Matemática Computacional

Aula 6

Professor Luís Gonzaga de Paulo

Conversa Inicial

Você chegou ao último encontro de **Matemática Computacional**!

Como você faz para manter o sigilo e segurança de seus dados na internet? Você sabia que existem técnicas para transformar um dado de sua forma original para uma forma super segura? Sobre isso, hoje você vai trabalhar com a Criptografia, além de entender o que é cifra, código e como os algorítmos e sistemas criptográficos funcionam.

Pronto para mais essa? Então vamos lá!

Visualize a introdução desta aula no material online com o professor Luís!

Contextualizando

Desde os primórdios da civilização o ser humano preocupa-se com a armazenagem e o transporte seguro de informações, especialmente quando se tratam de valores financeiros e informações militares. Muitas formas, algumas até engraçadas foram criadas, aprimoradas e utilizadas no decorrer da história, culminando com o advento da computação eletrônica e a efetiva constituição da criptografia como ciência, com embasamento matemático e apoiada na capacidade computacional. E pode-se perguntar o quão efetiva é tal ciência e o que temos conseguido a partir das suas formulações e postulados.

Afinal, como é possível – se é que isto é possível – garantir a confidencialidade, a integridade e a disponibilidade das informações digitais armazenadas nos computadores ou em trânsito por meio de redes e dispositivos removíveis e transportáveis?

Como podemos nos assegurar de estarmos comunicando com o interlocutor correto, sem interferências ou interceptações? É realmente possível evitar golpes e fraudes no mundo digital?

Quem pode nos garantir de que os processos que estamos usando são seguros e que nossas informações não serão usadas, divulgadas ou modificadas sem o nosso consentimento?

Nesta etapa da disciplina vamos abordar as bases do conhecimento necessário para pesquisar, entender e buscar as respostas para estas questões. O professor Luís explica um pouco sobre isso!

Confira no material online a contextualização feita pelo professor Luís.

Pesquise

TEMA 1: Criptografia

Existem muitas histórias a respeito da origem da criptografia, e muitas versões para estas muitas histórias. O que é a origem do termo, vem do Grego: *Kryptós*, que significa escondido, secreto, oculto e *Gráphein* que significa escrita. Ou seja, **criptografia = escrita escondida, secreta ou oculta.**

> A criptografia, como ciência, é uma área da Matemática destinada ao estudo de técnicas e princípios de transformação da informação de sua forma original para outra, ininteligível, de forma que possa ser conhecida e utilizada apenas quando autorizado.

Este processo de transformação da informação em seu estado original, geralmente chamado de texto plano (*plain text*), em um formato protegido pela ocultação de seu significado, chamado comumente de texto cifrado ou codificado é denominado **cifragem** (ou também criptografia, encriptação).

Ainda há o processo oposto, é denominado **decifragem** (ou descriptografia, descriptação), e quando é feito à revelia dos interessados ou proprietários da informação – de forma maliciosa ou não – é chamado de "quebra" da criptografia ou do código.

Recentemente o aplicativo WhatsApp começou a usar um sistema criptográfico mais moderno, no vídeo de Jefferson Meneses ele explica um pouco mais sobre esta atualização, confira no ícone a seguir e comece a entender o que é a criptografia na prática e no dia a dia!
https://www.youtube.com/watch?v=ucFuqi8zkYM

A criptografia também se refere ao estudo e ao uso de algoritmos criptográficos em programas de computador, e pode abranger ou se referir a outras áreas do conhecimento humano, tais como:

Criptoanálise

É a busca por informações que permite decifrar ou interpretar informações codificadas ou cifradas, descobrindo a chave ou método empregado para isto.

Esteganografia

Trata da ocultação de uma mensagem dentro de outra ou da mensagem em uma imagem ou música, por exemplo. Não é sinônimo de criptografia, pois enquanto a criptografia busca ocultar o sentido ou significado da mensagem ou da informação, a esteganografia visa ocultar a existência da mensagem, como diz o ditado popular: "o que os olhos não veem...". Isto é, a segurança por base no obscurantismo ou ocultação total.

Esteganalise ou Esteganoanálise

É a busca pela identificação de mensagens ocultas ou subliminares, isto é, a tentativa de identificar o uso da esteganografia.

Criptologia

É a ciência que congrega o uso de matemática e computação com as demais áreas do conhecimento humano para promover o avanço da criptoanálise e da criptografia. Antes tratada como questão acadêmica e restrita às áreas acadêmicas, financeiras e militares, tem ganhado impulso especialmente devido ao comércio eletrônico.

O uso da criptografia contribui para a solução dos diversos problemas de segurança da informação, no sentido de prover a confidencialidade, garantir a integridade, a disponibilidade, a privacidade, promover a autenticação e a irretratabilidade - ou não-repúdio - em operações realizadas por meio de computadores e dispositivos eletrônicos. Para isto, a criptografia lança mão do uso de diversas técnicas e métodos, dentre os quais:

- A criptografia assimétrica (Chave Pública).
- Criptografia simétrica (Chave única).
- Resumo criptográfico (Hash).
- Assinatura digital.
- Certificação digital.

O professor Luis agora traz um pouco mais sobre a criptografia para nós. Acompanhe no material online!

TEMA 2: Cifra e código

O processo de modificação da informação para tornar o armazenamento e o transporte seguro pode ser feito por meio do uso de **codificação** ou **cifragem**.

Embora o efeito prático seja parecido, são processos bastante diferenciados entre si. A **cifragem** é o tratamento de elementos mínimos da informação (nos computadores, o *bit*, por exemplo) para dificultar a sua compreensão. Este processo dispensa o conhecimento prévio da informação ou de regras de formato, sintaxe ou semântica. A cifragem é mais efetiva e, não obstante, mais complexa – mesmo do ponto de vista computacional, de se implementar. Além disso, a cifragem descaracteriza totalmente a informação, tirando-lhe qualquer sentido.

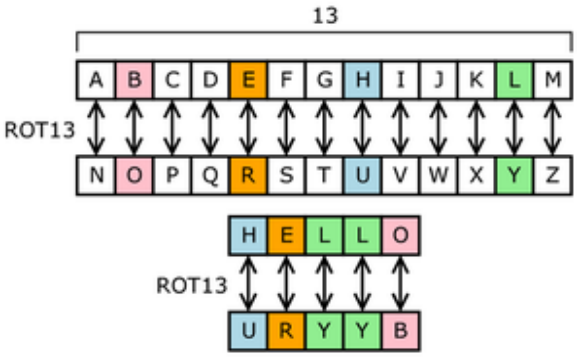
Quanto à sua complexidade, a cifragem é utilizada há muito tempo. Um dos mecanismos mais antigos de cifragem era a cítala.

Um bastão com determinado diâmetro no qual era enrolada uma faixa de couro na qual era escrito, no sentido longitudinal, a mensagem. Uma vez desenrolada a faixa o texto aparente na faixa tornava-se sem sentido, e para voltar a fazê-lo era necessário enrolar a faixa em um bastão do mesmo diâmetro.

Fonte: https://pt.wikipedia.org/wiki/C%C3%ADtala

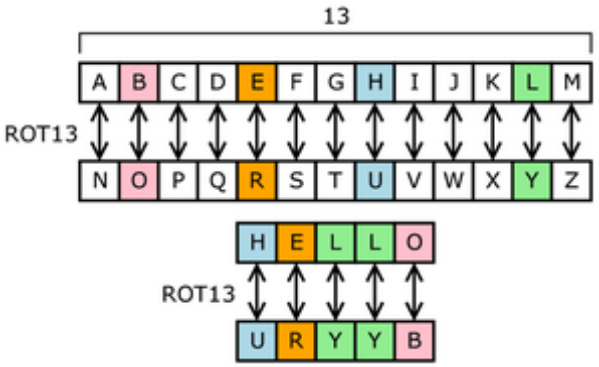
Outro mecanismo de cifragem bastante conhecido e empregado por um bom tempo pelos Romanos era a **Cifra de César**, baseada em um deslocamento da sequência de caracteres do alfabeto conhecida pelo emissor e pelo receptor da informação.

Esta cifragem é conhecida como cifragem de rotação e foi utilizada pelos alemães para a construção da máquina **Enigma**.



Fonte: https://pt.wikipedia.org/wiki/ROT13

Atualmente os modelos de cifragem fazem uso do mesmo princípio, porém com a introdução de chaves elaboradas matematicamente e sua sucessiva aplicação à informação por meio de algoritmos complexos. Neste processo as chaves são valores secretos que modificam a informação de um jeito determinado – o algoritmo – permitindo a ocultação da informação e também o seu acesso. Por isso a chave é compartilhada entre o emissor e o receptor no processo de comunicação.



Fonte: http://www.wikiwand.com/pt/Cifra_de_substitui%C3%A7%C3%A3o

Figura 1 - Cifragem com chave simétrica

Por outro lado, a **codificação** é a substituição de palavras ou elementos da comunicação com o propósito de dificultar a compreensão. Neste caso é necessário um conhecimento prévio do conteúdo e do contexto da informação. Exemplos de codificação são os conhecidos códigos: **Morse**, utilizado na telegrafia e rádio-comunicação em CW (*continuous wave)*, o **código fonético internacional**, utilizado no meio militar e na aviação e o **código Q**, bastante utilizado no radioamadorismo.

Veja no link a seguir um trecho do filme “Wildtalkers”, o qual aborda o uso do idioma dos índios Navajo pelas forças armadas norte-americanas no Pacífico durante a segunda guerra mundial.

https://www.youtube.com/watch?v=zQHhbhtpJ3M

Outro filme sobre o assunto e bastante interessante é “Breaking the Code”, de 1996, direção de Herbert Wise, que trata a biografia de Alan Turing, considerado o pai da computação, entenda o que isso tem a ver com criptografia lendo o texto que você encontra no link:

http://guiadoestudante.abril.com.br/aventuras-historia/conheca-vida-alan-turing-matematico-considerado-pai-computacao-688593.shtml

No material online você confere o fechamento deste tema pelo professor Luís!

TEMA 3: Algoritmos e sistemas criptográficos

Com o advento da computação eletrônica e a elevação da criptografia ao grau de ciência, passou- se a empregar modelos matemáticos para o estudo e o desenvolvimento de técnicas e modelos criptográficos. Muitos dos avanços nesse campo são devidos aos estudos e trabalhos de Alan Turing, John Von Neumman e Claude Shannon. Em razão disso foram desenvolvidos modelos e técnicas de criptografia, sobre os quais passamos a discorrer.

Os modelos mais comuns são os *message digest* ou resumos criptográficos, denominados **HASH**, pelos quais é possível criar um resumo capaz de representar uma grande quantidade de informação e validar sua integridade.

O *Hash* é um resumo criptográfico de comprimento padrão, gerado por funções matemáticas e tabelas de *hashing*. Veja alguns exemplos online de hash nos links a seguir.

https://www.tools4noobs.com/online_tools/hash/

http://onlinemd5.com/

O **MD-5** ou *Message Digest 5* é um algoritmo unidirecional de dispersão criptográfica, desenvolvido em 1991 por Ronald Rivest, da RSA Data Security, Inc., e muito usado em redes P2P como verificação de integridade de arquivos e *logins*. É importante ressaltar que o MD-5 constitui-se de uma função criptográfica, porém não realiza o processo de criptografia, pois não é possível recuperar a informação original a partir do HASH, mas somente validar ou comparar informações.

O **SHA** - *Secure Hash Algorithm* ou algoritmo de dispersão segura é uma função criptográfica criada pela NSA – *National Security Agency* e padronizado pelo NIST – *National Institute for Standard and Technology*.

Seu princípio de funcionamento é semelhante ao MD5, porém com melhor performance, o que o torna bastante usado, tendo passado por evoluções nas quais recebeu as seguintes denominações: SHA-0, SHA-1, SHA-2 e SHA-3. Alternativas a estas duas funções – MD e SHA são os algoritmos RIPMED-160 e Tiger.

Em ambiente de software livre e de código aberto destacam-se o **PGP** – *Pretty Good Privacy*, desenvolvido por Phil Zimmermann em 1991, que é muito empregado em segurança de comunicação por e-mail. O **GPG** - *GNU Privacy Guard*, desenvolvido em 1997 por Werner Koch, que oferece uma alternativa ao PG e utiliza a combinação de criptografia de chaves simétricas para melhorar o desempenho e também a criptografia de chaves públicas para a troca de mensagens seguras.

O **SSL** - *Secure Sockets Layer* e sua evolução, o **TLS** – *Transport layer Security*, compõem um protocolo de segurança para a comunicação de dados, como e-mails e navegação pela internet. Baseiam-se nos estudos de Diffie-Hellman (criptografia de chave pública) e de Phil Zimmermann (PGP). O **IPSec** – *IP Secutiry Protocol* é IPsec é, na verdade, um conjunto de funções e de protocolos que tem por finalidade prover a segurança no nível da camada IP para a troca de informações pela Internet. Ainda o **Free S/WAN** é uma das várias implementações do IPSec que possibilita a configuração de uma VPN entre redes distintas sobre a internet, possibilitando a comunicação segura.

Criptografia de chave pública assimétrica

A criptografia de chave assimétrica ou criptografia de chave pública assimétrica compõe-se de um **conjunto de técnicas e métodos criptográficos com base em algoritmos que exigem duas chaves**.

Uma destas chaves é a chave privada – de conhecimento reservado, e a outra chave é pública, que é divulgada aos interessados ou destinatários da comunicação.

Ambas têm a mesma origem, baseada em cálculos matemáticos de fatoração inteira de grandes números primos, logaritmos discretos e curva elíptica. A chave pública é distribuída para ser usada na criptografia de mensagem a ser enviada para o detentor da chave privada ou para validar uma assinatura digital encaminhada de/para ele.

A chave privada permite descriptografar a mensagem ou criar uma nova assinatura digital. Esta técnica é denominada assimétrica devido ao uso de chaves diferentes para as funções realizadas, opostas entre si. O processo todo é apresentado nas figuras a seguir. Acompanhe a primeira:

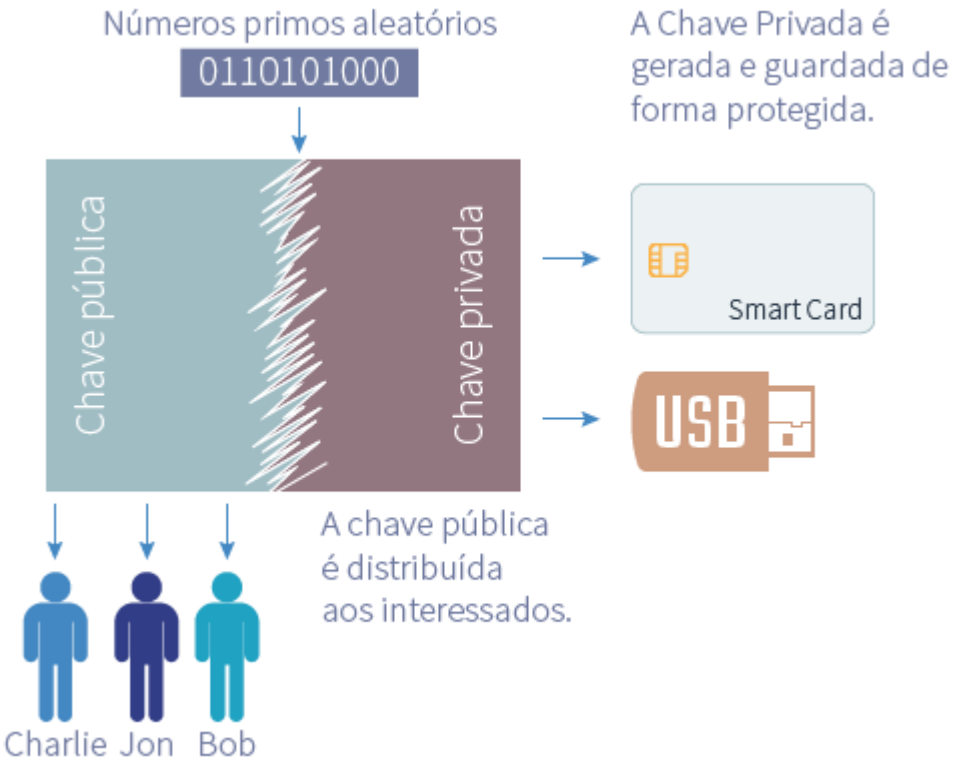


Figura 2 - Geração e distribuição de chaves assimétricas.

Do ponto de vista matemático e computacional é relativamente fácil gerar o par de chaves, sendo uma pública e uma privada.

Entretanto, é praticamente impossível do ponto de vista da capacidade computacional atual, determinar ou recuperar uma chave privada devidamente formada fazendo uso de uma chave pública. Desta forma, a chave pública pode ser disposta sem comprometer a segurança, sendo necessário proteger apenas a chave privada. Graças a isso esta técnica é usada para transferir uma chave de criptografia simétrica entre emissor e receptor, e assim possibilitar a criptografia e descriptografia da mensagem de forma bastante otimizada. Isto porque a criptografia simétrica utiliza algoritmos mais simples, o que a torna muito mais rápida. Veja a figura a seguir.

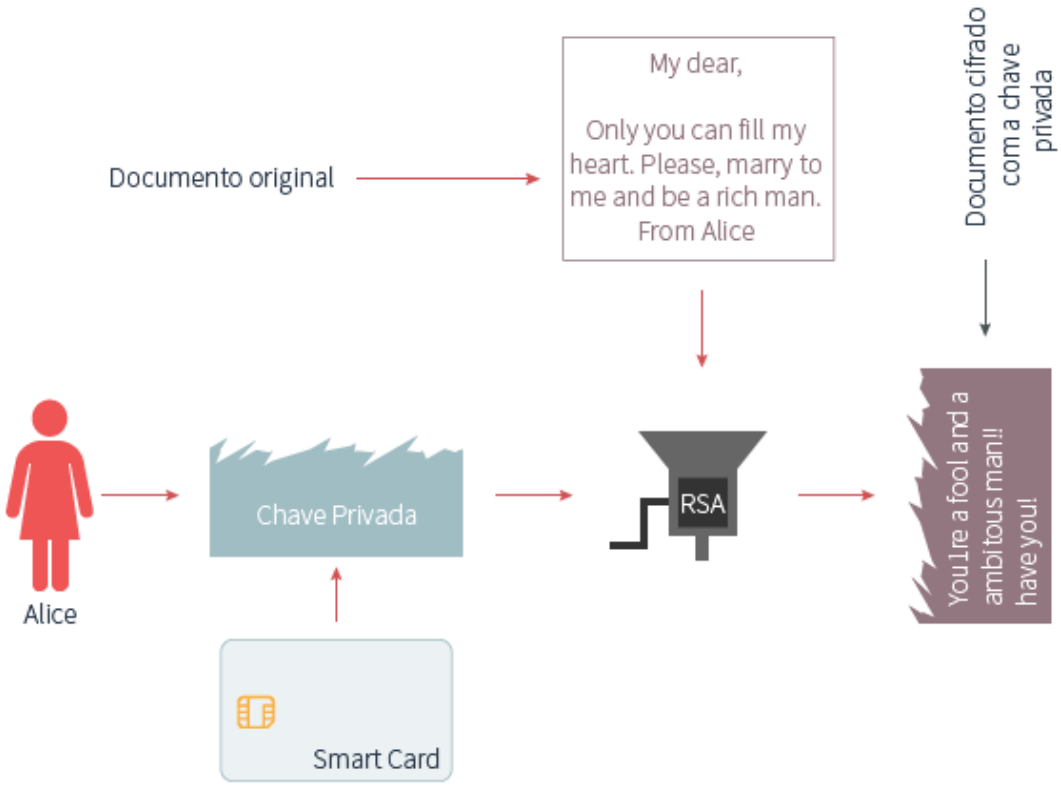


Figura 3 - Uso da Chave Privada para criptografar um documento

Entre os algoritmos de Chave Pública Assimétrica destacam-se o de Diffie-Hellman, algoritmo de troca de chaves desenvolvido por Whitfield Diffie e Martin Hellman em 1976, assim como o DSA - *Digital Signature Algorithm*.

O RSA, desenvolvido pelos professores do MIT Ronald Rivest, Adi Shamir e Leonard Adleman, fundadores da RSA Data Security, Inc., trouxe grandes inovações em criptografia de chave pública, além de possibilitar a criptografia e a assinatura digital.

Na criptografia assimétrica vista na tela anterior, se o Bob quer compartilhar informações com a Alice:

1) Alice compartilha sua chave pública com Bob.
2) Bob cifra a mensagem com a chave pública e envia para Alice.
3) Alice decifra a mensagem com a sua chave privada.
4) Se Alice quiser responder a Bob, usa sua privada para cifrar a resposta e enviar para Bob.
5) Bob usa a chave pública de Alice para decifrar a resposta.
6) Na criptografia assimétrica um par de chaves – pública/privada – é compartilhado e usado para cifrar e decifrar. Criptografia de chave única ou simétrica.

Diferente da criptografia assimétrica, a criptografia de chave única ou simétrica utiliza apenas uma chave para criptografar e descriptografar a mensagem. Portanto esta chave precisa ser muito bem guardada, e seu envio por um meio de comunicação representa um risco.

Os algoritmos utilizados para a criptografia simétrica apresentam desempenho muito superior, razão pela qual são preferidos em processos de criptografia de bloco e de fluxo. São exemplos deste tipo de algoritmo o **DES** – *Data Encryption Standard*, criado pela IBM em 1974, evoluindo depois para o **3-DES** ou *triple DES*. O algoritmo **RC4**, desenvolvido por Ronald Rivest, é utilizado no SSL e um dos mais empregados na criptografia de fluxo de dados. Já o **RC5**, do mesmo autor, é empregado para cifragem de blocos e de extrema facilidade. Ambos têm a chave de tamanho fixo. O **Blowfish** é um algoritmo de criptografia de blocos com chave de tamanho variável, desenvolvido em 1993 por Bruce Schneier, e seu código fonte é aberto e pode ser obtido na *internet.*

O **IDEA** - *International Data Encryption Algorithm* foi criado em 1991 por James Massey e Xuejia Lai. É também um algoritmo de bloco semelhante ao DES e de fácil implementação. O algoritmo **AES** - *Advanced Encryption Standard* ou Padrão de Criptografia Avançada é um algoritmo de criptografia de bloco padronizado pelo NIST em 2001 e usado pelo governo dos Estados Unidos em substituição ao DES/3-DES, sendo um dos mais populares algoritmos da atualidade, por combinar as características de segurança, desempenho, facilidade de implementação e flexibilidade.

Na criptografia simétrica, se Bob quer compartilhar informações com Alice:

1) Bob gera uma chave criptográfica e encaminha para Alice.
2) Bob cifra a mensagem com a chave gerada e envia para Alice.
3) Alice decifra a mensagem com a chave recebida.
4) Se Alice quiser responder a Bob, usa a mesma chave para cifrar a resposta e enviar para Bob.
5) A chave deve ser protegida tanto por que a usa quanto no processo de comunicação.

Assinatura Digital

A Assinatura Digital é um processo criptográfico para assegurar o não-repúdio da comunicação, isto é, **não permitir que o emissor negue que tenha encaminhado a informação recebida**. A Assinatura Digital é uma forma de garantir que o emissor da comunicação seja conhecido do destinatário. Além disso, é possível assegurar que o emissor da mensagem não possa negar, isto é, repudiar uma mensagem que enviou.

O processo consiste em assinar a mensagem com a chave privada do emissor, ou seja, gerar um *hash* com esta chave, e ao receptor permite acessar a mensagem com a chave pública do emissor, previamente recebida. Confira como isso funciona a seguir.

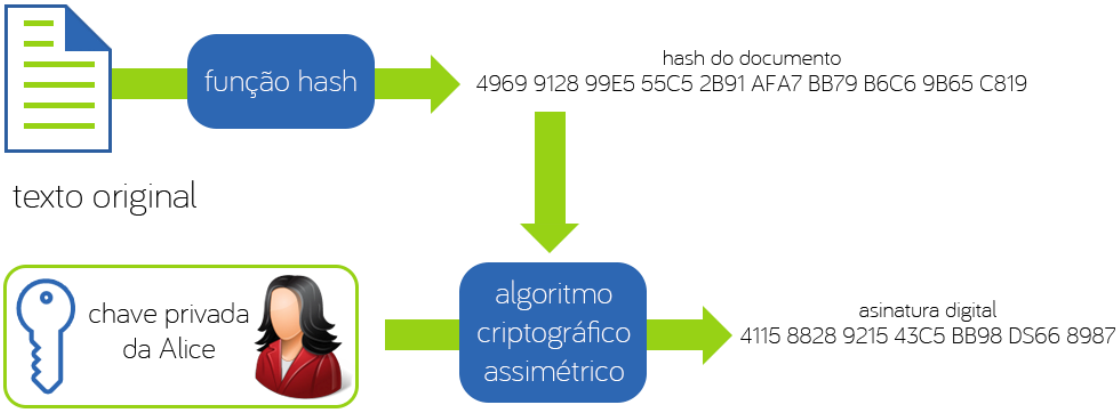


Figura 4 - Envio de mensagem assinada

Desta forma o receptor da mensagem pode confirmar que:

1) A mensagem foi enviada realmente por quem diz ser o emissor;
2) A mensagem não foi alterada no processo de comunicação.

O que você acabou de ver é garantido pelo processo de comparação dos *hashs* - recebido e gerado, como mostra a figura a seguir:

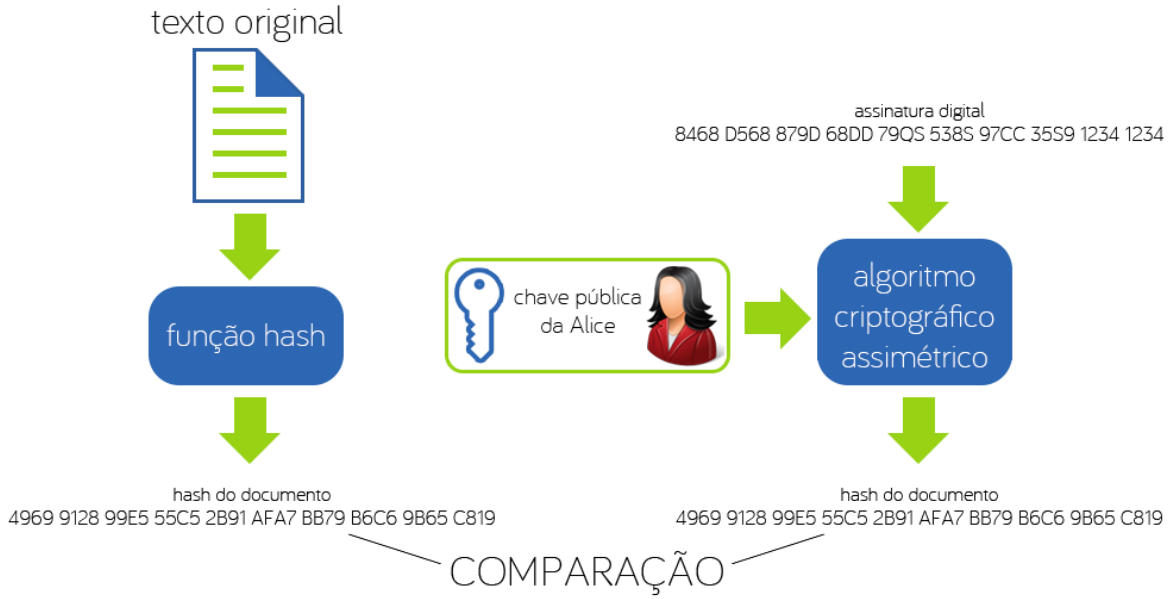


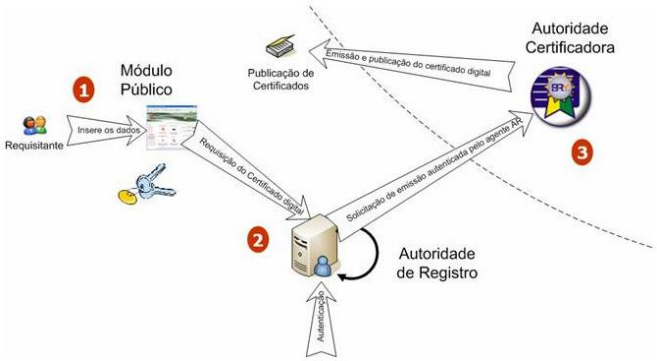
Figura 5 - Validação da mensagem recebida.

Certificado Digital

O Certificado Digital é um **documento no qual estão armazenados um conjunto de informações de uma organização, a empresa**, pessoa física ou computador, que é a entidade para a qual este certificado foi emitido por uma CA – *Certification Authority* ou Autoridade Certificadora. Neste documento está incluída a chave pública vinculada à chave privada, que deverá estar de posse somente da entidade especificada no certificado.

Modelos de Certificados Digitais do Brasil em Smart Card.

Um Certificado Digital é usado para ligar uma entidade a uma chave pública, por isso o certificado digital é assinado pela Autoridade Certificadora (AC) que o emitiu. Esta AC normalmente faz parte da ICP – Infraestrutura de Chaves Públicas, organismo responsável por gerir todo o sistema de certificação e normalmente ligado ao governo de um país. Tal como o reconhecimento de firma em um sistema de cartórios, as assinaturas digitais contidas em um certificado digital são atestadas emitidas por uma entidade certificadora, pelas quais essa AC afirma confiar nos dados contidos naquele certificado.



O processo de obtenção e validação de Certificados Digitais

Agora é com o professor Luís! Que nos explica um pouco mais sobre os algoritmos e mecanismos responsáveis pela criptografia, bem como os seus vários modelos no material online!

Trocando ideias

Na Biblioteca Virtual você tem acesso a dois títulos que poderão lhe acrescentar muito mais no que foi estudado até aqui: “Matemática discreta para ciência da computação” e “Criptografia e segurança de redes, 6ª edição”. Além do livro “Como Quebrar Códigos: a arte de explorar (e proteger) software”.

Acesse o **Ambiente Virtual de Aprendizagem (AVA)** e opine no fórum o que lhe chamou atenção no assunto estudado até aqui e discuta sobre isso. Compartilhando suas conclusões, esclarecendo as dúvidas e relatando as aplicações da criptografia no seu dia a dia e no mundo dos negócios.

Converse!

Na Prática

A criptografia tem um vasto uso na comunicação digital, está presente em quase todas as trocas de informação feitas deste modo e em especial nos negócios via internet. Contudo, ela não é o único recurso e nem mesmo o mais importante para a garantia da segurança da informação, pois o uso adequado e o desenvolvimento de funcionalidades criptográficas requer profundo conhecimento da matemática computacional. Mas a criptografia é uma das áreas da computação que mais tem exigido e recebido investimentos em termos de pesquisa e desenvolvimento.

Pesquise e identifique aplicações da criptografia que você utiliza em seu dia a dia, ou que estejam incluídas nos processos ou atividades dos quais você toma parte, depois e compare com o conteúdo que você aprendeu neste encontro.

Estamos chegando ao fim deste encontro! Veja o que o professor Luís tem a dizer no material online!

Síntese

Nesta aula discorremos sobre os conceitos e a aplicação da Criptografia nos sistemas computacionais e na comunicação digital. Apresentamos as características da cifragem e da codificação, bem como suas diferenças. Abordamos também os principais algoritmos e sistemas criptográficos, tais como os de criptografia simétrica, de criptografia assimétrica e de HASH, sua aplicação nos processos de assinatura digital e também de certificados digitais. É muito importante que você saia desta aula sem dúvidas, assim, se tiver sentido dificuldade em algum ponto, não hesite em retomar o conteúdo!

Foi bom estudar com você. Até uma próxima!

E não perca o vídeo de sintetização do professor Luís no material online!

Referências

- Stein, C., Drysdale R. L. e Bogart, K. **Matemática discreta para ciência da computação**. São Paulo: Pearson Education do Brasil, 2013.
- Stallings, William. **Criptografia e segurança de redes**, 6ª edição. São Paulo: Pearson Education do Brasil, 2015.
- Hoglund, G., McGraw, G. **Como Quebrar Códigos:** a arte de explorar (e proteger) software. São Paulo: Pearson Makron Boos, 2006.