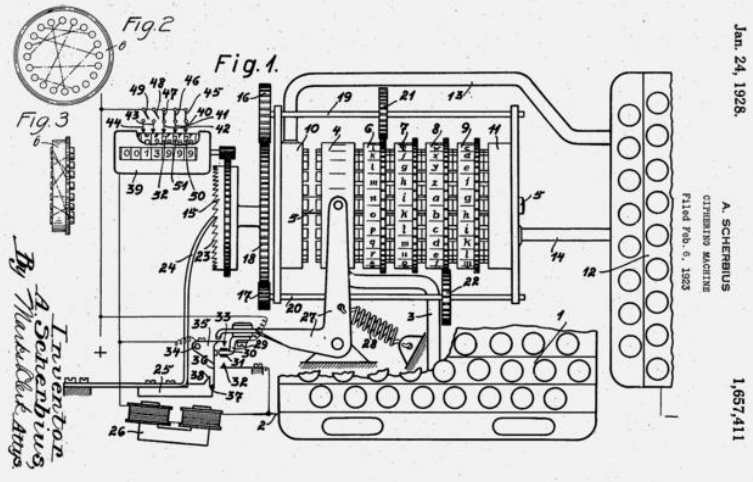
Introdução à disciplina

Fundamentos da Criptografia

Nicollas Mocelin Sdroievski



Quem sou eu?

- Nicollas Mocelin Sdroievski
  - Bacharel em Sistemas de Informação – UTFPR
  - Mestre em Informática – UFPR
  - Doutor em Ciência da Computação – UW Madison

  - Área de pesquisa: Complexidade Computacional

  - Hobbies: jogos de computador, jogos de tabuleiro, jiu-jitsu

Quem são vocês?

- Nome
- Algo interessante sobre você
- O que espera aprender?

Questões administrativas

- Logística
- Chamada
- Avaliação
  - Próximos slides

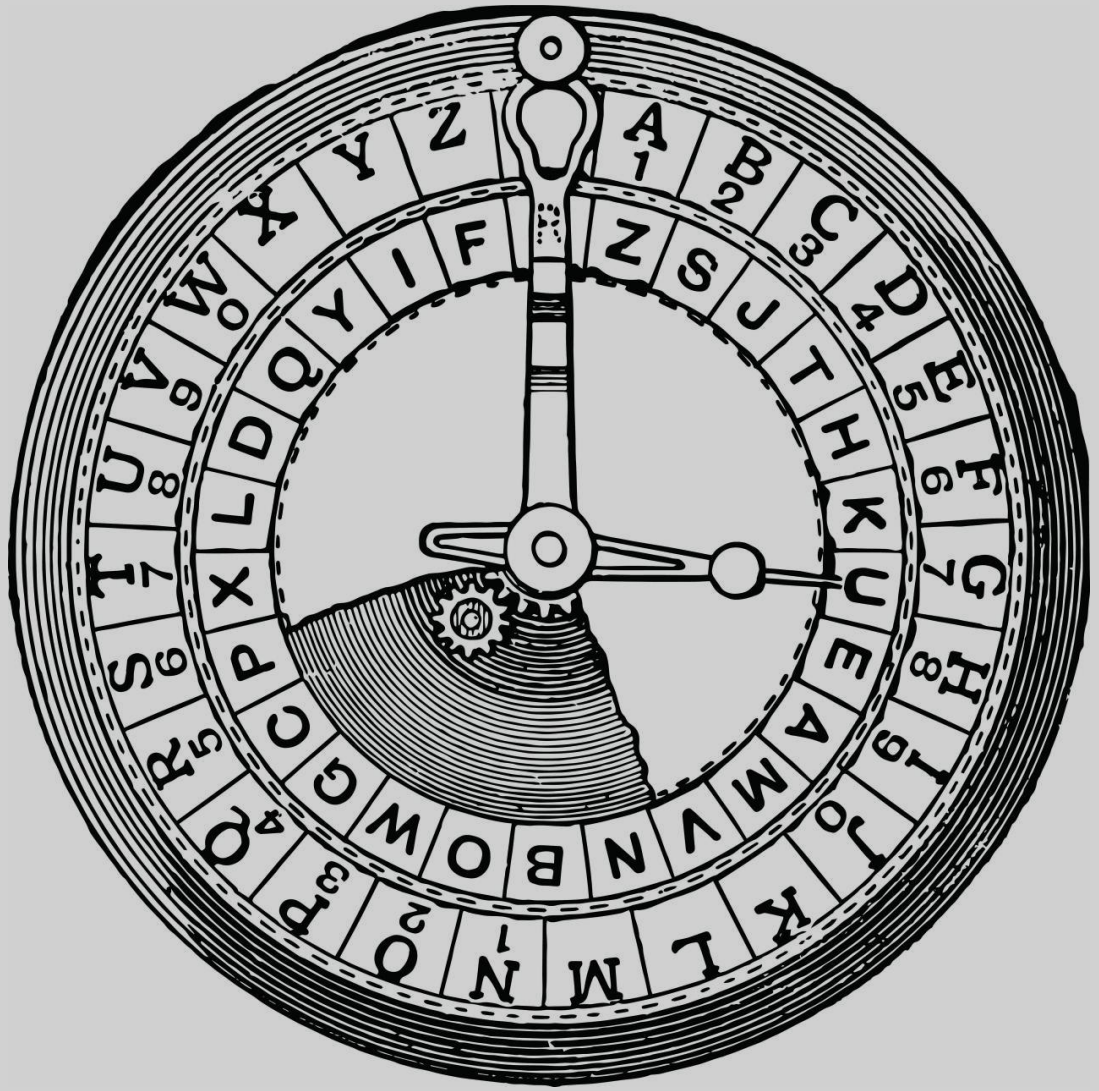
Avaliação

- Duas opções
- Listas de exercícios
  - $(L_1 + L_2 + L_3)/3$
  - Recomendadas para aprender o conteúdo mais à fundo
  - Razoavelmente desafiadoras
  - Posso ajudar vocês sem nenhum problema
- Projeto semestral
  - Três “entregas” $(P_1 + P_2 + 3 \cdot P_3)/5$
    - Proposta
    - Andamento
    - Apresentação

Mais sobre o projeto

- Sugestões na página do curso, algumas opções:
- Teórico
  - Estudar e apresentar conceitos que não veremos em detalhes
  - Estudar e apresentar conexões com a área de complexidade computacional
- Prático
  - Apresentar detalhes de implementação de protocolos criptográficos usados na prática
  - Implementar e apresentar algum ataque à um protocolo inseguro
- Ligado à sua área de interesse
  - Apresentar conceitos que combinam o que veremos em sala com alguma área que seja de seu interesse, como banco de dados, SO, IA, ...

Conteúdo



Parte 1

- Criptografia clássica versus moderna
- Segredo perfeito
- Criptografia de chave privada
  - Noções básicas de segurança
  - Construção de protocolos seguros
- Primitivas criptográficas
  - funções unidirecionais
  - geradores pseudo-aleatórios
  - funções pseudo-aleatórias

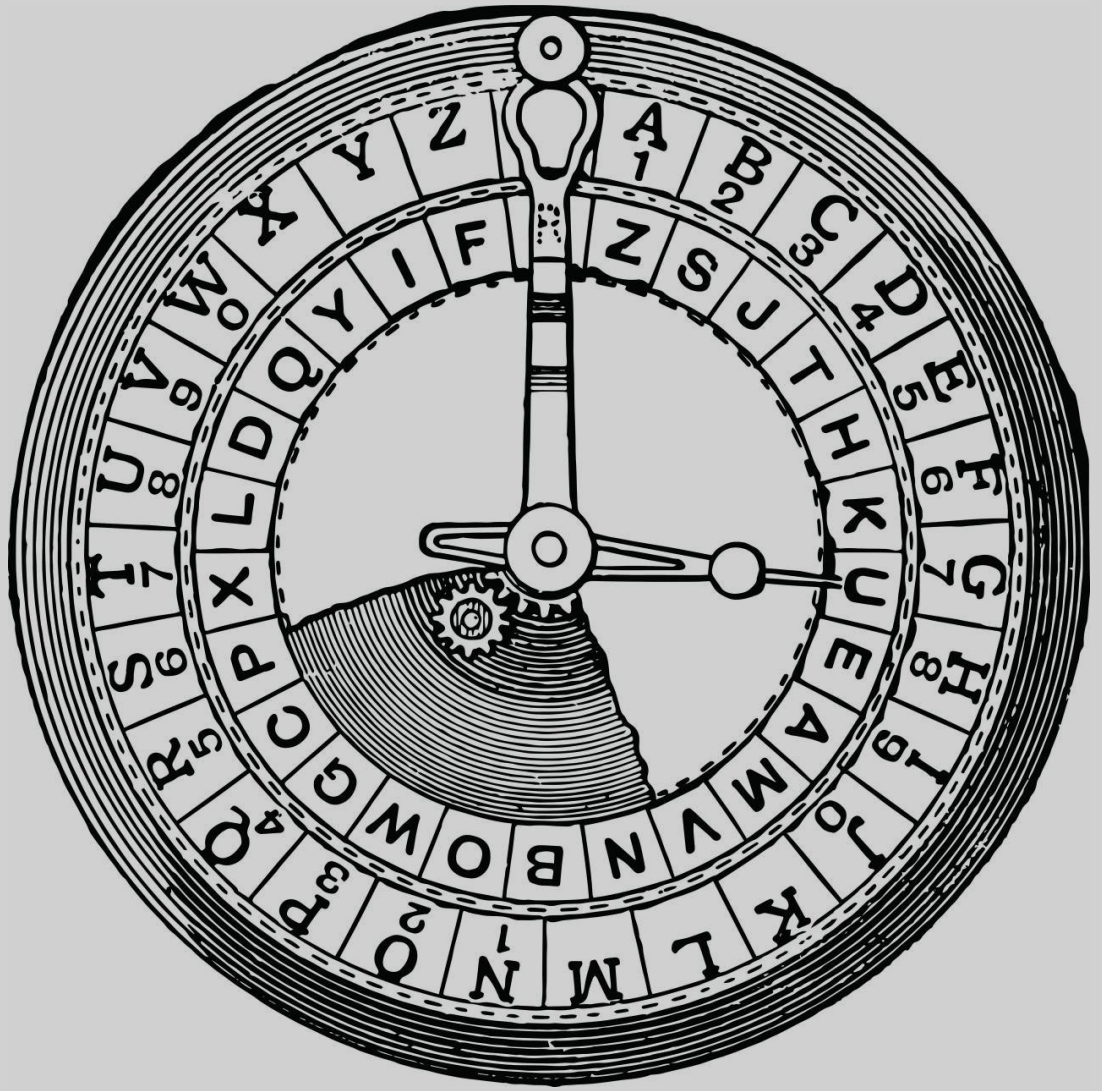
Parte 2

- MACs (códigos de autenticação de mensagens)
  - Construções
  - Segurança mesmo quando o adversário possui um oráculo de cifragem/decifragem
- Funções hash criptográficas
  - Diferentes das que vimos para tabelas hash!
  - Resistência de colisão e pré-imagem
- Criptografia de chave pública
  - Teoria de números
  - Diffie-Hellman, RSA, ...
  - Assinaturas digitais

Parte 3

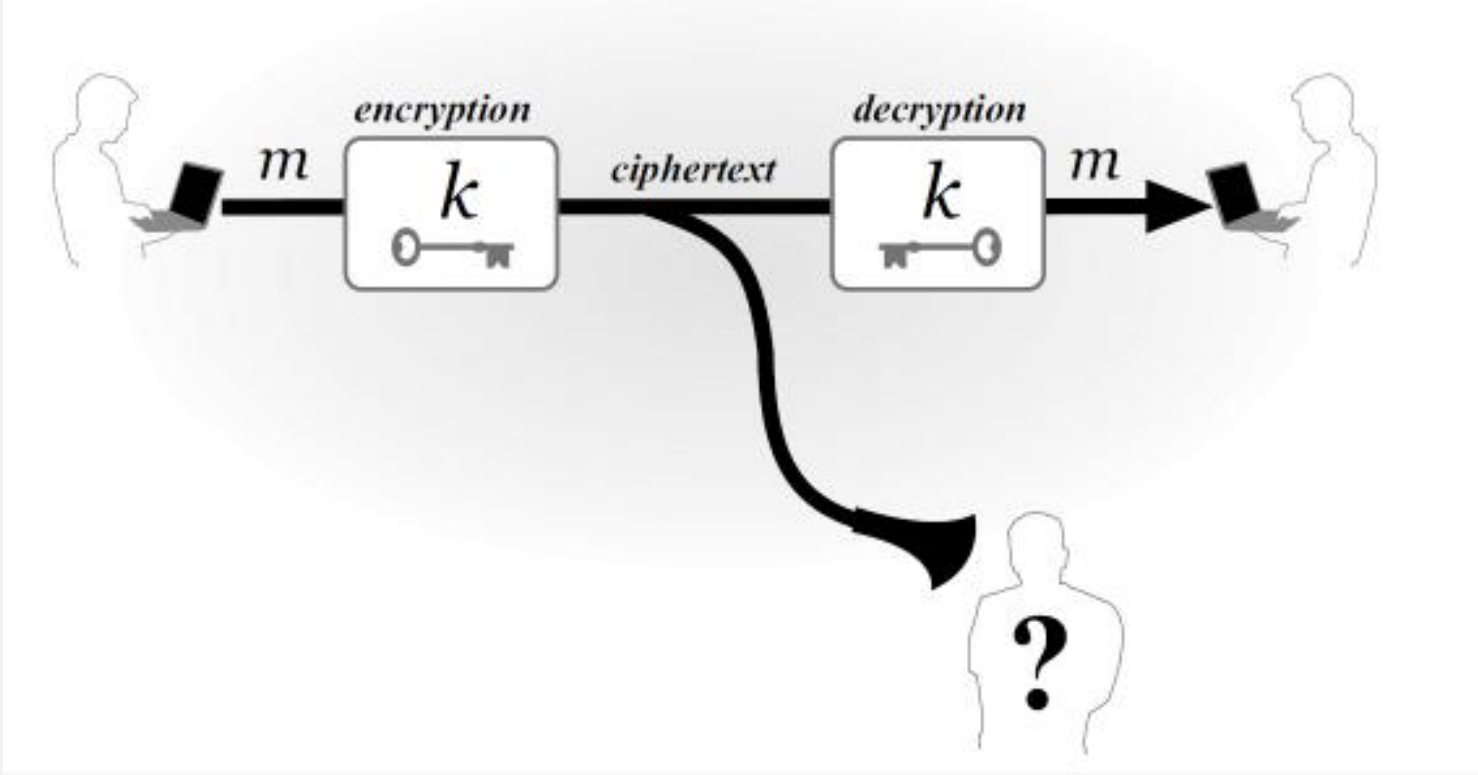
- Provavelmente, mais criptografia de chave pública
- Criptografia pós-quântica
- Provas de conhecimento zero
- Construção de primitivas criptográficas
- Criptografia e complexidade computacional

Algumas definições



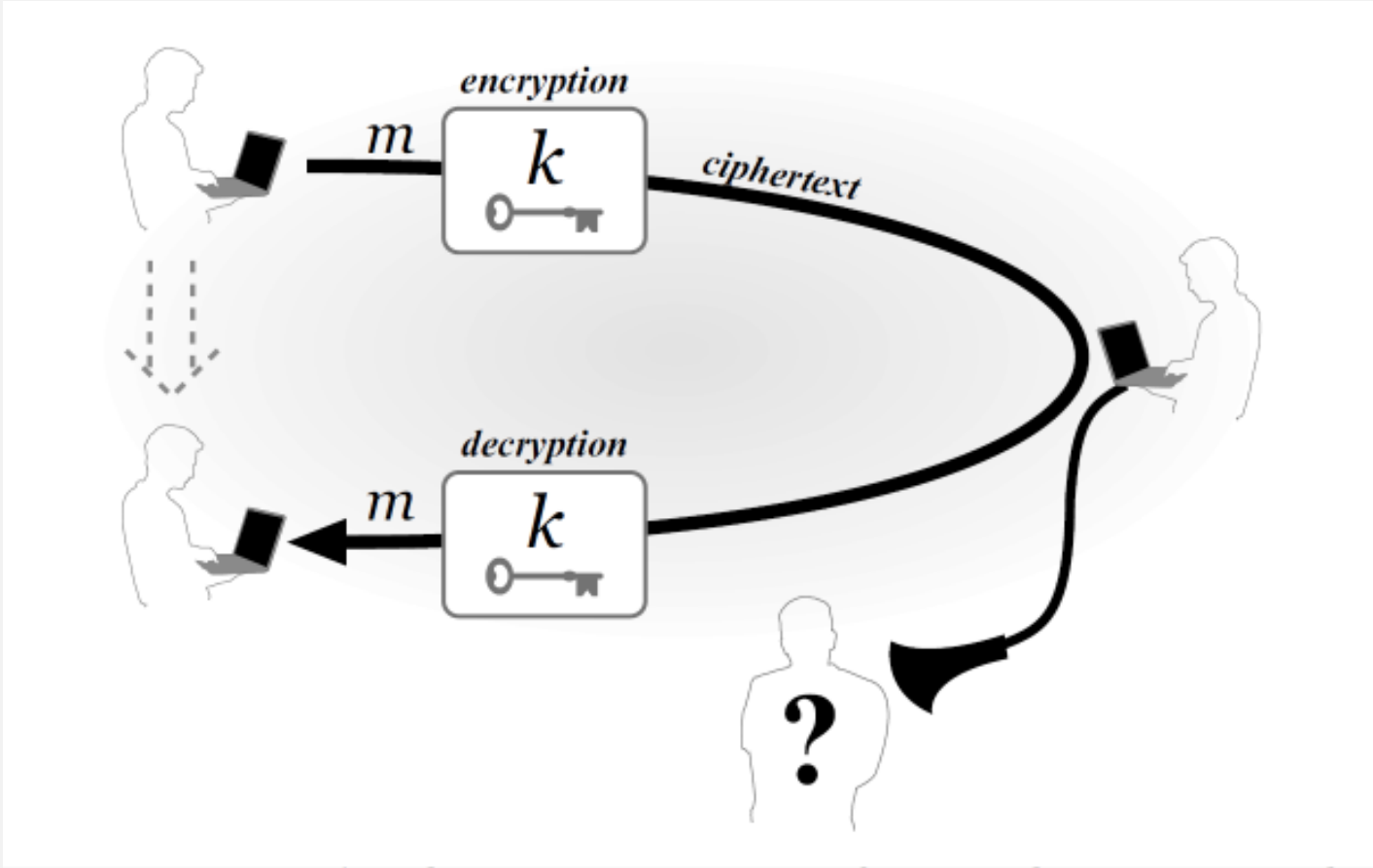
O cenário inicial

- Desejamos enviar uma mensagem para outra pessoa, sem que “bisbilhoteiros” consigam decifrar a mensagem
- Para isso, compartilhamos uma chave privada com esta outra pessoa



Outra possibilidade

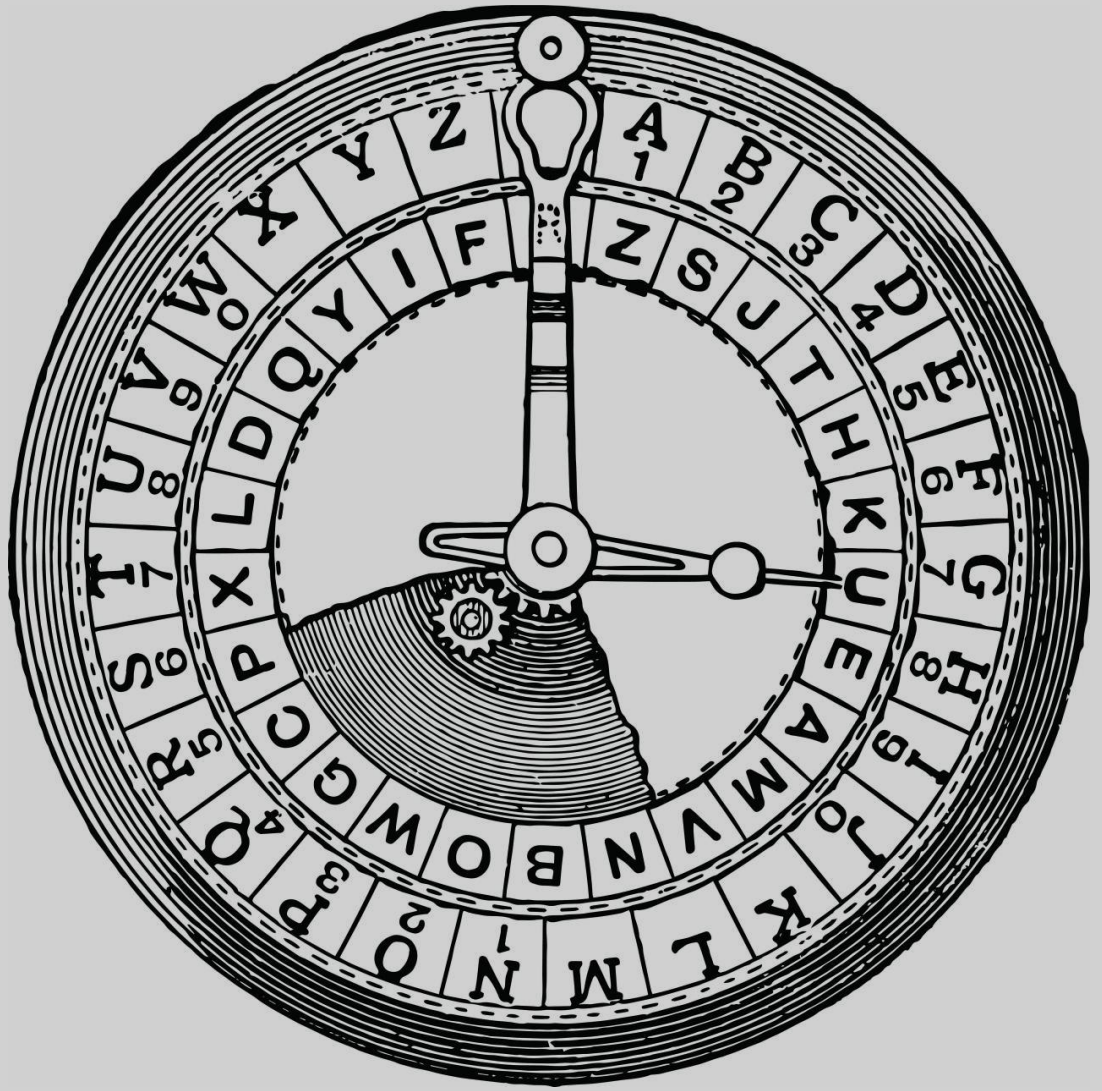
- Um usuário se comunicando consigo mesmo no futuro
- Exemplo: cifragem de disco
- Distribuição da chave não é mais um problema



Cifras simétricas

- Uma cifra simétrica (de chave privada) é definida por um espaço de mensagens $\mathcal{M}$ junto de três algoritmos $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$:
  1. Gen é o algoritmo probabilístico de geração de chaves, que produz uma chave k
  2. Enc é o algoritmo de cifragem (encriptação), que recebe uma chave k e uma mensagem m, produzindo um texto cifrado c. Denotamos esse processo por $\mathrm{Enc}_k(m)$
  3. Dec é o algoritmo de decifragem (decriptação), que recebe uma chave k e um texto cifrado c, produzindo uma mensagem m. Denotamos esse processo por $\mathrm{Dec}_k(c)$
- Corretude: $\mathrm{Dec}_k\big(\mathrm{Enc}_k(m)\big) = m$ para todo $m \in \mathcal{M}$

Criptografia Clássica



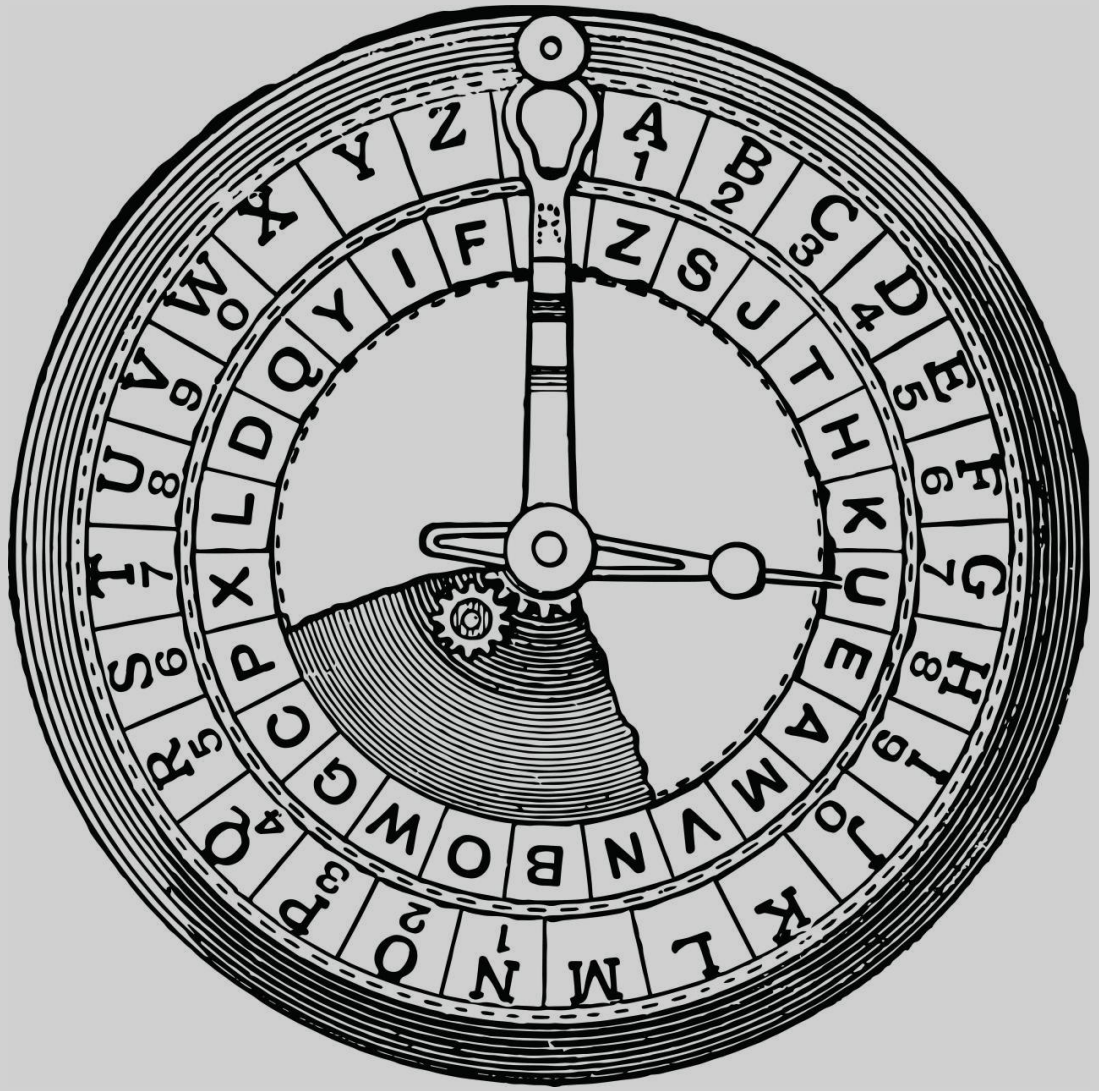
Uma arte

- **No dicionário.** Arte ou processo de escrever em caracteres secretos ou em cifras
- Até o século 20, de fato a criptografia era uma arte
  - Pouca teoria
  - Bastante criatividade
  - E bastante complexidade (não computacional)
- Como se determinava se um protocolo era seguro?
  - Se ninguém tivesse conseguido quebrar ainda

Alguns exemplos, por cima

- César / Single-byte XOR
  - Desloca cada letra um valor secreto k para frente
  - Exemplo: $k = 2$, a letra a vira c
- Mono-alfabética
  - Troca cada letra por alguma outra, baseada em uma permutação de todas as letras do alfabeto
- Vigenère
  - Também desloca cada letra, porém baseado em uma palavra secreta k
  - Exemplo: $k = ab$, o texto $abcd$ vira $bddf$

Criptografia Moderna



Princípio de Kerckhoffs

- “O método de cifragem/decifragem não deve precisar ser secreto, e deve poder cair na mão do adversário sem consequência”
- Todos os envolvidos devem conhecer os algoritmos $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$
- A única coisa secreta deve ser a chave
  - E a “segurança depende somente do segredo da chave”
- Alguns motivos:
  - Mais fácil manter o segredo da chave do que de todos os algoritmos utilizados
  - Mais fácil trocar uma chave comprometida do que todo o método de cifragem/decifragem
  - Se todos conhecem os algoritmos, todos podem tentar quebrá-lo (e fornecer credibilidade para sua segurança quando falham)

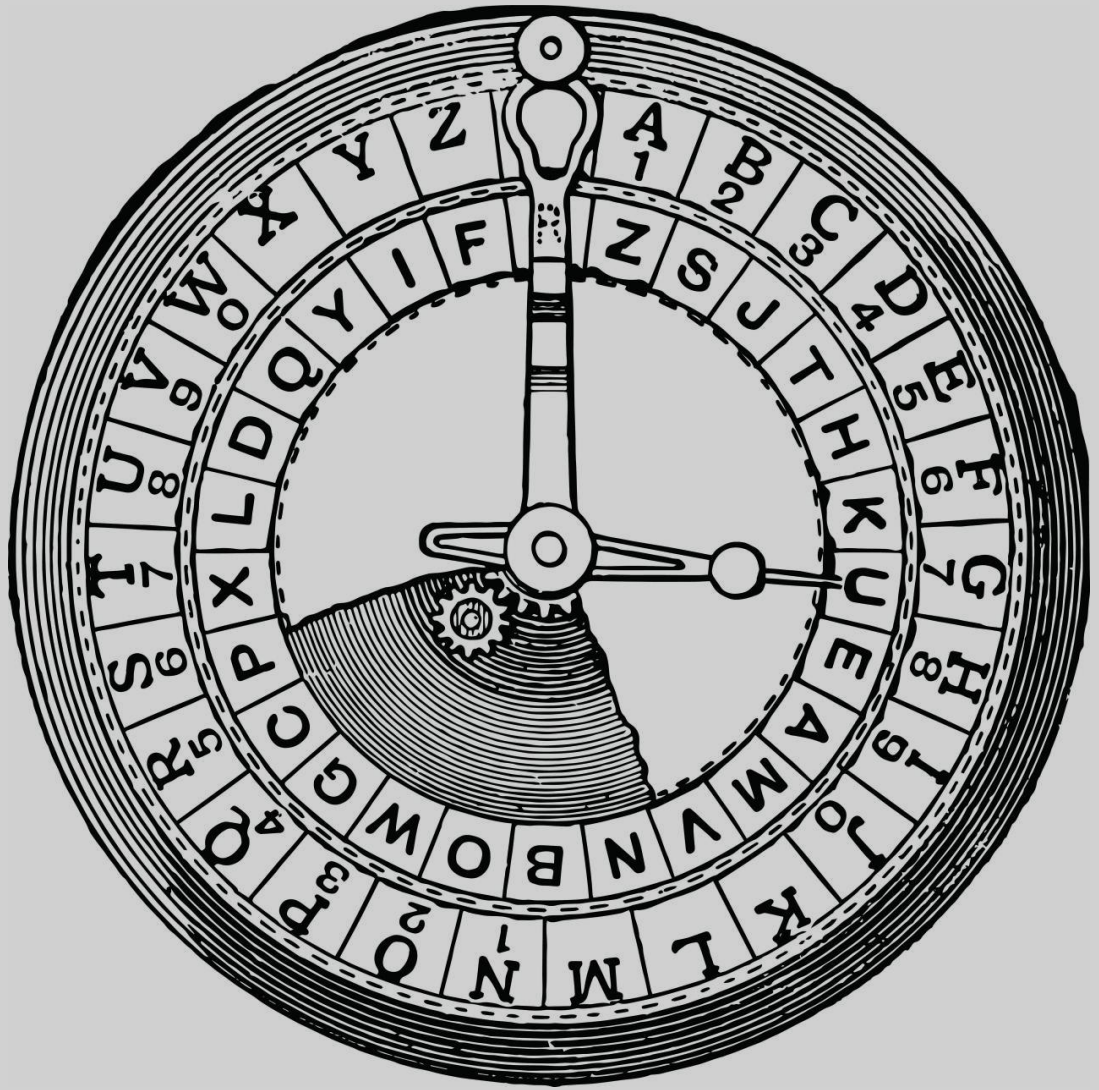
Os três pilares

- Definições formais
  - Capacidades do adversário
  - Segurança esperada
- Hipóteses precisas
  - Coisas como $P \neq NP$
  - Idealmente, hipóteses extensivamente testadas
- Provas de segurança
  - Se meu esquema é inseguro, então a hipótese é falsa
  - Se meu esquema é inseguro, então $P = NP$

Cuidados específicos

- Uma prova só garante segurança no mundo real se as definições de fato modelarem a situação real
- **Exemplo**
  - Prova assume que o adversário não pode influenciar que mensagens são cifradas
  - Útil para as situações que discutimos
  - Não é útil para um sistema de terminal público que criptografa todos os comandos enviados pelos usuários
- Não resolve o problema entre “atacante” e “defensor”, mas trás uma perspectiva que favorece o “defensor”

Outros caminhos



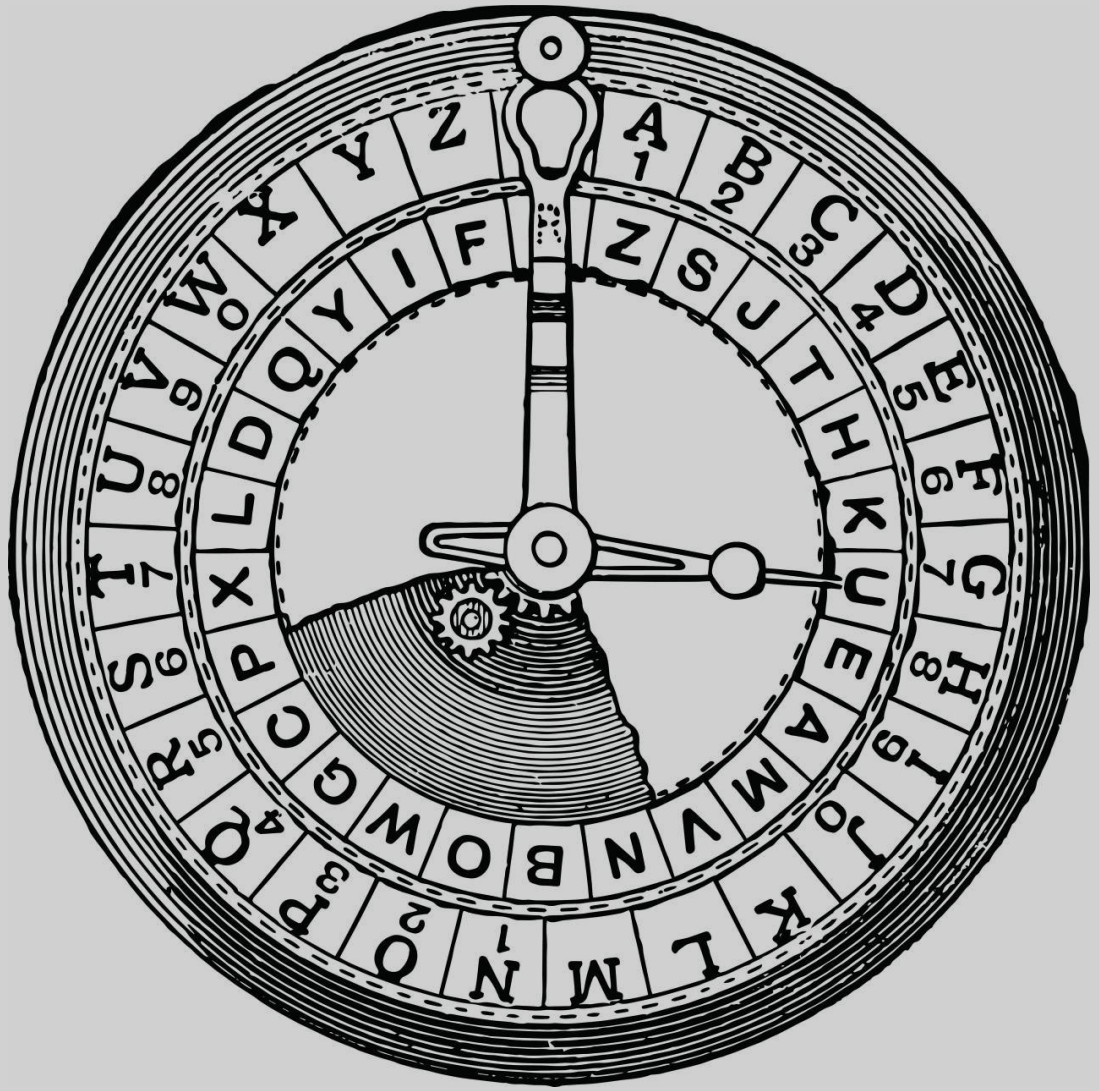
Algoritmos práticos

- Algoritmos usados na prática como DES, AES, variações de RSA, etc.
- Não serão nosso foco (no geral)
- Mas podem ser o foco de projetos semestrais

Ataques

- Criptanálise
  - A arte de explorar falhas em protocolos inseguros
  - Normalmente possível por falhas de implementação ou modificações sem a devida prova de segurança
- Um pouco de material sobre este tema disponível na minha página
  - https://www.inf.ufpr.br/nicollas/topicos/UNESPAR/
  - Parte de um grupo de estudos de criptografia desenvolvido na UNESPAR
- Sugestões para alunos interessados (pode ser um trabalho semestral)
  - CryptoPals: https://cryptopals.com/
  - CryptoHack: https://cryptohack.org/

Para fechar



Para fechar

- Hoje
  - Ideia geral e logística da disciplina
  - Criptografia clássica versus moderna
- Na próxima aula
  - Criptografia clássica
    - Cifras específicas
    - Ataques para estas cifras