1.Não repúdio

O não repúdio é quando um sujeito não pode negar que fez algo, tal como criar, modificar ou enviar um documento. Impedir que uma pessoa negue ter realizado uma ação específica, como enviar uma mensagem ou realizar uma transação. Mecanismos de não repúdio, tal como assinaturas digitais, podem ser usados para garantir a autenticidade das ações.

1.1 Hashing

Uma função hash é um algoritmo matemático que recebe um conjunto de dados de entrada e produz uma sequência de caracteres ou valores de tamanho fixo, chamados de *hash* ou *valor de hash*. Essa função tem a propriedade de ser rápida de calcular e determinística, ou seja, a mesma entrada sempre produzirá o mesmo *hash*. As funções hash são amplamente utilizadas em diversas áreas da computação, como criptografia, verificação de integridade de dados, autenticação e indexação de informações. Elas desempenham um papel fundamental na segurança e na eficiência de muitos sistemas.

1.2 Assinaturas digitais

As assinaturas digitais são uma técnica matemática usada para fornecer autenticidade, integridade e não repúdio. As assinaturas digitais têm propriedades específicas que permitem autenticação de entidade e integridade de dados. As assinaturas digitais são comumente usadas em **assinaturas de códigos e certificados digitais**.

Além disso, as assinaturas digitais fornecem não repúdio da transação. Em outras palavras, a assinatura digital serve como prova legal de que o intercâmbio de dados ocorreu. As assinaturas digitais usam criptografia assimétrica.

1.2.1 Autenticidade

A assinatura não pode ser falsificada e fornece prova de que o signatário, e ninguém mais, assinou o documento.

1.2.2 Inalterável

Após assinar um documento, ele não pode ser alterado.

1.2.3 Não reutilizável

A assinatura do documento não pode ser transferida para outro documento.

1.2.4 Não repudiado

O documento assinado é considerado o mesmo que um documento físico. A assinatura é a prova de que o documento foi assinado pela pessoa real.

Assinar digitalmente o código fornece várias garantias sobre o código como garantir que o código é autêntico e é realmente originado pela editora; O código não foi modificado desde que saiu do editor do software e a editora publicou inegavelmente o código. Isso fornece não repúdio do ato de publicação.

2.Extras

O conceito de não repudiação é quando você não pode negar o que disse/fez, quase como se fosse um contrato. Isto adiciona uma perspectiva diferente para a criptografia como a prova de integridade e prova de origem com garantia de autenticidade.

É a garantia de que os dados recebidos não foram alterados de nenhuma forma, isso é, preciso e consistente. Para conseguir, é necessário utilizar um *hash*, um algoritmo que representa dados em uma *string* de texto. A saída de um *hash* é denominado *message digest*, similar a digital humana. Se houver alteração, o *hash* produzido pelo receptor não irá bater com o *hash* de quem enviou. Apesar disto, um *hash* não associa dados a um indivíduo específico, logo, se houver alteração, não tem como saber quem fez a alteração.

A prova de origem (*proof of origin*) serve para garantir que a mensagem não foi alterada (integridade), provando que a mesma veio de quem estamos esperando (autenticação) e garantindo que a assinatura não foi forjada (não-repúdio). A prova de origem é feita com uma chave privada, onde a mensagem não precisa estar criptografada. A verificação da mensagem pode ser feita através da chave pública enviada em conjunto da mensagem.