



**Faculdade Sumaré**  
*Educação para uma Mentalidade Transformadora*

# P-TRIS

**Carlos Henrique Calazans Ribeiro, Davi Rodrigues  
Patoleia, Rodrigo Rana de Miranda**

**Faculdade Sumaré – Campus Imirim  
São Paulo - SP**

# Conteúdo

---

- ▶ Introdução
- ▶ Segurança em Saúde
- ▶ SET
- ▶ SET - Processos
- ▶ Segurança x Custo Computacional
- ▶ P-TRIS
- ▶ P-TRIS - Processos
- ▶ Análise P-TRIS x SET
- ▶ Vantagens e Desvantagens
- ▶ Conclusão



# Introdução

---

- ▶ A evolução da TI tem aberto novas possibilidades a área de saúde
- ▶ Possibilidade de diagnósticos mais precisos
- ▶ Comunicação mais ágil e ampla (tele medicina)



# Segurança em Saúde

---

- ▶ O tráfego de dados precisa ser seguro
- ▶ Informações médicas devem estar isentas a ataques de terceiros
- ▶ As informações transmitidas entre receptor e emissor devem ser totalmente íntegras



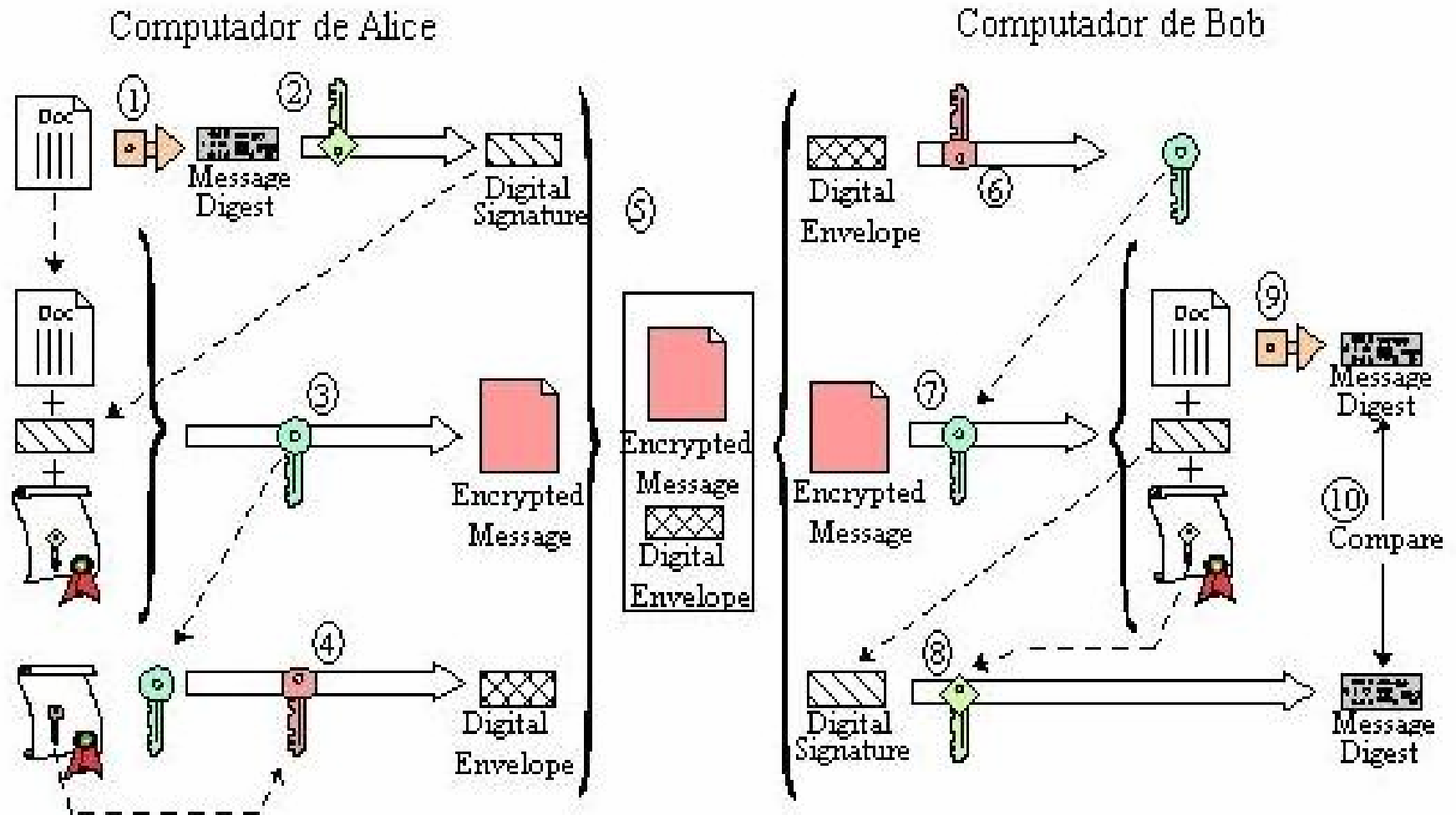
# SET

---

- ▶ Um dos principais padrões de transmissão do mercado
- ▶ Protocolo híbrido
- ▶ Utiliza criptografia, assinatura digital e hash
- ▶ Para envio e autenticação de mensagens são necessárias treze operações



# SET - Processos



# Segurança x Custo Computacional

---

- ▶ Dados médicos necessitam de transmissão segura
- ▶ As técnicas de segurança implementadas não devem consumir recursos computacionais e muito tempo de execução (agilidade no envio e recepção de respostas)
- ▶ Eficiência e segurança devem caminhar juntas



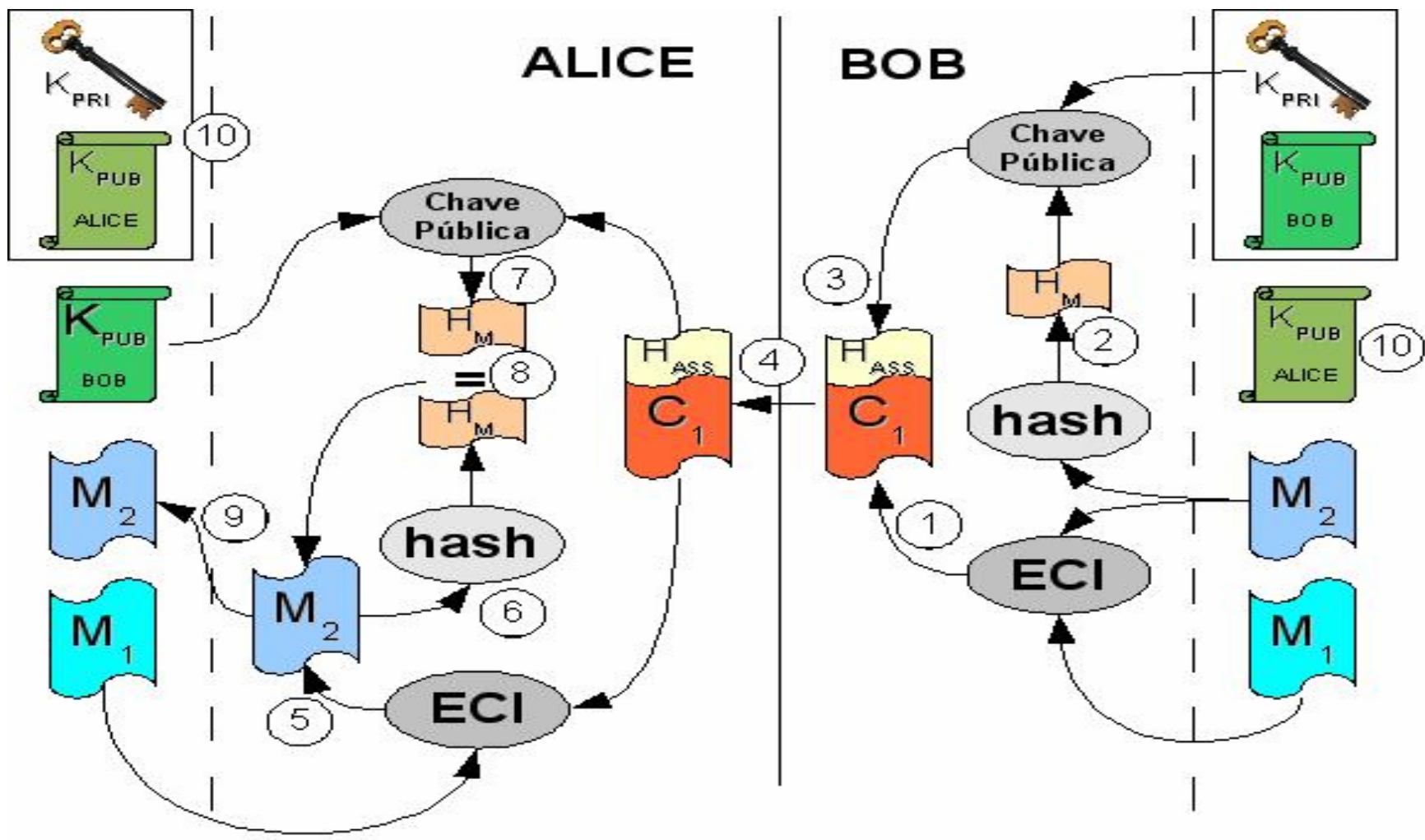
# P-TRIS

---

- ▶ Nova proposta de algoritmo de segurança
- ▶ Utiliza esteganografia e criptografia em conjunto
- ▶ Prima pela segurança sem perder a eficiência



# P-TRIS - Processos



## Análise P-TRIS x SET

---

- ▶ O P-TRIS apresenta um algoritmo mais leve em relação ao SET
- ▶ São necessárias menos operações nos envios de mensagens
- ▶ O custo computacional total (envio, recepção) seria inferior com o uso do P-TRIS
- ▶ Apesar de mais leve, não apresenta comprometimento em confidencialidade, autenticação, controle de acesso, integridade e irretratabilidade.

# Vantagens x Desvantagens

---

- ▶ Algoritmo leve
- ▶ Relativamente fácil de ser implementado
- ▶ Necessita de outro algoritmo para o envio da primeira mensagem
- ▶ Não há facilidade em executar multicast (todas as partes devem possuir a estego imagem)



# Conclusão

---

- ▶ O P-TRIS surge como uma alternativa eficiente e leve comparado com outros padrões (SET)
  - ▶ O uso de técnicas de esteganografia, criptografia e hash garantem a confidencialidade e autenticação
  - ▶ O P-TRIS pode ser implementado para uso em chats e medicos e segunda opiniao
  - ▶ Pode ser usado em outras áreas além da área de saúde
-