Assinatura e Verificação com RSA

July 2022

1 Introdução

O trabalho consistiu em implementar um gerador e verificador de assinaturas RSA. Também é feita a encriptação de uma mensagem usando o algoritmo AES, bem como é feito a codificação da cifra gerada para o padrão BASE64. Todas essas funcionalidades têm suas respectivas inversões, isto é, decriptação do AES e decodificação BASE64.

2 AES

O algoritmo AES (do inglês Advanced Encryption System), também conhecido por Rjindael, seu nome original, é um algoritmo de cifra simétrica que executa um conjunto de operações definidas e, com base numa chave de 128, 192 ou 256 bits, encripta uma dada mensagem.

A chave é estendida para que possa ser utilizada nas várias rodadas da encriptação. A extensão da chave é feita de acordo com um método também predefinido pelo algoritmo. A partir deste, a chave que antes continha 4 *words* de 32 bits passa a ter 44 *words*.

As mensagens são divididas em diversos blocos de 16 *bytes* (128 bits), na forma de uma matriz 4×4, e encriptadas de acordo com as seguintes operações:

- Sub-Bytes - os *bytes* da mensagem são substituídos através da busca em uma tabela predefinida.
- Shift Rows - as linhas do bloco (a matriz) são deslocadas, isto é, seus elementos mudam de posição.
- Mix Columns - são executados cálculos aritméticos nas colunas do bloco que, de certa forma, combinam os *bytes*.
- Add Round Key - é feita uma operação de "ou exclusivo" (XOR) entre o bloco e a chave da rodada.

3 RSA

O algoritmo RSA (dos nomes dos criadoes Rivest-Shamir-Adleman) consiste em um algoritmo de chaves assimétricas. Isto é, serão gerados dois pares de chaves, sendo uma pública e uma privada. Estas chaves se invertem e a mensagem cifrada por uma pode ser cifrada pela outra.

Desta forma a chave pública, como o nome indica, pode ser exposta e qualquer pessoa pode cifrar uma mensagem para a qual só o dono da chave privada poderá decifrar.

Para a geração da chave são usados dois números primos de 1028 bits cada. Para o teste de primalidade foi utilizado o algoritmo Miller-Rabin.

3.1 Assinatura Digital

Com base no que foi definido das chaves assimétricas, estas permitem fazer uma assinatura digital.

Uma mensagem assinada com a chave privada de um usuário só poderá ser decifrada pela chave pública. Sendo assim, se é possível decifrar com a chave pública e, assumindo que a chave privada está em posse da pessoa correta, então a mensagem só pode ter vindo desta.

Para a assinatura o que é feito não é a cifração da imagem por inteiro, mas sim de um *hash* da mensagem. No projeto foi utilizado o algoritmo de *hash* SHA-3.

Então usa-se o SHA-3 para obter o *hash* da mensagem. Este é encriptado pela chave privada e enviado para o destinatário.

O destinatário recebe a mensagem, decifra com a chave pública, calcula o *hash* SHA-3 da mensagem e compara com o valor recebido, que acabou de ser decifrado. Se os dois valores são iguais, então a assinatura é válida.

4 Funcionamento do Programa

Ao executar o programa este pedirá uma mensagem para ser encriptada. Esta mensagem é a única forma entrada do programa.

O programa é executado da seguinte maneira, para a encriptação e assinatura:

1. Recebe uma mensagem de entrada.
2. Encripta mensagem usando AES.
3. Codifica a cifra para BASE64.
4. Calcula o *hash* da mensagem.
5. Encripta o *hash* utilizando RSA.

E para a decriptação e verificação de assinatura:

1. Recebe código BASE64.
2. Decodifica o código para a cifra AES.
3. Decifra com AES.
4. Calcula *hash* da mensagem.
5. Decifra *hash* encriptado pelo RSA.
6. Compara *hash* recebido com calculado.