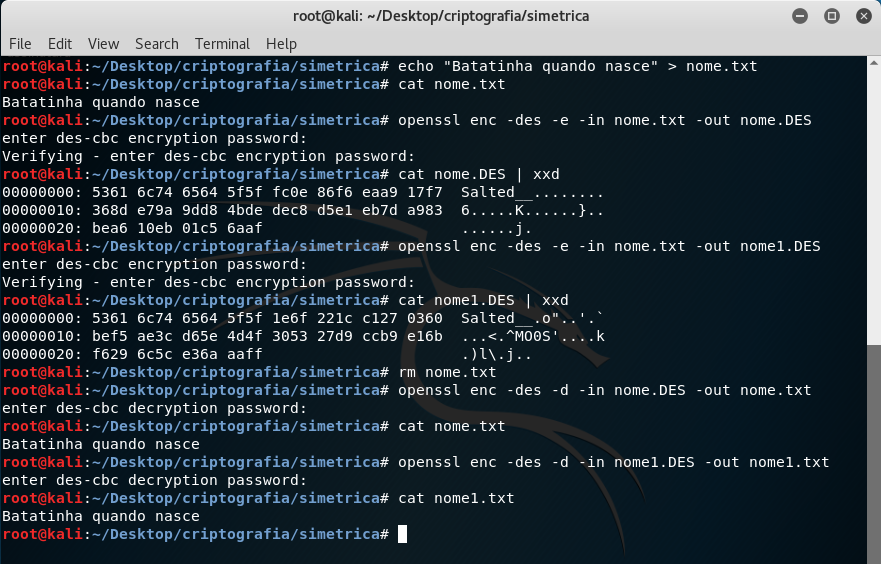
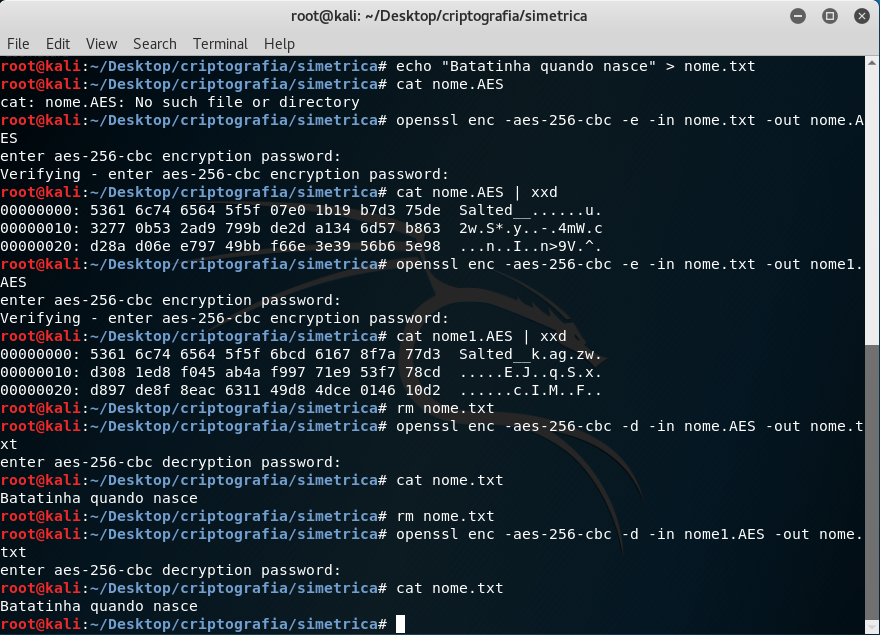
**Igor Correa 15.00588-7**

**Rodrigo Franciozi 14.04014-0**

DES:



AES:

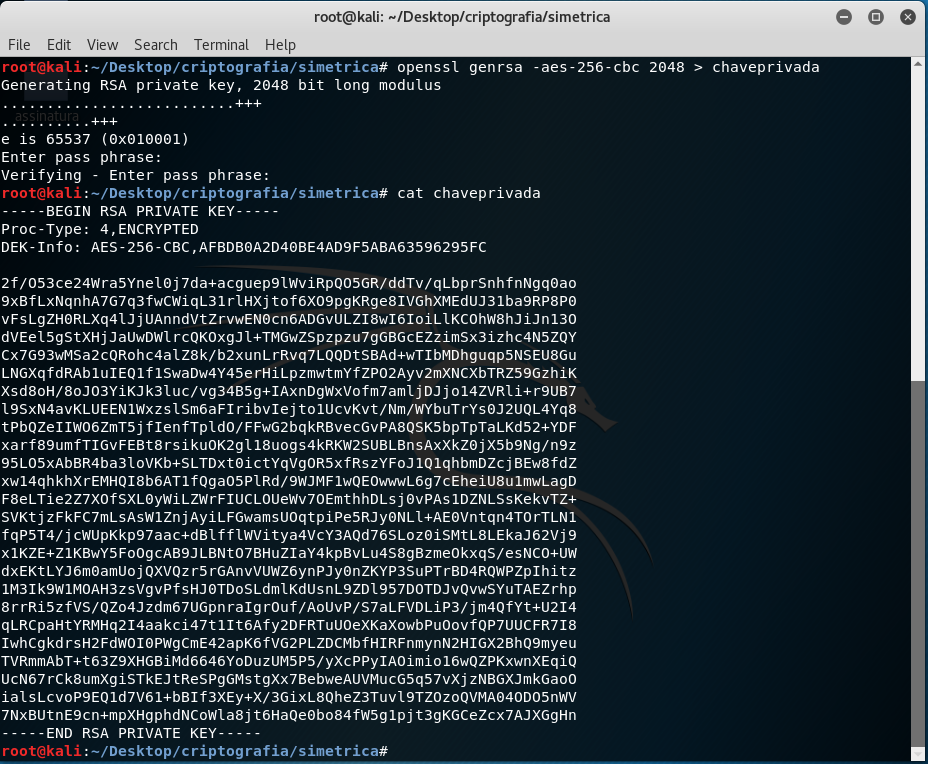


1.2) Os dois são algoritmos geram valores diferentes para uma mesma entrada por conta da utilização do sal, que é uma entrada adicional gerada aleatoriamente, colocada nessa entrada.

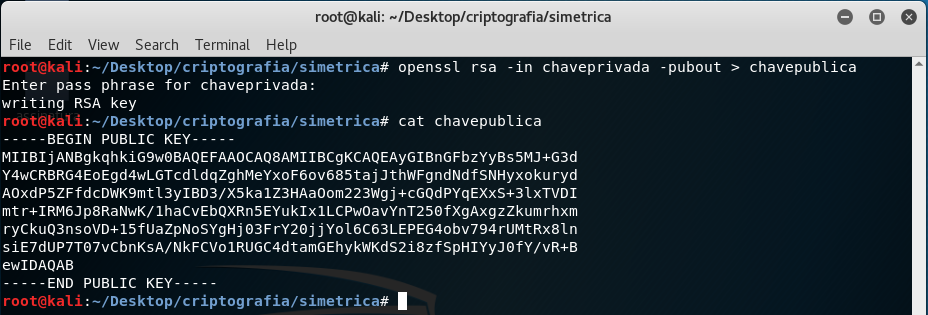
1.3) O DES é um algoritmo mais vulnerável que o AES por conter uma chave de criptografia de tamanho menor.

2.1)

Privada:

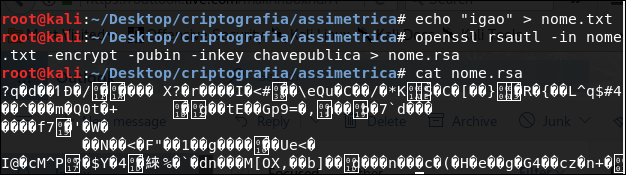


Publica:

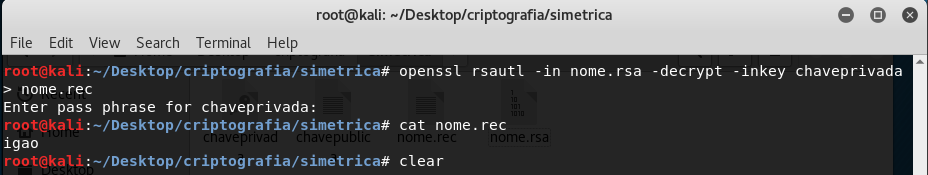


﻿

Arquivo:



Decriptografia:



2.1) O destinatário, pois ele deverá decriptografar e receber o arquivo do remetente para ler os dados.

2.2) O remetente criptografa o arquivo, pois o a chave pública foi gerada a partir da privada, e apenas o remetente tem a chave privada para poder decriptografar o arquivo.

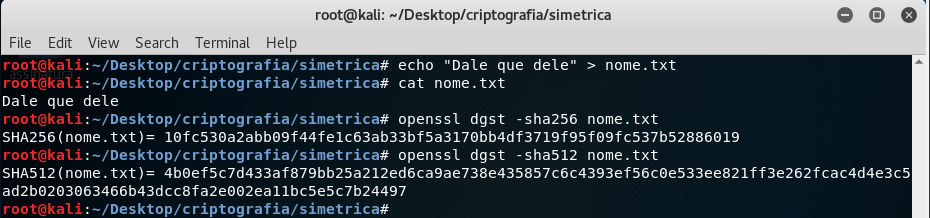
2.3) A chave pública do destinatário é usada para se criptografar o arquivo, pois quando for devolvido a ele necessita-se haver uma comparação e verificação do arquivo enviado.

2.4) O destinatário decriptografa o arquivo para poder ler a analisar o que lhe foi enviado.

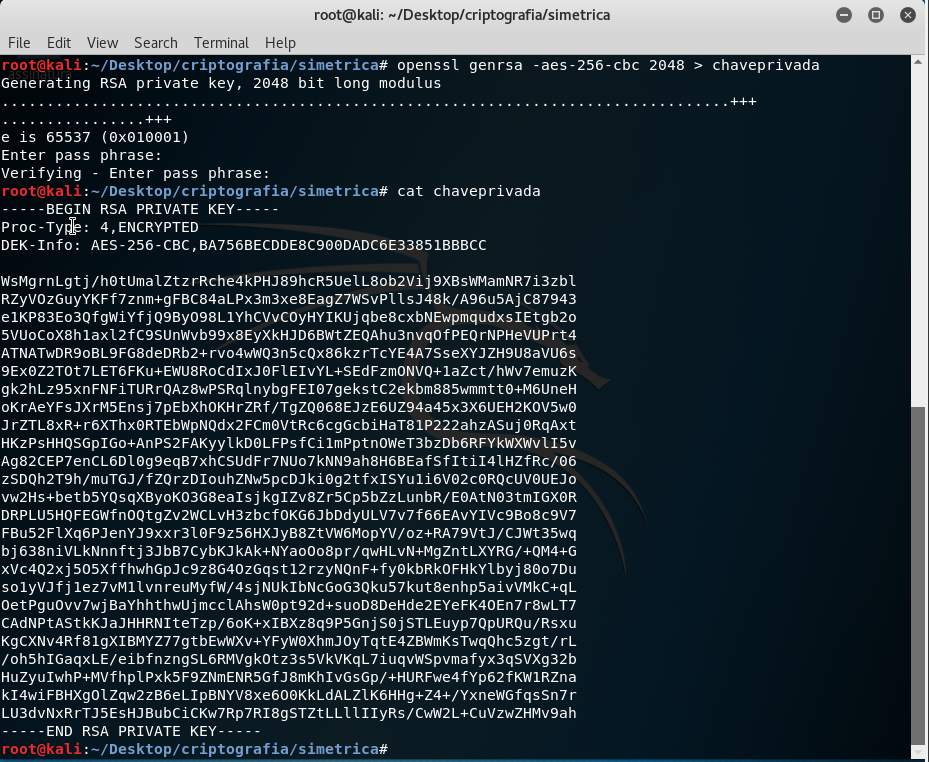
2.5) A chave privada do destinatário, pois como somente ele tem acesso a essa chave é o único que pode abrir o arquivo.

3)

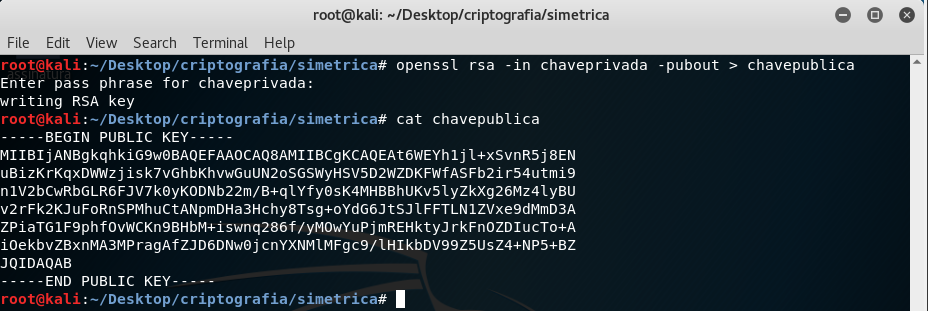
Arquivo e Hash:



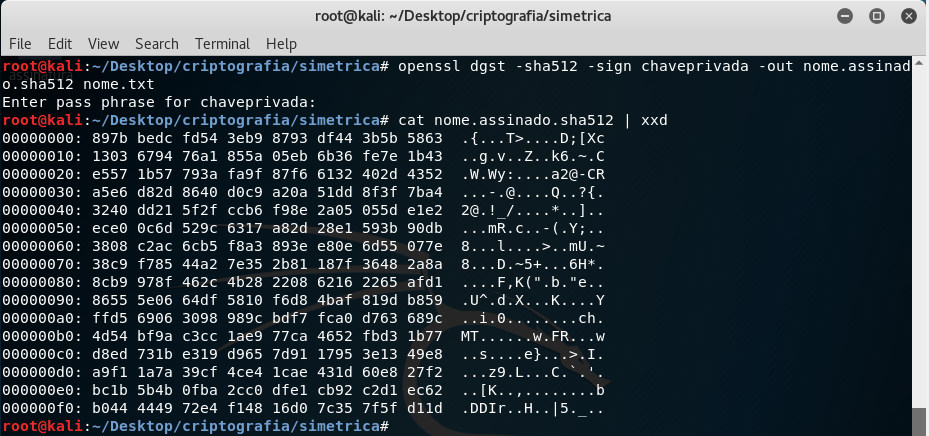
Chave privada:



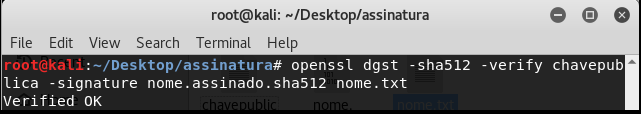
Chave pública:



Assinatura:



Verificação:



3.1) O remetente que deve gerar o par de chaves, pois ele precisa assinar o arquivo com elas antes de enviar para o destinatário.

3.2) O remetente que assina o arquivo, pois ele que tem a chave privada para poder gerar a assinatura.

3.3) A chave privada é usada para assinar o arquivo, pois o arquivo tem que estar criptografado com uma informação que não esteja acessível para todos.

3.4) O destinatário que verifica a assinatura do arquivo, pois como o foi o remetente que gerou o arquivo, não faz sentido ele mesmo verificar o arquivo.

3.5) O destinatário precisa da chave pública, o arquivo assinado e o arquivo sem assinatura, pois a chave pública junto com a assinatura consegue gerar o arquivo decriptografado e assim conferindo com o arquivo original.