

## Protocolos de Segurança

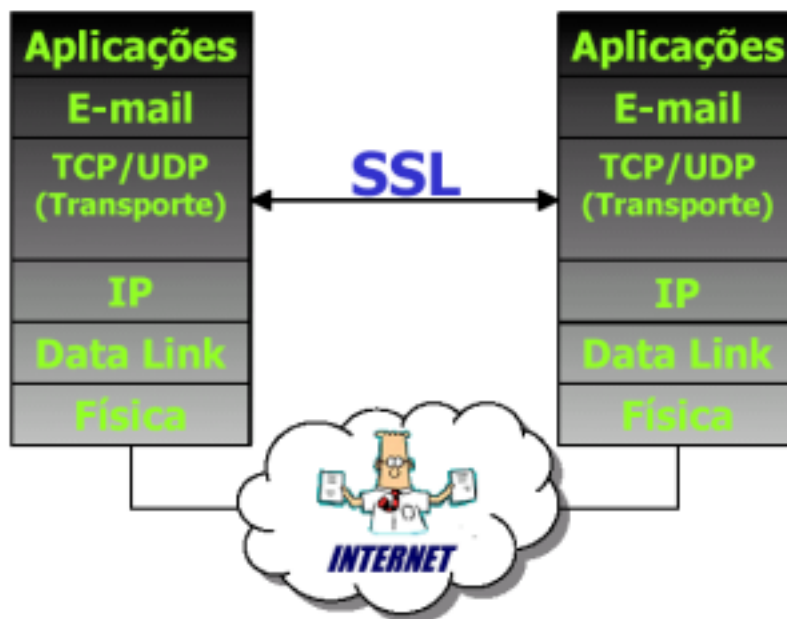
A criptografia resolve os problemas envolvendo a autenticação, integridade e o sigilo. Porém, isto não garante que uma comunicação seja segura. Há a necessidade da formalização de um protocolo de comunicação para que as técnicas de criptografia sejam eficientes.

Um protocolo é definido como uma série de passos, envolvendo duas ou mais partes, projetadas para realizar uma tarefa. Cada passo será executado um de cada vez, e nenhum passo pode ser iniciado antes que o passo anterior esteja concluído. Dessa maneira, o protocolo poderá garantir a legitimidade da comunicação.

## SSL

O SSL é um serviço que faz uso do TCP para prover um serviço seguro fim-a-fim. O Protocolo de Registro do SSL prove o serviço de segurança básica para as altas camadas do protocolo. Em particular ao HTTP que faz o serviço de transferência da Web na interação cliente/servidor.

Três outras camadas do protocolo são definidas como parte do SSL: protocolo inicial, Protocolo SSL de Troca de Cifrador, Protocolo SSL de Alerta.



Dois conceitos importantes do SSL são a conexão e a sessão. A conexão provém um serviço de transporte que esta associada a uma sessão. A sessão é

## AULA 08 – Protocolos de Segurança

uma associação entre um cliente e o servidor que é criada pelo protocolo inicial. A sessão define um grupo de parâmetros criptográficos de segurança.



O serviço de registro do protocolo SSL provê dois serviços para a conexão SSL:

- Confidencialidade: o protocolo inicial define a troca de chave secreta que será usada na criptografia convencional;
- Integridade da Mensagem: o protocolo inicial também define a troca de chave secreta que será usada no código de autenticação de mensagem (MAC).

O Protocolo SSL de Registro fragmenta os dados de aplicação em blocos de 16384 bytes, podendo usar ou não a compressão nos dados, adiciona o MAC, criptografando com a chave de sessão. Em seguida adiciona o cabeçalho de registro SSL e transmite o resultado para a unidade no segmento TCP.

### PGP

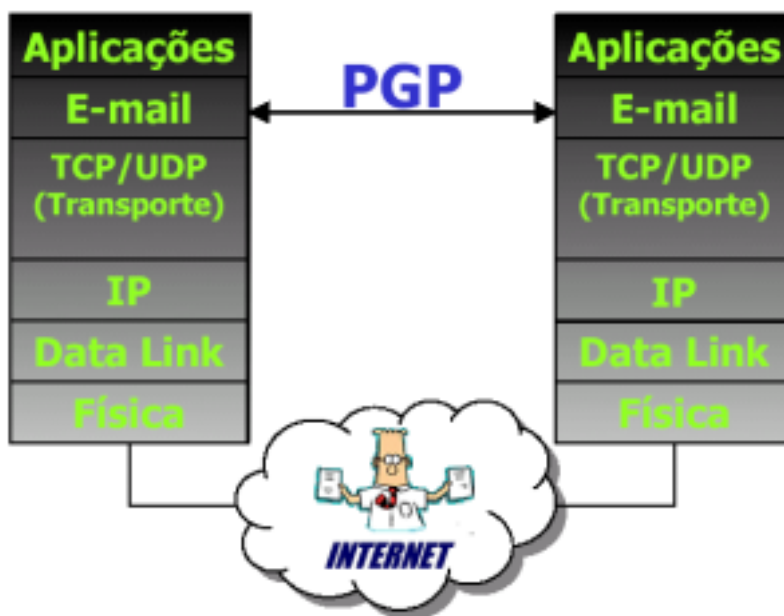
Como mencionado anteriormente, a criptografia é o método para obter uma transmissão de dados segura, onde apenas o receptor terá acesso à mensagem a ele endereçada e poderá ainda saber se o transmissor é realmente quem diz ser e se a mensagem foi alterada no caminho.

O correio eletrônico (e-mail) é um dos recursos mais utilizados na Internet, contudo não é intrinsecamente seguro. O internauta se conecta a um servidor SMTP para enviar uma mensagem. O servidor retransmite essa mensagem por vários caminhos, passando por diversos roteadores até ser armazenada em um provedor, aguardando que o destinatário se conecte na rede e leia. Em qualquer ponto deste trajeto, um outro internauta mal intencionado pode interceptar, ler e até mesmo alterar o conteúdo da mensagem.

## AULA 08 – Protocolos de Segurança

Um dos programas de criptografia para e-mail mais utilizado na atualidade é o PGP (Pretty Good Privacy - Ótima Privacidade), criado em 1991 por Philip Zimmermann. Os serviços fornecidos pelo PGP para arquivos e e-mails são:

- Confidencialidade;
- Autenticação da origem;
- Integridade da informação;
- Não-repúdio.



Os algoritmos de criptografia utilizados pelo PGP estão relacionados na tabela seguinte:

FUNÇÃO	ALGORITMO	DESCRIÇÃO
Assinatura Digital	DSS/SHA ou RSA/SHA	O SHA é usado para criar o HASH CODE
Criptografia	CAST ou IDEA ou 3DES	A mensagem é criptografada com um algoritmo convencional
Criptografia	Diffie-Hellman ou RSA	A chave de criptografia usada é anexada à mensagem, após criptografada com um algoritmo de chave pública/privada
Compressão	ZIP	Após assinar e antes de criptografar. Redução de 50%
Segmentação		Devido ao tamanho limitado das mensagens
Compatibilidade de e-mail	RADIX 64	Aumento de 30% no tamanho original da mensagem

Tabela 1 – Algoritmos de criptografia do PGP

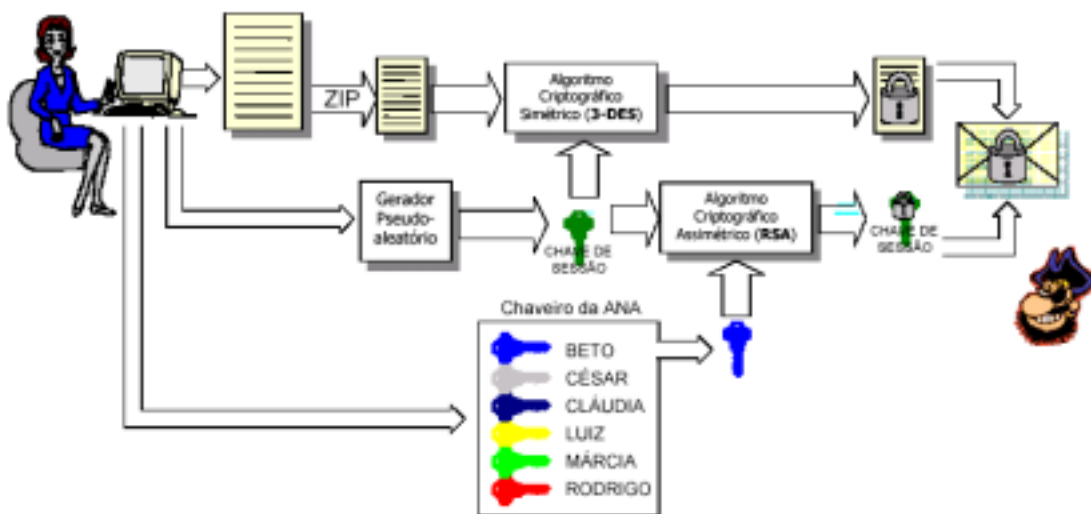
## AULA 08 – Protocolos de Segurança

### Chave de Sessão

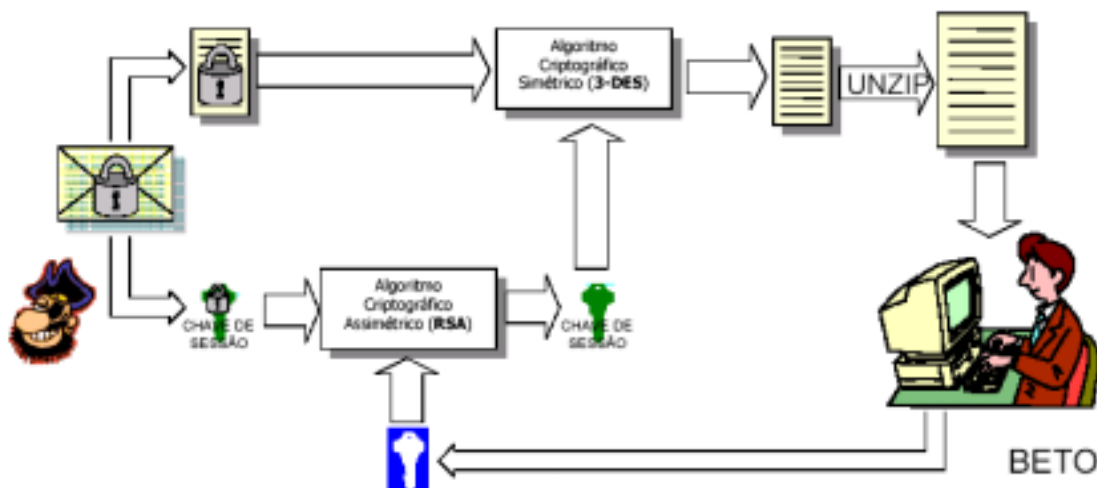
Como o próprio nome diz, chave de sessão é criada somente para uma determinada sessão. No caso do PGP, por questões de performance, a mensagem é encriptada com um algoritmo simétrico e somente a chave de sessão é encriptada com a chave pública do destinatário. A mensagem enviada contém o texto cifrado e a chave de sessão encriptada.

O PGP possui um chaveiro (keyrings), o qual contém sua chave privada e pública e as chaves públicas dos destinatários. O PGP trata as chaves da seguinte maneira:

1. As chaves públicas e privadas são armazenadas de forma criptografada no disco (o conjunto é chamado de keyrings);
2. O usuário pode ter mais de um conjunto de chaves publica/privada;
3. O usuário pode adicionar chaves públicas de outras pessoas;
4. Se a chave privada for perdida não há maneira de ser recuperada;



## AULA 08 – Protocolos de Segurança



Com o PGP é possível enviar mensagens com sigilo (somente encriptada com a chave pública do destinatário), assinada (somente com a chave privada do remetente), assinada e com sigilo (utilizando a chave privada do remetente e a chave pública do destinatário).

O PGP não inclui uma autoridade certificadora para associar os usuários a seus certificados, adotando um princípio de confiança mútua. Em termos práticos isto se dá através da assinatura nos certificados. Os certificados do PGP ficam em um diretório público e uma pessoa pode assinar (garantir a identidade) o certificado de outra.

O estabelecimento de confiança entre duas pessoas pode ser definido da seguinte maneira:

- Uma pessoa “A” deseja trocar informações com uma pessoa desconhecida “B”;
- Existe uma terceira pessoa “X” que conhece e confia em “A” e conhece e confia também em “B” e vice-versa;
- Se “A” confia em “X” e “X” confia em “B”, então “A” pode confiar em “B”.

### IP Seguro (IPSec)

A Internet foi projetada inicialmente visando fornecer conectividade entre computadores para um número restrito de usuários que confiavam mutuamente entre si. Por esse motivo, o Internet Protocol (IP) não foi projetado para fornecer segurança, foi projetado para ser tolerante a falhas de hardware. Assumiu-se que a tarefa de segurança fosse realizada por protocolos de maior nível de abstração.

## AULA 08 – Protocolos de Segurança

### Arquitetura

O IPSec provê a capacidade de comunicação segura entre LAN's, WAN's e Internet, podendo ser utilizado em conexões entre organizações e para aumentar a segurança no uso do comércio eletrônico.

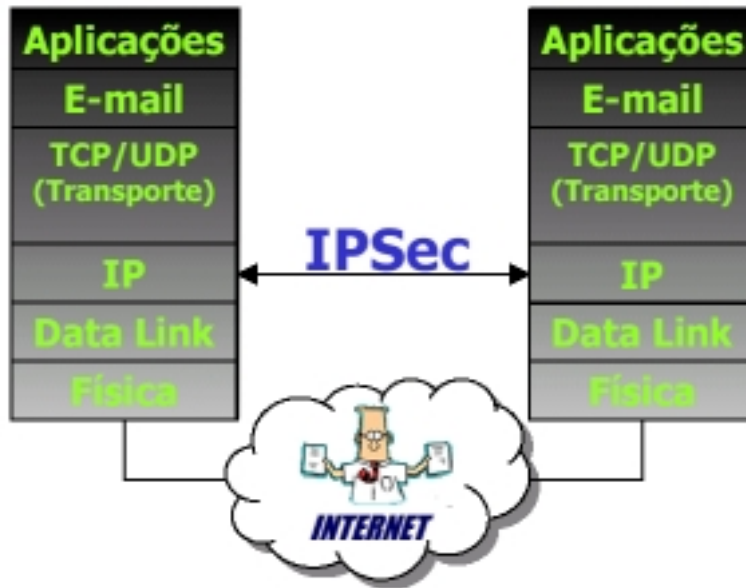


Figura 1 - Cenário do IPSec

A especificação do IPSec foi definida pelo IETF - Internet Engineering Task Force, através de um conjunto de documentos (RFC's - *Request For Comments*), cada um abordando detalhes específicos do IPSec:

- **RFC 1825** - Arquitetura de Segurança do IP traz uma visão geral dos mecanismos de segurança aplicados no IP, ou seja define a estrutura do IPSec (autenticação, confidencialidade, integridade, Não-repúdio, encriptação, análise de tráfego, gerência de chave e acesso de controle);
- **RFC 1826** - Authentication Header (AH) - descreve o mecanismo de autenticação e integridade para os datagramas do IPv4 e IPv6;
- **RFC 1827** - Encapsulating Security Payload (ESP) - o protocolo ESP é um mecanismo que fornece integridade e confidencialidade aos datagramas do IP e, em determinadas circunstâncias, pode também fornecer autenticação, pode ser usado no IPv4 e IPv6. Dependendo do domínio do usuário o protocolo ESP pode ser usado em vários segmentos da camada de transporte como TCP, UDP, ICMP E IGMP;
- **RFC 1828** - Especificação do Mecanismo de Autenticação - aborda questões quanto ao uso de chaves, tamanho de dados e performance;

## AULA 08 – Protocolos de Segurança

- **RFC 1829** - Especificação do Mecanismo de Encriptação – aborda questões como o uso de chaves, inicialização de vetores, tamanho de dados, performance, formato do Payload, algoritmo de encriptação e decriptação.

