Segurança de E-mail

- O e-mail é hoje um meio de comunicação tão comum quanto o telefone e segue crescendo
- Gerenciamento, monitoramento e segurança de e-mail têm importância cada vez maior
- O e-mail é muito inseguro, pois pode atravessar várias redes até chegar ao destino
- E-mail é vulnerável a:
  - Interceptação e quebra de privacidade
  - Replicação, adulteração, falsificação de conteúdo
  - Falsificação de identidade

Requisitos de Segurança de E-mail

- Privacidade de conteúdo
  - Tecnologia de criptografia para codificação
- Integridade da mensagem
  - Algoritmo de *hash* / *message digest* ou MAC
- Verificação de remetente
  - Assinatura digital
- Verificação de destinatário
  - Criptografia com chave-pública

Protocolos de E-mail Seguro

- Padrões
  - PGP - Pretty Good Privacy & OpenPGP
  - S/MIME - Secure Multipurpose Internet Mail Extension (MIME)
  - PEM - Privacy-Enhanced Mail
  - MOSS - MIME Object Security Service
  - MSP - Message Security Protocol (uso militar)
- Padrões competidores não inter-operáveis dificultam sua popularização
- Mais difundidos: PGP e S/MIME

PGP – Pretty Good Privacy

- PGP
  - Mais popular ferramenta de privacidade e autenticação, principalmente para uso pessoal
  - Esforço pessoal de Philip R. Zimmermann
  - Essência do trabalho:
    - Selecionados os melhores algoritmos de criptografia como componentes
    - Algoritmos integrados em aplicação de uso geral e fácil
    - O produto, sua documentação e todo o código fonte disponibilizados publicamente na Internet
    - Acordo com uma empresa (Viacrypt, agora NAI) para disponibilização de uma versão comercial

PGP – Pretty Good Privacy

- Histórico do PGP
  - Versão pública inicial do PGP: Junho de 1991
  - PGPi 5.0: 1997
    - 1ª versão legalmente disponível fora dos EUA/Canadá
    - Exportado como código fonte em livros impressos e re-montado a partir de digitalização/OCR
  - Network Associates: versão comercial Dez/1997
  - OpenPGP: Padrão aberto IETF RFC 2440
    - GnuPG: implementação freeware do OpenPGP, sem o algoritmo patenteado IDEA (patente RSA expirou 2000)
    - OpenPGP Alliance: promove interoperabilidade entre implementações do padrão OpenPGP

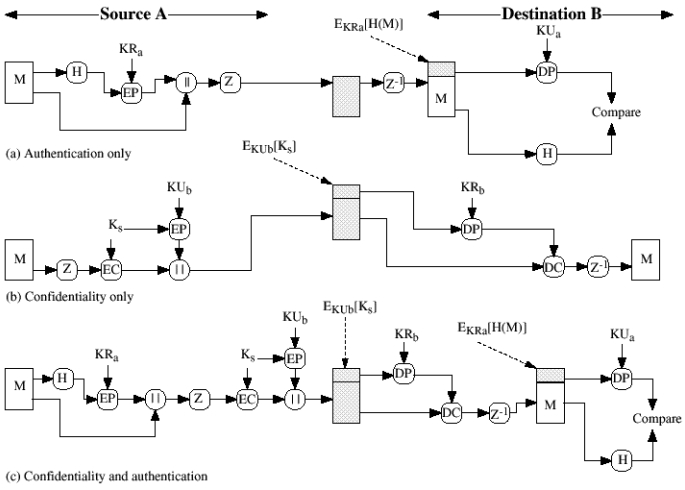
PGP – Pretty Good Privacy

- Sucesso do PGP
  - Disponibilidade gratuita e versões para muitas plataformas, com ferramentas para fácil utilização
  - Distribuição pública do código permitiu amplo estudo e garante credibilidade (certeza de não haver *back doors*) e amadurecimento (depuração)
  - Uso de algoritmos considerados muito seguros
  - Aplicável na segurança de e-mail, arquivos, VPN
  - Não desenvolvido ou totalmente controlado por nenhuma organização governamental ou privada

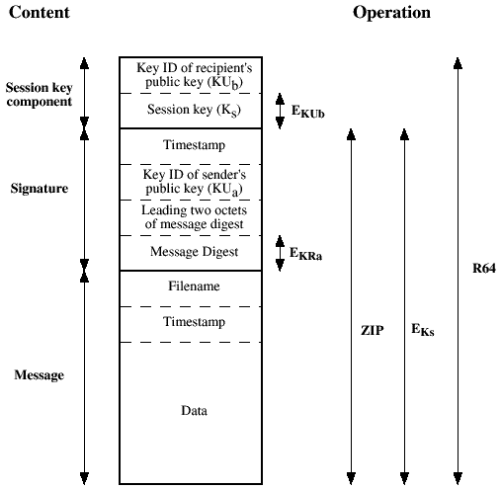
Operações do PGP

Função	Algoritmos	Descrição
Assinatura digital	Digest (hash) + Chave pública	Digest SHA cifrado com DSS ou RSA (chave privada do remetente)
Encriptação da mensagem	Criptografia convencional + Chave pública	Mensagem c/ encriptação convencional, chave secreta (sessão) protegida pela chave pública do destinatário (DH, RSA)
Compressão	ZIP	Reduzir tamanho e eliminar redundância compactando
Compatibilidade	Radix-64	Conversão do resultado para ASCII (uso em e-mail)
Segmentação		Capacidade de dividir a mensagem resultante em blocos de tamanho limitado

Operações do PGP



Formato da Mensagem PGP



Aspectos do PGP

- Assinatura digital:
  - Obtida por uma sinopse (*digest*) da mensagem criptografada com a chave privada do remetente
- Confidencialidade:
  - Encriptação usa criptografia convencional, que é em geral bem mais rápida que a de chave pública
  - Chave de sessão: uma chave secreta é gerada aleatoriamente para uso uma única vez, i.e., uma nova chave para cada mensagem cifrada
  - A chave da sessão vai junto com a mensagem, protegida pela chave pública do destinatário

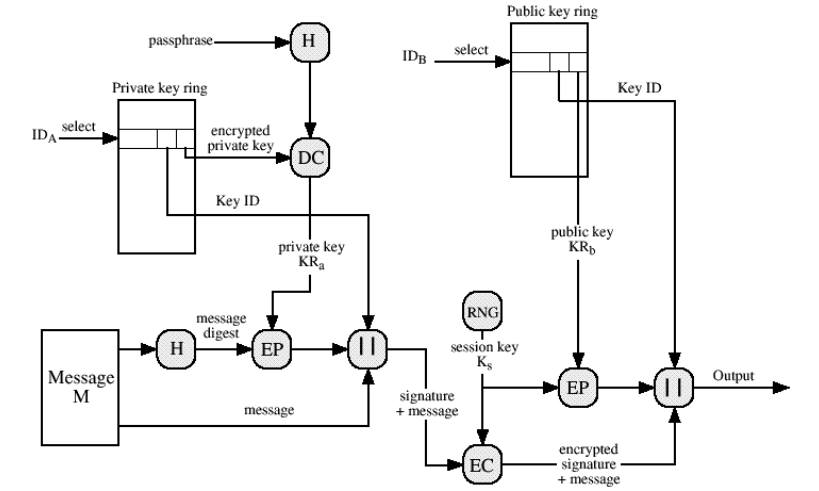
Aspectos do PGP

- Compactação ZIP:
  - Reduz o tamanho a armazenar ou transmitir
  - Realizada depois da assinatura e antes da criptografia convencional da mensagem
  - Depois da assinatura: validação da mensagem s/ depender de comprimir antes e do algoritmo ZIP
  - Antes da criptografia: reduz redundância (padrões) na mensagem original, aumentando a segurança
- Compatibilidade com e-mail:
  - Codificação do resultado em ASCII com Radix64
  - Possibilidade de segmentar resultado, se grande

Tratamento de Chaves PGP

- Private key ring (Chaveiro de chave privada)
  - Existe uma chave mestre associada ao usuário, define sua identificação e é usada para assinatura
  - Podem ser definidas chaves alternativas para codificação, que podem ter validade ou ter a chave pública revogada em caso de problema
  - A chave privada é armazenada codificada por criptografia convencional. A chave secreta é hash da senha (frase-passe) escolhida pelo usuário

Uso de Chaves no PGP



Tratamento de Chaves PGP

- Public key ring (Chaveiro de chaves públicas)
  - As chaves públicas podem ser assinadas digitalmente por usuários que atestem sua legitimidade
  - Para o usuário atestar/aceitar a validade de uma chave pública em seu chaveiro, deve assiná-la e associar um nível de confiança
  - A legitimidade de uma chave pública é dada pelo conjunto dos níveis de confiança dos assinantes

S/MIME

- S/MIME
  - Secure/Multipurpose Internet Mail Extension
  - Baseado em tecnologia da RSA Security
  - Embora tanto PGP quanto S/MIME sejam definidos como padrões pela IETF, S/MIME surge mais como padrão de indústria para uso comercial e organizacional, enquanto PGP é mais escolhido em segurança pessoal de e-mail
  - Essencialmente, tem as mesmas funções de autenticação e confidencialidade do PGP, embutidas no padrão MIME de conteúdo

S/MIME

- Nomeclatura das funções S/MIME:
  - **Enveloped data**: conteúdo (de qualquer tipo) criptografado, com chave de sessão criptografada para um ou mais destinatários
  - **Signed data**: é feita uma assinatura digital do conteúdo por uma *message digest* cifrada com a chave privada do assinante. Tanto o conteúdo quanto a assinatura são codificados em base64
  - **Clear-signed data**: é formada uma assinatura digital do conteúdo, mas apenas a assinatura é depois codificada em base64 (conteúdo intacto)
  - **Signed and enveloped data**: assinatura + cifra

S/MIME

- Chaves públicas
  - Distribuídas em certificados X.509v3 assinados por Autoridade de Certificação (CA)
- Certificados Chave-Pública S/MIME Verisign
  - Vários classes de segurança, de acordo com a forma de confirmação de identidade
  - Classe 1: validação automática do nome e e-mail (envio de um PIN e ID digital para o e-mail)
  - Classe 2: Classe 1 + validações automatizadas no cadastro de pagamento e sobre o endereço postal
  - Classe 3: Classe 2 + identificação pessoalmente