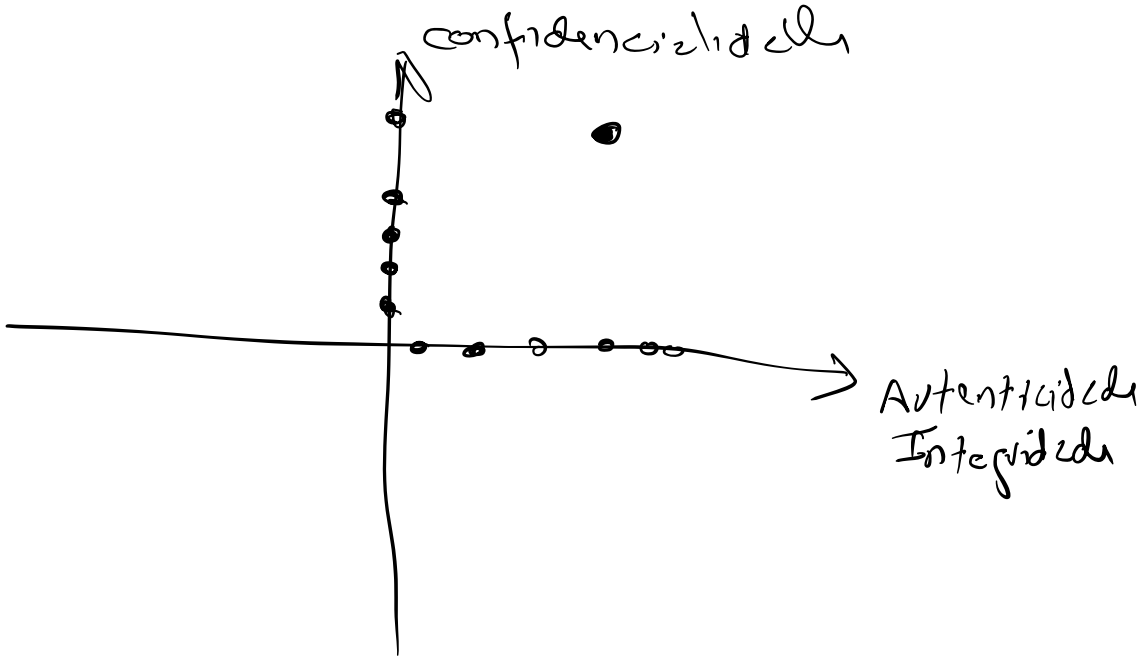


Cripto Simétrica

- Confidencialidade → Cifras simétricas → AES-CTR
- Autenticidade → MACs → HMAC

→ Cifras autenticadas AEAD

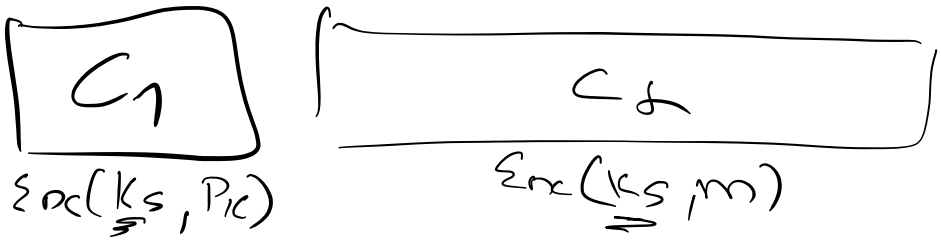
Chave secreta partilhada → autentica, confidencial

Criptografia de Chave Pública

Assinaturas Digitais

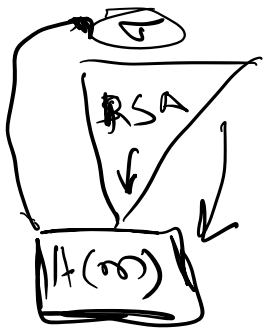
Cifras Assimétricas

Cifras Híbridas



chave privada { decifrar → cifra
assinar → assinatura
chave pública { cifrar → cifra
verificar → assinaturas

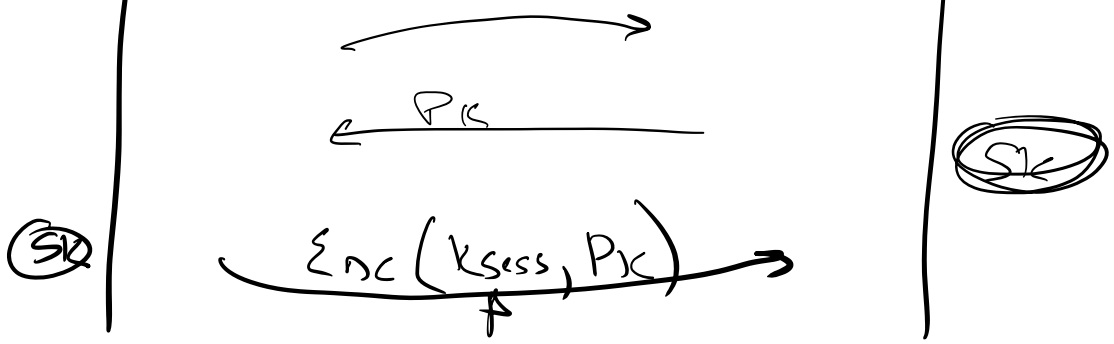
RSA – FDH



EC – DSA

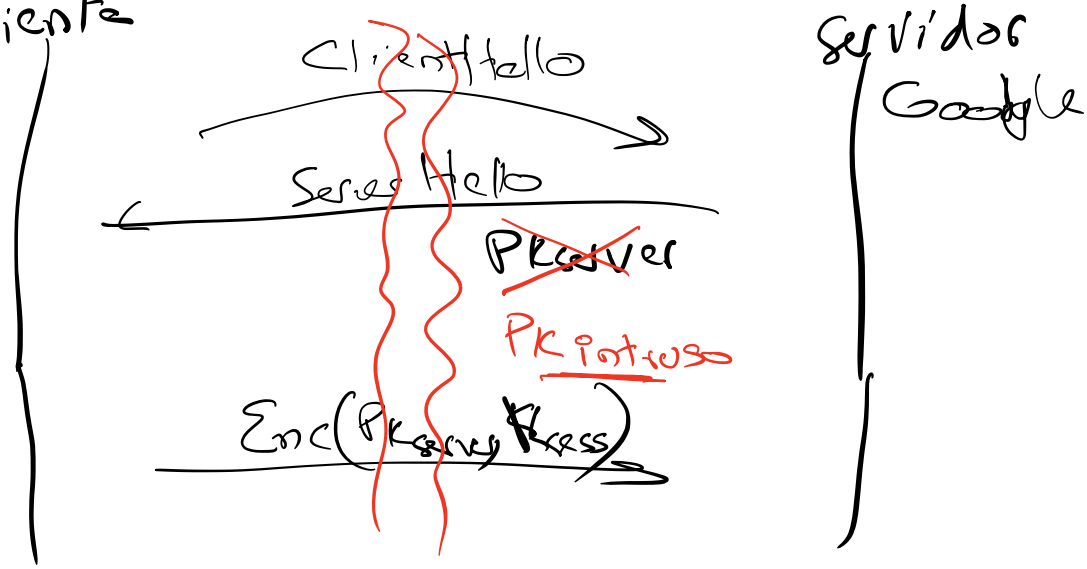
Cliente

Servidor



Perfect Forward Secrecy

Man in the Middle contra RSA-OAEP



Não funciona contra todas as técnicas de chave pública