Hashing e Criptografia

- Funções hash são usadas em muitos protocolos de criptografia (ex. MD5, SHA)

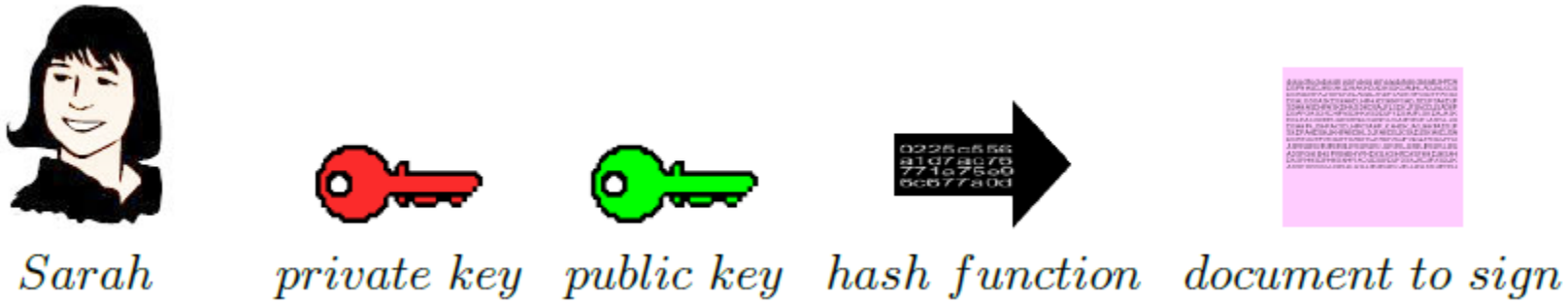
- Principais características de assinaturas manuais
  - Únicas para cada pessoa
  - Verificáveis como pertencentes aos seus donos

- As assinaturas digitais são a sua versão eletrônica

- Diferença: a assinatura digital é diferente para cada documento

Como funciona?

- Consideremos Sarah como a remetente do documento
- Sarah possui um par de chaves pública/privada

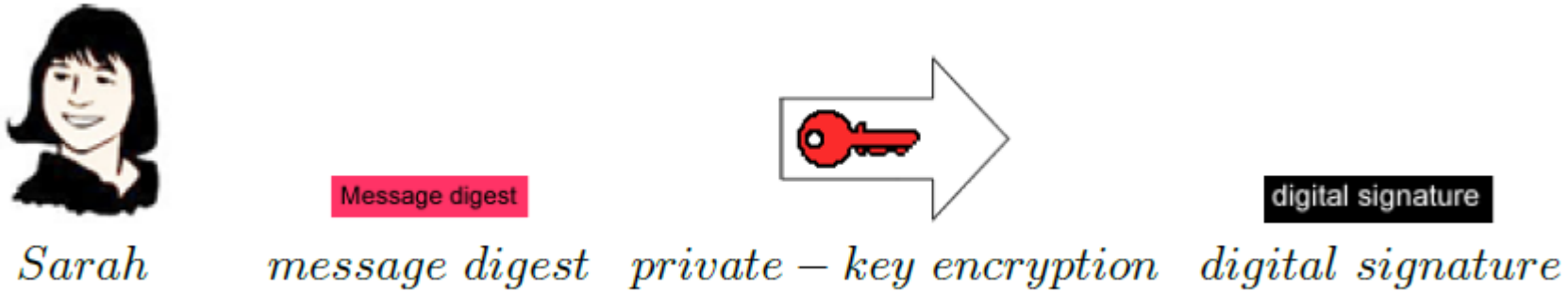


- Ela vai enviar uma mensagem a Remy

Como funciona?

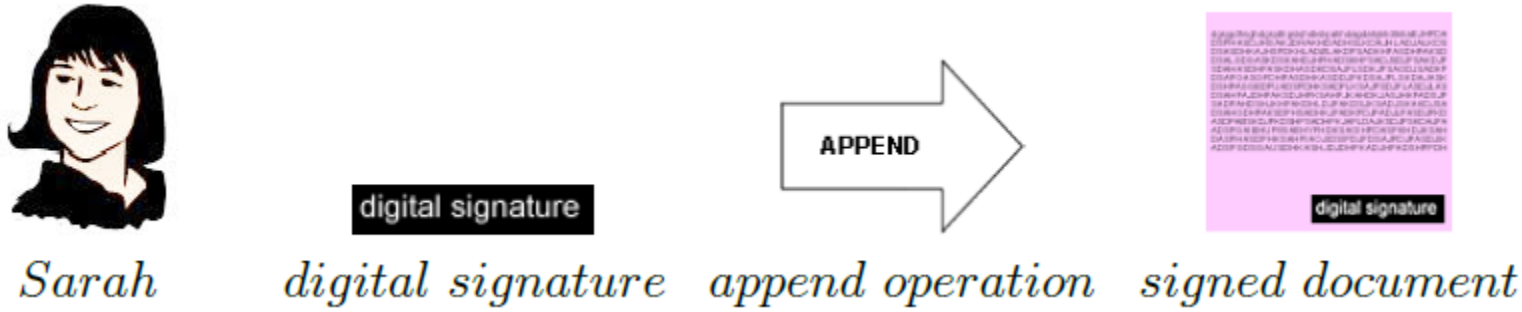
1. Sarah gera o código hash do documento

2. Sarah criptografa o código hash com sua chave privada produzindo sua assinatura digital

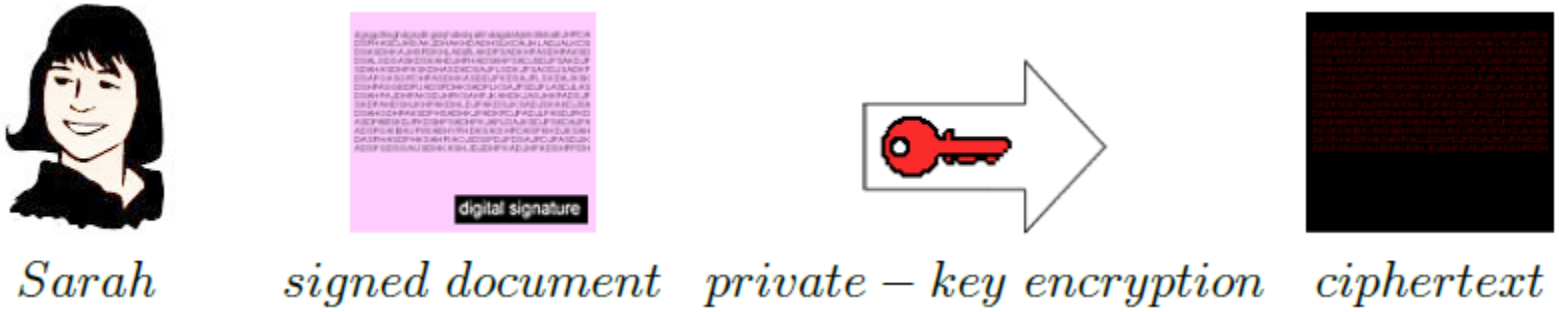


Como funciona?

3. Sarah concatena a assinatura digital ao documento

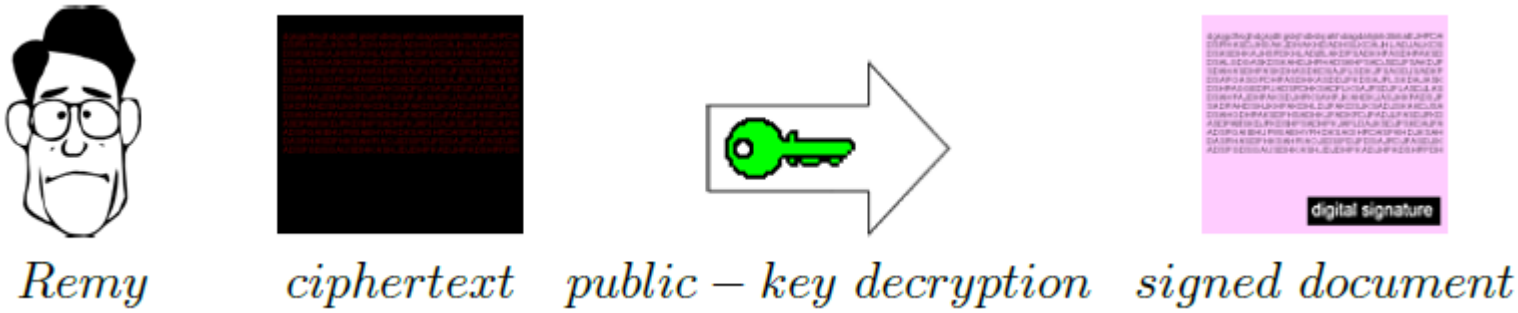


4. Sarah criptografa o documento assinado com sua chave privada e o transmite a Remy



Como funciona?

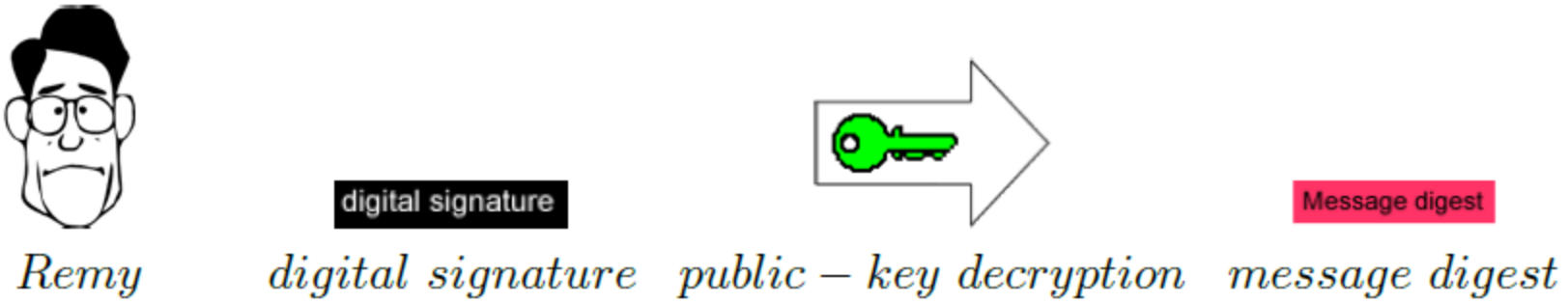
5. Remy recebe o documento e o descriptografa usando a chave pública de Sarah



6. Remy gera um novo código hash a partir do documento de Sarah

Como funciona?

7. Remy concorrentemente descriptografa a assinatura digital de Sarah com sua chave pública obtendo outro código hash



8. Finalmente, Remy compara os dois códigos hash obtidos
9. Se eles forem iguais, a mensagem está intacta