

PGP: Pretty Good Privacy

TEORIA DA INFORMAÇÃO



Eduardo Kauer e Juliano Flores

Agenda

- ▶ História
- ▶ Características
- ▶ Como Funciona
 - ▶ Algoritmos
 - ▶ Chaves Pública Privada
 - ▶ Autenticação (Assinatura Digital)
 - ▶ Compressão
 - ▶ Confidencialidade (Encriptação / Decriptação)
 - ▶ Modelos de Confiança
- ▶ Conclusão
- ▶ Referências

História

- ▶ Pretty Good Privacy (*“Privacidade Bastante Boa”*)
- ▶ Phil Zimmermann
- ▶ 1991
- ▶ Sem interferência do governo (EUA) ou por agências de regulamentação
- ▶ Processo judicial por exportação de munição
- ▶ Processo judicial por patentes dos algoritmos RSA e IDEA

Características

- ▶ Utilização de Chaves Públicas e Privadas
- ▶ Encriptação de texto plano ou arquivos
- ▶ Autenticação
- ▶ Confidencialidade
- ▶ Utilização de algoritmos amplamente conhecidos e de forma integrada
- ▶ Código aberto e free (OpenPGP, GnuPG, etc...)

Alogritmos

▶ Encriptação

▶ Chave Pública e Privada

- ▶ Diffie-Hellman (DSA) / ElGamal

- ▶ RSA

▶ Simétrico

- ▶ AES (Rijndael)

- ▶ 3DES


- ▶ IDEA

- ▶ TwoFish

▶ Hash

- ▶ SHA-1

Chaves Públicas e Privadas

 A PGP key allows you to encrypt email or files to other people.

Full Name:

Email Address:




Comment:


▼ **Advanced key options**

Encryption Type:

Key Strength (bits):



Expiration Date: ☒ **Never Expires**

 **Help**  **Cancel**  **Create**

 Enter the passphrase for your new key twice.

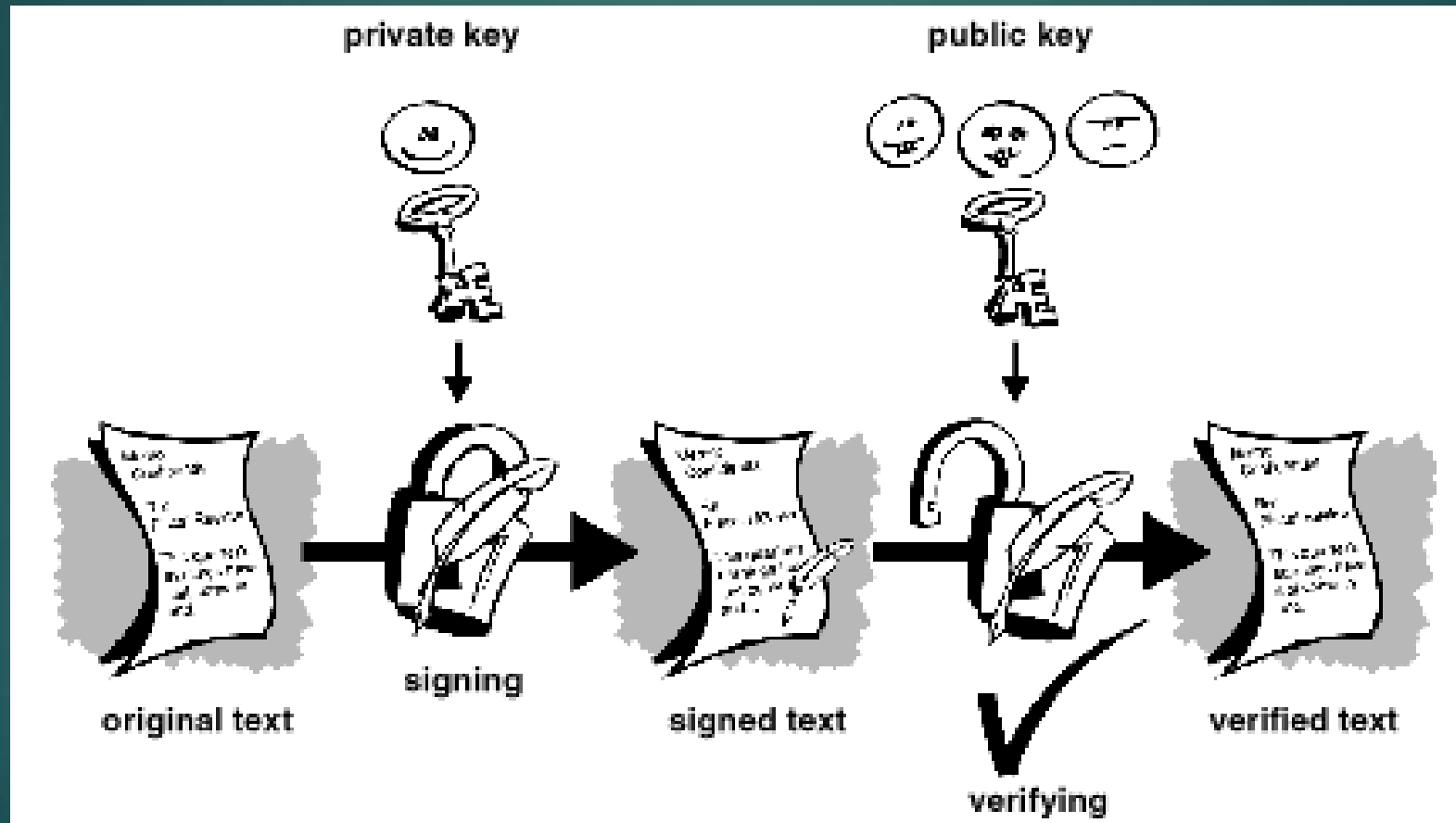
Password:

Confirm:

 **Cancel**  **OK**

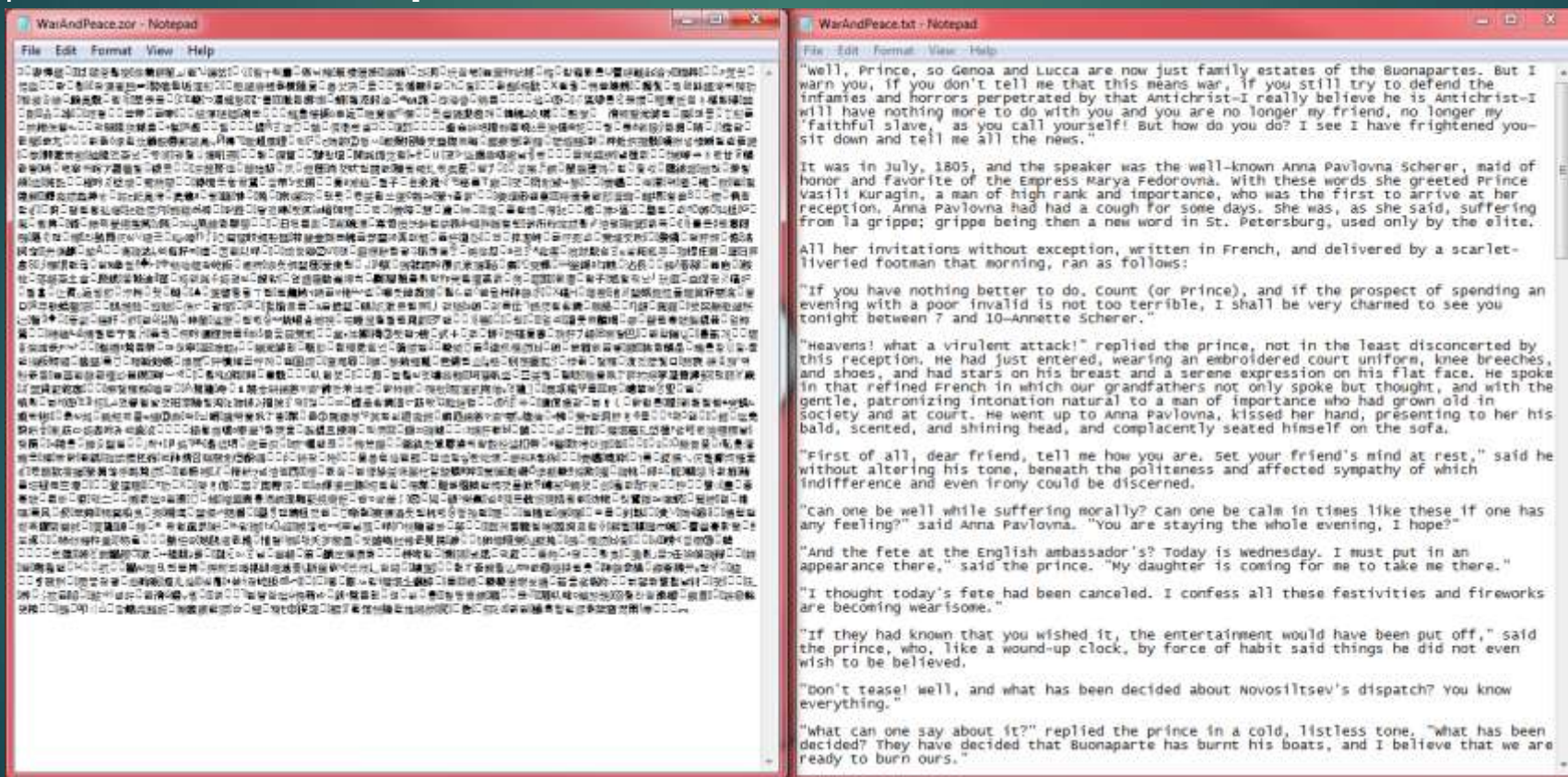


Autenticação (Assinatura Digital)

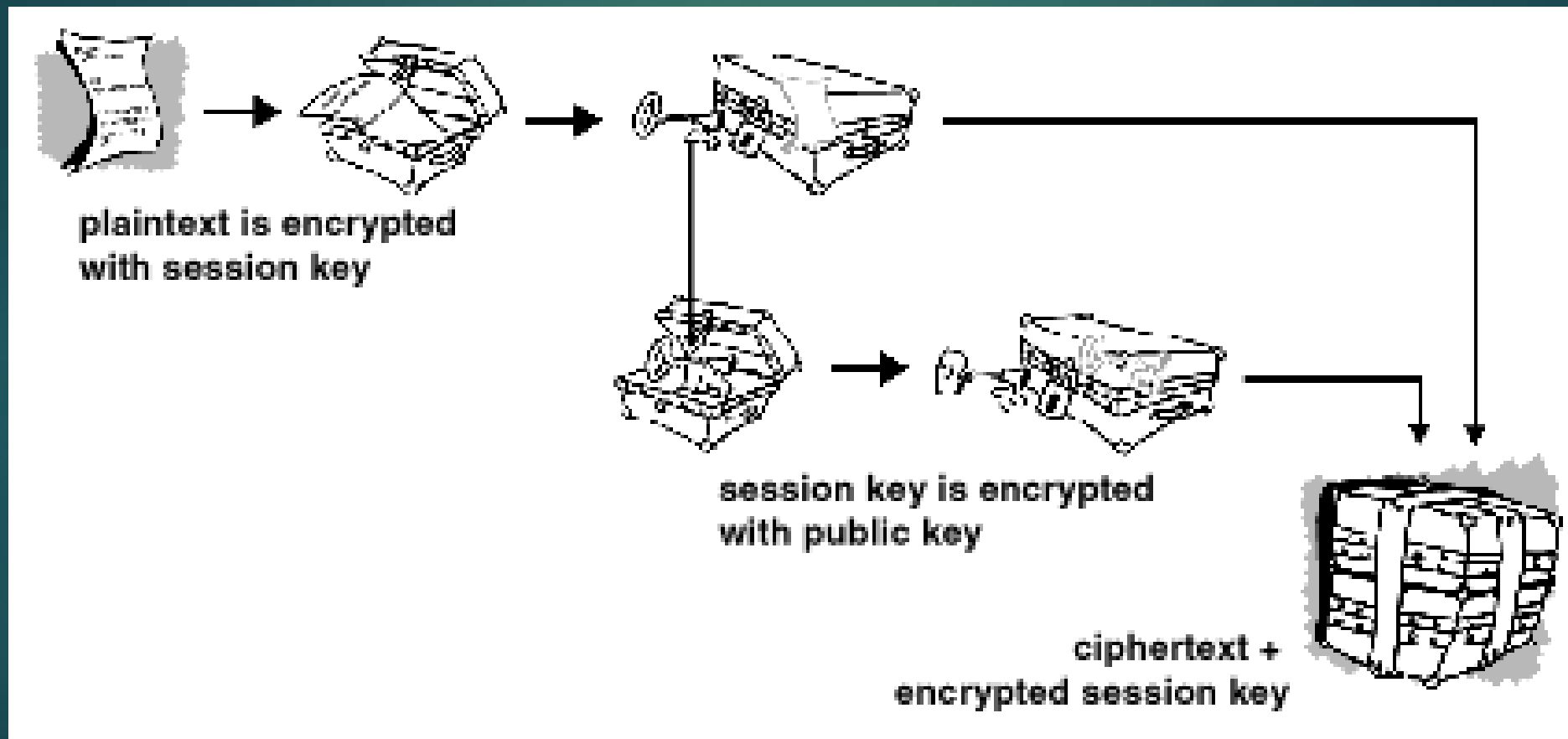


Compressão

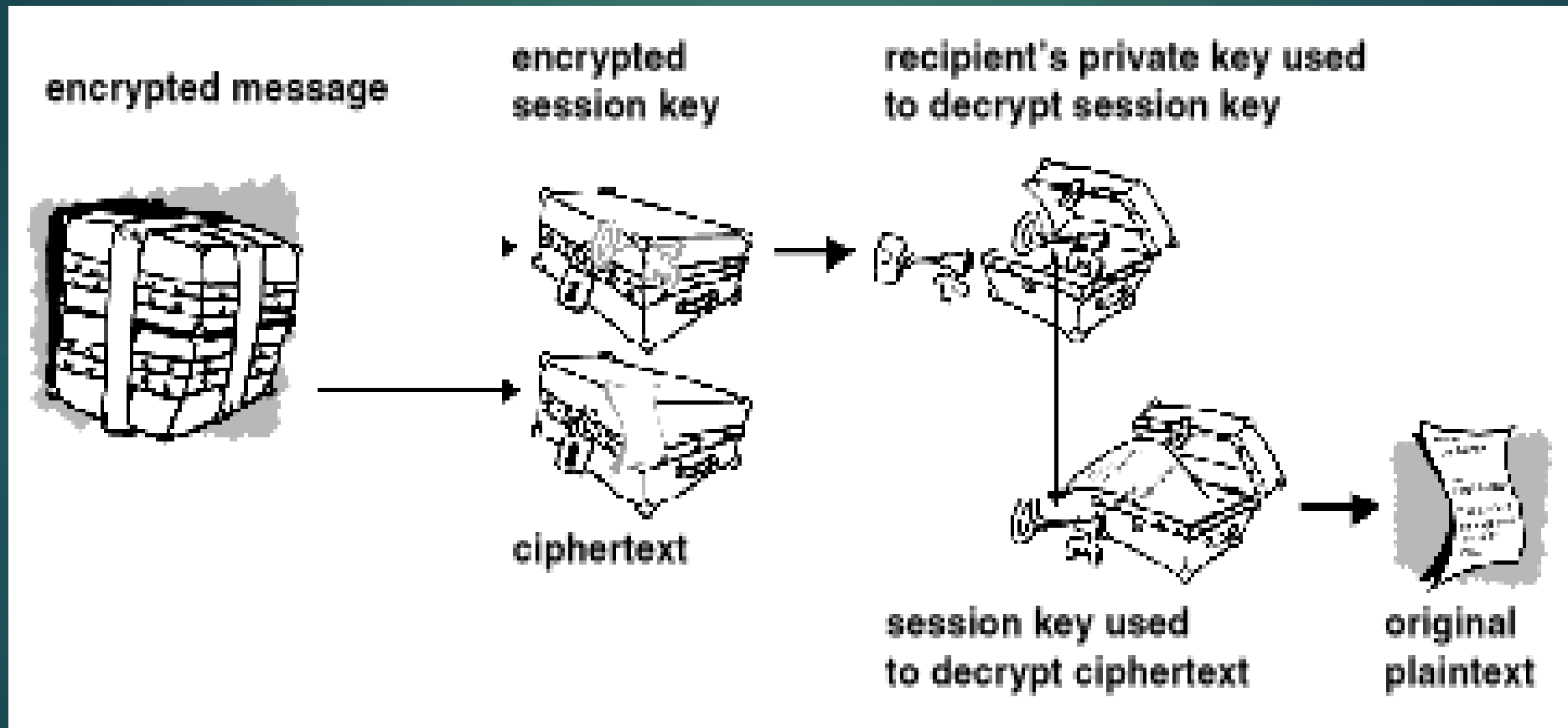
- ▶ Entre a etapa de assinatura da mensagem e a criptografia propriamente dita é aplicada a compressão Zip (LZ78) no texto plano: **reduzir os padrões!**



Confidencialidade: Encriptação



Confidencialidade: Decifração



Modelos de Confiança

- ▶ Confiança Direta
- ▶ Confiança Hierárquica
- ▶ Rede de Confiança
 - ▶ Níveis de Confiança
 - ▶ Confiança Completa
 - ▶ Confiança Marginal
 - ▶ Inconfiável
 - ▶ Níveis de validade
 - ▶ Válido
 - ▶ Marginalmente Valido
 - ▶ Inválido

Conclusão

- ✓ Utilização de esquema de chaves públicas e privadas
- ✓ Confiança mútua entre clientes
- ✓ Encadeamento de codificações
- ✓ Interoperabilidade entre diversos algoritmos amplamente conhecidos
(LZ78, RSA, IDEIA, DAS, ElGamal, SHA, CAST, AES, TripleDES, Twofish...)

Referências

- ▶ TENENBAUM, A. *Computer Networks*. 4th Ed. Elsevier Brasil, 2003.
- ▶ ZIMMERMANN, P.. *Pretty Good Privacy: "To PGP or not to PGP"*. 2003.
- ▶ YAW, D. PGP: An Algorithmic Overview. Rochester Institute of Technology Rochester, NY. 2001.
- ▶ PGP 6.5.1 Documentation <<http://www.pgpi.org>>. Acesso em: 14 jun. 2013.
- ▶ Algoritmo ElGamal <http://en.wikipedia.org/wiki/ElGamal>. Acesso em: 11 jun. 2013.



Dúvidas?



Obrigado!