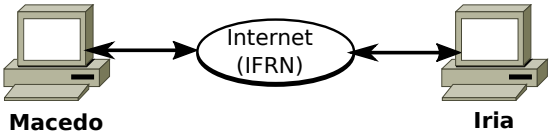
Professor: Macêdo Firmino
Disciplina: Segurança de Rede
Prática 14: Criptografia de Chave Simétrica com OpenSSL e Esteganografia com Steghide

---

Olá, meus alunos!! Como é que vocês vão? Na aula de hoje iremos entender o conceito de criptografia simétrica e realizar a criptografia e descriptografia de arquivos no Kali Linux utilizando ferramentas de linha de comando. Conheceremos ainda uma técnica de esconder segredos chamado de esteganografia. Utilizaremos a ferramenta Steghide para esconder informações dentro de um arquivos de imagem, de forma que sua existência passe despercebida. Vamos lá!!! Preparados???

Configurando o Ambiente

Para estudarmos estes conceitos e ferramenta iremos utilizar duas máquinas virtuais. Uma para transmitir os segredos (Iria) e outra para receber os segredos (Macedo). Podemos utilizar qualquer distribuição Linux. Nos nossos testes utilizei Kali Linux configurada em "Rede Nat".



Criptografia

Criptografia é o conjunto de técnicas utilizadas para proteger informações, transformando dados legíveis (texto claro) em dados embaralhados (texto cifrado), de forma que apenas pessoas autorizadas consigam entendê-los.

Ela é utilizada há milênios e que atualmente faz parte do nosso cotidiano oferecendo soluções eficazes no que diz respeito à segurança da informação. Ela é uma ferramenta de segurança amplamente utilizada nos meios de comunicação e consiste basicamente na transformação de determinado informação a fim de ocultar seu real significado.

Por exemplo:

- Mensagem original (texto claro): A senha é 1234
- Mensagem criptografada (texto cifrado): F#3h$@1xVj!

Só quem souber o algoritmo e tiver a chave certa poderá reverter a mensagem cifrada para o conteúdo original.

Existem atualmente duas abordagens para criptografia, as simétricas e as assimétricas. A criptografia simétrica foi o primeiro tipo de criptografia criado. Os algoritmos que a utilizam têm como característica principal o uso de uma mesma chave criptográfica para criptografar ou descriptografar uma informação. Sem a chave, não é possível decifrar a informação recebida.

As vantagens da criptografia simétrica: alta velocidade (ideal para grandes volumes de dados), algoritmos mais simples e eficientes e menor uso de recursos computacionais. Por outro lado, as desvantagens da criptografia simétrica são: necessidade de trocar a chave de forma segura, se a chave for interceptada, todo o sistema está comprometido e pouco escalável para muitos usuários (cada par precisa de uma chave compartilhada).

A criptografia assimétrica, também denominada como criptografia de chave pública, possui como característica básica o uso de duas chaves ao invés de uma, sendo elas:

- Chave pública: chave que pode ser distribuída para outros usuários.
- Chave privada: deve ser mantida em segredo.

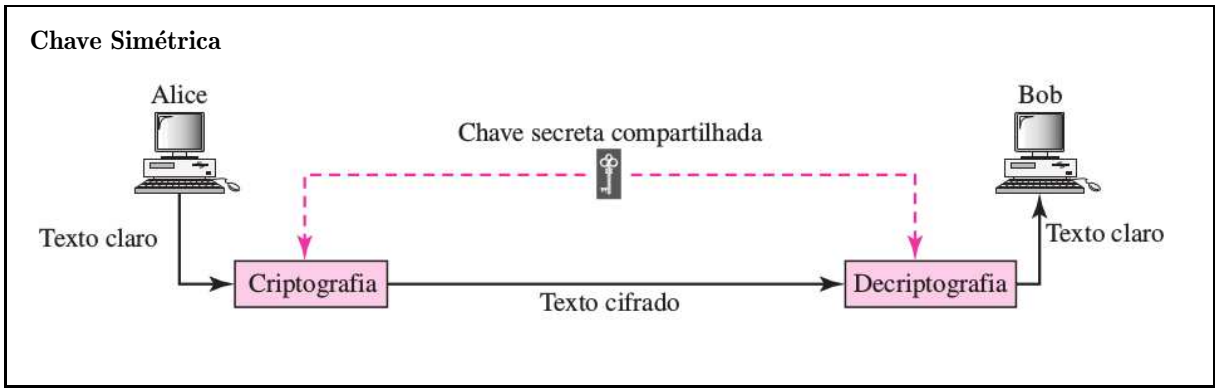
Neste modelo de criptografia, o texto cifrado pela chave pública somente poderá ser decifrado com a chave privada.

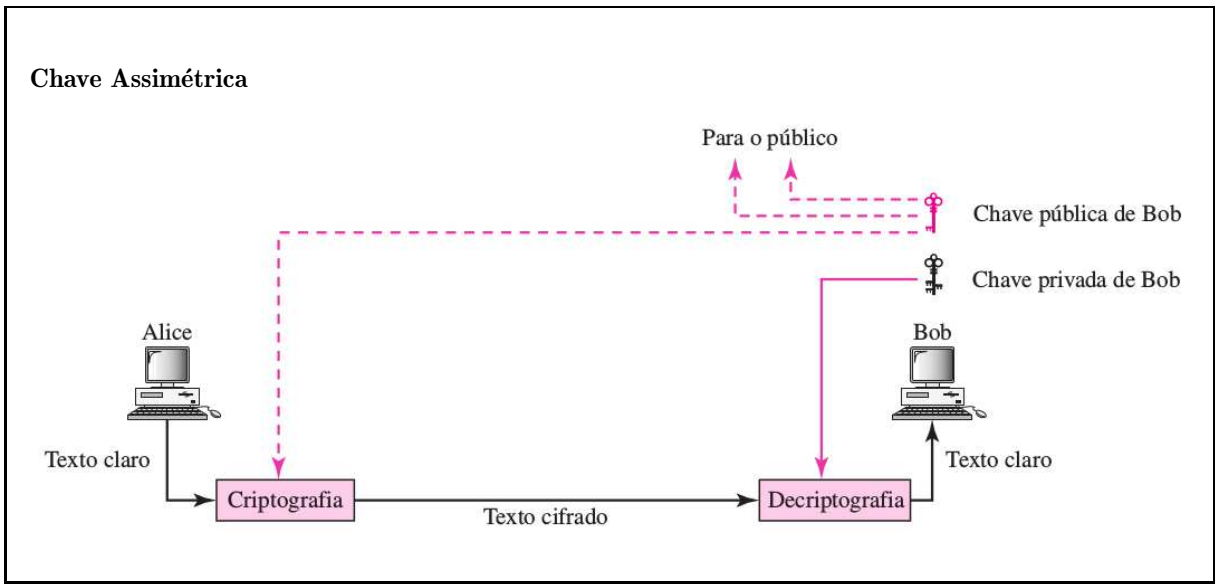
As vantagens da criptografia assimétrica: não exige compartilhamento da chave privada, permite assinatura digital e verificação de autenticidade e é melhor escalabilidade (uma única chave pública pode ser usada por muitos). Entretato, tem como desvantagens: mais lenta (muito mais pesada que a simétrica), requer mais processamento e energia e algoritmos e implementação são mais complexos.

Na sequência iremos utilizar algumas ferramentas que implementam algoritmos de criptografia para vermos o funcionamento da criptografia simétrica na prática.

OpenSSL

OpenSSL é um conjunto de ferramentas e bibliotecas de código aberto que permite a realização de tarefas relacionadas à segurança, como criptografia, geração de certificados, assinatura digital e conexões seguras (SSL/TLS). O Kali Linux já vem com o OpenSSL instalado por padrão, pois é uma ferramenta essencial em testes de segurança, criptografia e análise de redes.





O OpenSSL suporta uma ampla gama de algoritmos de criptografia, tanto simétricos quanto assimétricos, entre eles:

- AES (Advanced Encryption Standard): é o algoritmo simétrico mais recomendado atualmente. Suporta chaves de 128, 192 e 256 bits. Pode operar em diversos modos como CBC, ECB, CFB, OFB e GCM.
- Triple DES (3DES): realiza criptografia simétrica o processo DES três vezes, oferecendo maior segurança que o DES original. Suporta chaves de 112 ou 168 bits, mas é mais lento.
- RSA (Rivest-Shamir-Adleman): é o algoritmo assimétrico mais conhecido. Suporta tamanhos de chave de 1024 a 4096 bits, sendo usado para criptografia de chaves, assinatura digital e em certificados SSL/TLS.
- DSA (Digital Signature Algorithm): usado exclusivamente para assinaturas digitais. As chaves geralmente variam entre 1024 e 3072 bits.
- ECDSA e ECDH: baseados em curvas elípticas, são algoritmos assimétricos modernos, mais eficientes, que oferecem alta segurança com chaves menores (entre 160 e 521 bits).

Criptografia com AES no OpenSSL

Agora iremos utilizar o OpenSSL para criptografar um arquivo para mandar pela internet para o destinário realizar a decriptografia e realizar a leitura. Para isso siga os seguintes passos:

01. Criar um arquivo de texto com uma mensagem simples. Você poderá utilizar o seu editor preferido. Abaixo está um exemplo de criação usando o comando echo.

```
echo "Invasao amanha as 8h" > segredo.txt
```

02. Criptografar o arquivo usando criptografia AES de 256 bits no modo CBC.

```
openssl enc -aes-256-cbc -in
 segredo.txt -out segredo.txt.enc
```

Será solicitado que você informe uma senha e depois que você confirme a senha. Podemos utilizar a senha "ifrn". Na sequência será criado o arquivo segredo.txt.enc.

03. Com um visualizador abra o arquivo criptografado. Seria possível entendermos o conteúdo do arquivo?

```
cat segredo.txt.enc
```

04. Envie o arquivo criptografado para a outra máquina (Macedo).

05. Agora no destino (Macedo) vamos descriptografar o arquivo utilizando o OpenSSL e a senha compartilhada, com o comando:

```
openssl enc -aes-256-cbc -d -in
 segredo.txt.enc -out
 segredo_recuperado.txt
```

07. O arquivo segredo_recuperado.txt irá surgir, agora basta ler o conteúdo do arquivo.

```
cat segredo_recuperado.txt
```

Esteganografia

A esteganografia é uma técnica utilizada para esconder informações dentro de outros arquivos digitais, de forma que sua existência passe despercebida. Diferente da criptografia (que oculta o conteúdo de uma mensagem) a esteganografia tem como objetivo ocultar a própria presença da mensagem.

A esteganografia moderna utiliza arquivos comuns, como imagens, áudios, vídeos ou documentos, como meios de cobertura (chamados de cover files) para esconder mensagens ou arquivos inteiros dentro deles. A modificação geralmente é imperceptível ao olho ou ouvido humano, o que garante a discrição da comunicação.

Ferramentas de esteganografia normalmente criptografa a mensagem (ou arquivo) com um algoritmo (como AES, por exemplo) e, em seguida, o conteúdo criptografado é embutido dentro de um arquivo de cobertura (como uma imagem, áudio ou vídeo).

Por exemplo iremos esconder um arquivo de texto dentro de uma imagem JPEG. Ao abrir a imagem, ela parecerá normal, mas com ferramentas específicas e, em alguns casos, com uma senha, é possível extrair o conteúdo secreto. Para isso, utilizaremos a ferramenta steghide criptografa os dados com AES-128 antes de escondê-los.

Steghide

O Steghide é uma ferramenta de linha de comando que permite ocultar arquivos dentro de imagens ou arquivos de áudio, utilizando técnicas de esteganografia. Desenvolvido para sistemas Unix/Linux, ele utiliza criptografia simétrica, tornando-se uma solução poderosa para proteger informações de forma discreta e segura.

O Steghide embute dados no arquivo de cobertura de forma imperceptível, utilizando técnicas como a substituição de bits menos significativos (LSB - Least Significant Bit). Isso significa que pequenas variações são feitas em áreas do arquivo que não afetam sua visualização ou reprodução, mantendo o conteúdo oculto invisível para usuários comuns.

Caso ele não esteja isntalado utilizar os comandos:

```
sudo apt update
sudo apt install steghide
```

Iremos inserir uma mensagem de texto secreto e oculto em uma imagem. Para isso siga os seguintes passos:

01. Criar um arquivo de texto com uma mensagem simples. Por exemplo, utilize o comando echo.

```
echo "Invadir pelo Setor Norte" > secreto.txt
```

02. Pegar a imagem que irá ocultar o segredo. utilizaremos a imagem do IFRN (imagem_ifrn.jpg), mas poderá ser qualquer imagem.

03. Utilize o comando abaixo para esconder o texto secreto na imagem do IFRN.

```
steghide embed -cf imagem_ifrn.jpg
 -ef secreto.txt
```

onde: cf é arquivo de cobertura (imagem ou áudio) e ef especifica o arquivo que você quer esconder.

O Steghide solicitará uma senha (pode utilizar “ifrn”), que será usada para criptografar o conteúdo antes de embutir. Guarde-a bem, pois será necessária na extração.

Você pode até comparar o tamanho do arquivo antes e depois. A diferença será pequena, pois o conteúdo foi compactado.

Você pode enviar imagem.jpg para alguém por e-mail, pendrive ou outro meio. A imagem parecerá completamente normal.

04. O destinatário deverá utilizar o comando abaixo para recuperar o arquivo oculto.

```
steghide extract -sf imagem_ifrn.jpg
```

onde: sf deverá especificar o arquivo com dados escondidos (imagem ou áudio).

O Steghide solicitará a mesma senha usada na etapa de embutir. Se a senha estiver correta, o arquivo secreto.txt será extraído no mesmo diretório.

05. Veja o conteúdo do arquivo:

```
cat secreto.txt
```

Atividades

01. Forme duplas e troquem mensagens criptografadas com o openssl. Responda:

- **a)** O que acontece se usar uma senha errada na descriptografia?
- **b)** A criptografia por si só oculta a existência da mensagem?

02. De forma individual, crie um arquivo de texto com seu nome e sua matrícula. Criptografe o arquivo com algoritmo AES e senha "ifrn@sga". Depois mande o arquivo criptografado pelo Google Sala de Aula.

03. Escolha uma imagem.jpg qualquer para servir como arquivo de cobertura. Crie um novo arquivo de texto com o seu nome e sua matrícula. Use o steghide para esconder esse arquivo dentro da imagem, protegendo com senha ("ifrn@sga"). Depois mande a imagem com o texto secreto pelo Google Sala de Aula.