

Professor: Macêdo Firmino

Disciplina: Segurança de Rede

Prática 16: Criptografia de Chave Pública com RSA no OpenSSL

Olá, meus alunos!! Como é que vocês vão? Na aula de hoje iremos entender o conceito de criptografia assimétrica (pública), gerar um par de chaves (pública e privada) com OpenSSL e criptografar e descriptografar mensagens utilizando RSA e OpenSSL no Kali Linux. 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.

A criptografia com chave pública, também chamada de criptografia assimétrica, é um sistema de segurança da informação baseado no uso de dois pares de chaves diferentes: uma chave pública e uma chave privada. Essas chaves são matematicamente relacionadas, de modo que o que for criptografado com uma pode ser descriptografado apenas com a outra.

Nesse modelo, a chave pública é amplamente divulgada e pode ser usada por qualquer pessoa para criptografar uma mensagem ou arquivo. Já a chave privada é mantida em segredo pelo seu proprietário e serve para descriptografar as informações recebidas.

Esse tipo de criptografia oferece uma solução segura para a troca de mensagens em ambientes abertos, como a Internet, pois elimina a necessidade de compartilhar uma chave secreta entre as partes antes da comunicação.

A criptografia assimétrica é amplamente utilizada em sistemas de segurança digital, como em conexões HTTPS (utilizando protocolos como SSL/TLS), no envio de e-mails criptografados (PGP/GPG), em carteiras de criptomoedas, além de servir como base para a geração e validação de certificados digitais.

Entre os algoritmos mais conhecidos de criptografia com chave pública estão o RSA (Rivest-Shamir-Adleman), ECC (Criptografia de Curvas Elípticas), ElGamal e o DSA (Digital Signature Algorithm).

Esse modelo é considerado um dos pilares da segurança da informação, pois pode oferecer confidencialidade, autenticidade, integridade e não repúdio das informações trocadas entre usuários.

RSA

O algoritmo RSA, criado em 1977 pelos matemáticos Ron Rivest, Adi Shamir e Leonard Adleman. Ele é um dos sistemas de criptografia assimétrica mais utilizados no mundo. Ele se baseia em princípios da teoria dos números e na dificuldade de fatorar grandes números primos.

Na sequência iremos conhecer o algoritmo de geração das chaves (Chave pública e privada) RSA.

1. Escolhem-se dois números primos grandes:

$$p \text{ e } q$$

2. Calcula-se o produto desses primos

$$n = p \times q$$

3. Calcula-se o totiente de Euler:

$$\varphi(n) = (p - 1) \times (q - 1)$$

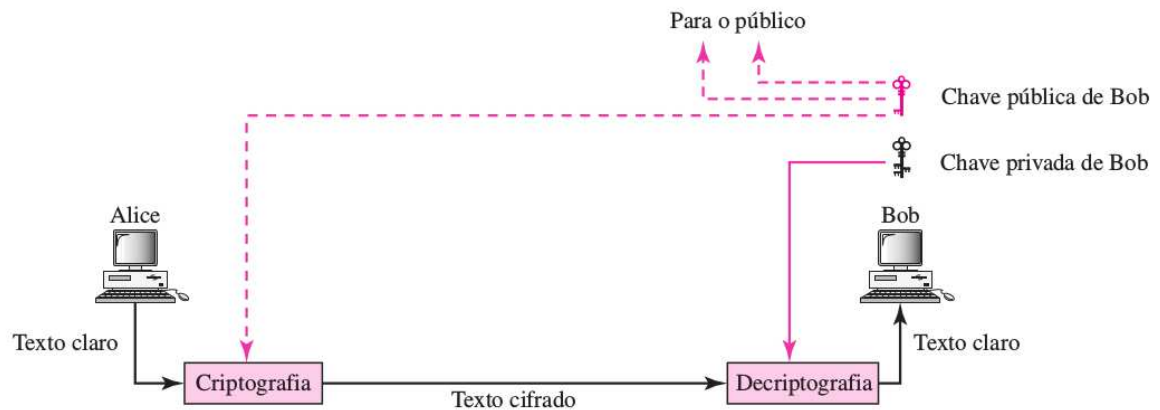
4. Escolhe-se um número e tal que (ou seja, e e $\varphi(n)$ são coprimos):

$$1 < e < \varphi(n) \text{ e } \text{mdc}(e, \varphi(n)) = 1$$

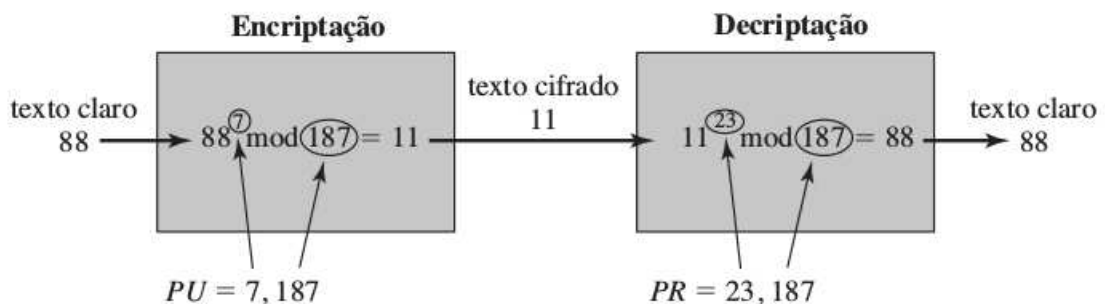
5. Calcula-se o d , tal que:

$$(d \times e) \bmod \varphi(n) = 1$$

Chave Assimétrica



Exemplo RSA



Como resultado temos:

- Chave pública: (e, n) usada para criptografar;
- Chave privada: (d, n) usada para descriptografar.

Para entendermos melhor o algoritmo iremos rodar um exemplo simples (com números pequenos):

1. Supondo $p = 17$ e $q = 11$,
2. Calculando

$$\begin{aligned} n &= p \times q \\ n &= 17 \times 11 \\ n &= 187 \end{aligned}$$

$$\begin{aligned} \varphi(n) &= (p-1)(q-1) \\ \varphi(n) &= (17-1) \times (11-1) \\ \varphi(n) &= 16 \times 10 = 160 \end{aligned}$$

3. Um valor adequado para e é 7, visto que $1 < 7 < 160$ e 7 e 160 são primos entre si.

4. Escolhe $d = 23$, pois:

$$\begin{aligned} (e \times d) \bmod z &= 1 \\ (7 \times 23) \bmod 160 &= 1 \\ 1 &= 1 \end{aligned}$$

A chave pública: $(7, 187)$ e a chave privada: $(23, 187)$.

Cifração e decifração são realizadas da seguinte forma, considere um texto original (M) e o texto criptografado (C). A relação entre eles é:

- Criptografia:

$$C = M^e \pmod{n}$$

- Decriptografia:

$$M = C^d \pmod{n}$$

Por exemplo, considere criptografando a mensagem 88.

$$\begin{aligned} C &= M^e \pmod{n} \\ C &= 88^7 \pmod{187} \\ C &= 11 \end{aligned}$$

A mensagem enviada será 11. O receptor irá receber o 11 e realizará a descriptografia com sua chave privada para recuperar a mensagem original, da seguinte forma:

$$\begin{aligned}M &= C^d \pmod n \\M &= 11^{23} \pmod{187} \\M &= 88\end{aligned}$$

Openssl

OpenSSL é um conjunto de ferramentas e uma biblioteca de software de código aberto que implementa os protocolos SSL (Secure Sockets Layer) e TLS (Transport Layer Security), além de fornecer suporte para criptografia de dados com diversos algoritmos. Nós já trabalhamos com ele na aula passada com o algoritmo simétrico AES.

Ele já geralmente já vem instalado por padrão nas distribuições Linux. Ele tem versões ainda para as distribuições Windows e MacOS.

Criptografia com RSA no OpenSSL

Agora iremos utilizar o OpenSSL para criptografar um arquivo para mandar pela internet para o destinatário realizar a descriptografia e realizar a leitura, usando criptografia com chave pública.

Neste exemplo, consideramos que Alice quer enviar uma mensagem secreta para Bob. Ela usará a chave pública de Bob para criptografar a mensagem. Apenas Bob, que possui a chave privada correspondente, poderá descriptografá-la. Para isso siga os seguintes passos:

01. Geração de par de chaves RSA de Bob com 2048 bits.

```
openssl genpkey -algorithm RSA
-out bob_private.pem
-pkeyopt rsa_keygen_bits:2048
```

Como resultado é gerado o arquivo bob_private.pem, que contém a chave privada RSA de Bob.

02. Extração da chave pública de Bob.

```
openssl rsa -pubout -in bob_private.pem
-out bob_public.pem
```

Este comando gera o arquivo bob_public.pem, que pode ser compartilhado com qualquer pessoa para que ela envie mensagens criptografadas para Bob.

03. O remetente (Alice) deverá 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 "Curso de Redes e Tranquilo" >
segredo.txt
```

04. O remetente (Alice) criptografa a mensagem usando a chave pública de Bob.

```
openssl pkeyutl -encrypt
-inkey bob_public.pem -pubin
-in segredo.txt
-out mensagem_criptografada.bin
```

O conteúdo de segredo.txt agora está cifrado em mensagem_criptografada.bin. Mesmo que esse arquivo seja interceptado, ninguém poderá lê-lo sem a chave privada de Bob.

05. O remetente (Alice) deverá enviar a mensagem_criptografada.bin para Bob.

06. Bob, após receber a mensagem irá descriptografá-la com sua chave privada.

```
openssl pkeyutl -decrypt
-inkey bob_private.pem
-in mensagem_criptografada.bin
```

O conteúdo original da mensagem será exibido no terminal. A confidencialidade está garantida pois somente Bob pode ler o que Alice enviou, mesmo se alguém tiver acesso ao arquivo criptografado.

Atividade

01. Você precisa enviar uma mensagem confidencial para o seu professor (com seu nome e sua matrícula). No entanto, como a mensagem pode ser interceptada, você deve criptografá-la com a chave pública do professor. Para isso, baixe a chave pública do professor Macedo no Google Sala de Aula, criptografe a mensagem e anexe o texto codificado também no Google Sala de Aula.