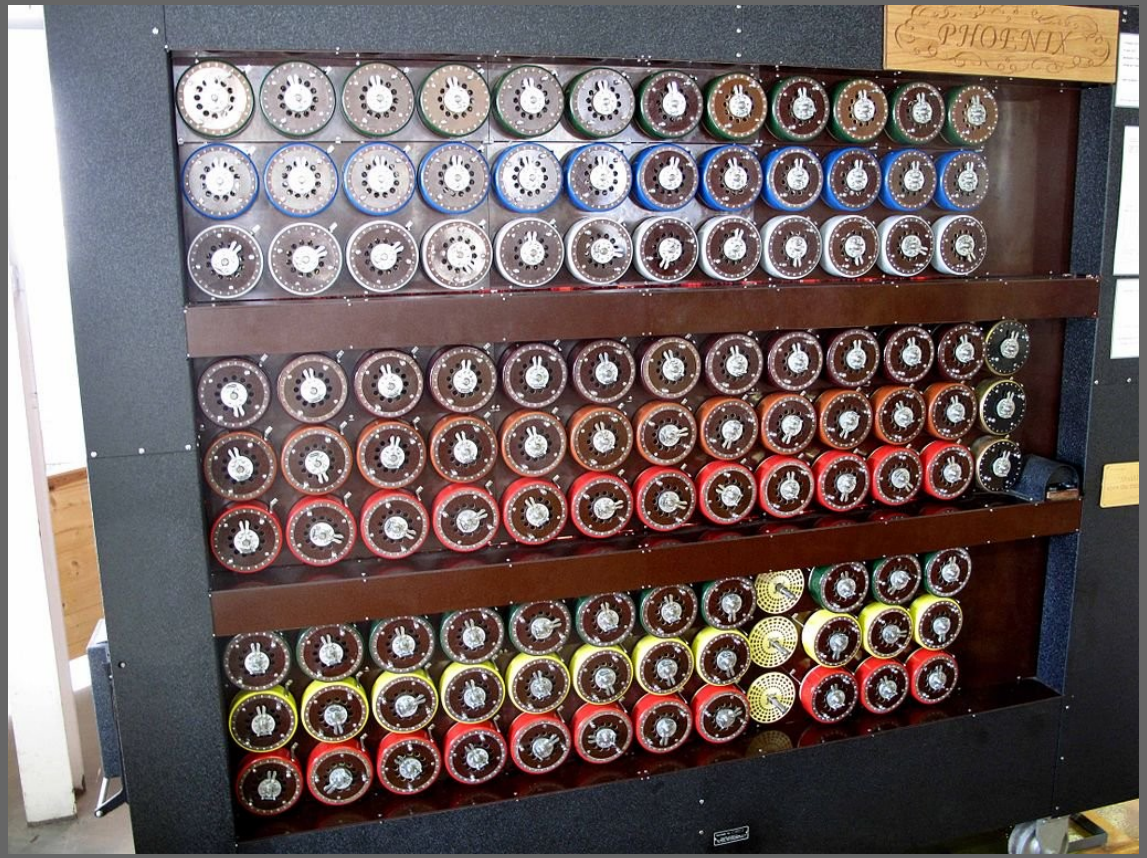
Vulnerabilidades

- Refletor
- Encriptação de mensagens muito grandes e/ou sem alteração prévia nos rotores
- Padrões conhecidos nas mensagens
  - “Previsão do tempo”
  - Começar novas mensagens com “continuação”, etc
- Regras para a escolha de rotores
  - Nenhum rotor poderia ser colocado na mesma posição que foi utilizado na configuração anterior

Enigma - ataque



Réplica da “Bombe”



GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br