TEMA 05
Criptografia

Habilidades:

- Entender a importância da criptografia para a segurança da informação.
- Aprender a elaborar o pensamento lógico e conhecer as principais cifras.
- Entender sistemas de defesa e resolução de falhas digitais e humanas.

A criptografia desempenha um papel importantíssimo na segurança digital, ao **proteger informações sensíveis contra acesso não autorizado e garantir a integridade e confidencialidade dos dados**. Envolve o uso de algoritmos matemáticos complexos para transformar os dados originais em uma forma ilegível, conhecida como texto cifrado.
Há dois principais tipos de criptografia utilizados na segurança digital: **criptografia simétrica e criptografia assimétrica**. Na criptografia simétrica, a mesma chave é usada tanto para criptografar quanto para descriptografar os dados, e exige que o emissor e o receptor compartilhem essa chave.
Já na criptografia assimétrica, são empregadas duas chaves diferentes: uma chave pública para criptografar os dados e uma chave privada correspondente para descriptografá-los. Isso permite uma comunicação segura entre duas partes, mesmo que nunca tenham se encontrado antes.
A criptografia desempenha um papel essencial em várias áreas da segurança digital. Por exemplo, é amplamente utilizada em transações financeiras online para proteger informações confidenciais, como números de cartão de crédito. Além disso, é fundamental para garantir a privacidade das comunicações, seja por e-mail, mensagens instantâneas ou chamadas de voz, o que impede que terceiros interceptem e compreendam as informações transmitidas. A criptografia também é usada em **redes privadas virtuais (VPNs)** para estabelecer conexões seguras em ambientes de rede não confiáveis.

História da Criptografia

A criptografia tem uma longa história, que remonta a milhares de anos. Desde os tempos antigos, as pessoas têm usado métodos de criptografia para proteger suas comunicações e informações confidenciais.
Uma das **primeiras formas de criptografia conhecidas é a cifra de César**, que era usada pelo imperador romano Júlio César. Nessa cifra, cada letra do alfabeto é substituída por outra que esteja três posições à frente no alfabeto. Essa técnica simples de substituição de letras foi usada para ocultar mensagens militares.
Outra forma de criptografia histórica é a **cifra de Vigenère**, desenvolvida no **século XVI** por Blaise de Vigenère. Essa cifra aplicava uma tabela de alfabetos deslocados, na qual a letra-chave determinava qual linha do alfabeto seria usada para cifrar cada letra da mensagem. A cifra de Vigenère era considerada muito segura na época e foi amplamente usada por séculos.
No entanto, o avanço significativo na criptografia ocorreu durante a Segunda Guerra Mundial, quando as máquinas de criptografia foram desenvolvidas. O exemplo mais famoso é a **máquina Enigma**, utilizada pelos alemães para criptografar suas comunicações militares. A equipe de criptoanalistas, liderada por Alan Turing, no projeto britânico chamado Ultra, conseguiu decifrar as mensagens da Enigma, o que foi essencial ao esforço de guerra dos Aliados.
Após a Segunda Guerra Mundial, a criptografia evoluiu rapidamente com o **advento da criptografia de chave pública.** Em 1976, Whitfield Diffie e Martin Hellman propuseram o conceito de criptografia assimétrica, em que duas chaves diferentes são usadas para criptografar e descriptografar dados. Essa abordagem inovadora possibilitou um novo nível de segurança e facilitou a troca de chaves em comunicações seguras.
Nos últimos anos, a criptografia desempenha um papel fundamental na segurança digital,

especialmente, com o crescimento da internet e comunicações eletrônicas. Sem contar que o desenvolvimento da **criptografia de curva elíptica (ECC)** e a ascensão das criptomoedas, como o Bitcoin, trouxeram novas aplicações e desafios à criptografia.
Em resumo, a história da criptografia mostra a evolução das técnicas e algoritmos ao longo dos séculos, impulsionada pela necessidade de proteger informações confidenciais. Desde as cifras antigas até a criptografia moderna, essa disciplina tem sido essencial para garantir a segurança das comunicações e a proteção dos dados em várias áreas da sociedade.

Conceitos

Os métodos para transformar e retomar a informação ao original, respectivamente, são denominamos de **encriptação** e **decriptação**, e podemos dividir os ativos de informação que passarão pelo processo de criptografia em três tipos. São eles:

Texto Claro - consiste no dado ou informação, o qual qualquer pessoa consegue compreender.
Texto Cifrado – o qual o dado ou informação que passou pelo processo de cifragem, e foi convertido a um texto não legível.
Texto Decifrado – dado ou informação que foi convertido novamente em texto claro.

Cifra

É um dos termos mais populares quando o assunto é criptografia. **A cifra** é um conjunto de algoritmos (técnicas e ações) responsáveis pela codificação ou decodificação de uma mensagem.
Esta, por sua vez, normalmente envolve o embaralhamento das letras ou palavras do conteúdo da mensagem principal, e este processo pode ser revertido pela pessoa que tem o conhecimento da cifra utilizada.

Contexto Histórico

Por mais que este termo esteja em destaque, a criptografia definitivamente não é algo novo.
Desde a Antiguidade, os seres humanos já viam a necessidade de compartilhar informações com mais privacidade. Podemos separar os períodos de métodos criptográficos de acordo com sua evolução durante o tempo. São eles a **criptografia clássica** e a **criptografia moderna**.

Criptografia clássica

Em tempos mais remotos, os mensageiros percorriam longas distâncias com o objetivo de transmitir a mensagem que lhes foi confiada. Ocorria que, por muitas vezes, eles eram alvos de pessoas mal-intencionadas no meio do caminho, no intuito de roubar, adulterar ou até mesmo destruir a mensagem a ser entregue. Dessa forma, o homem começou a planejar estratégias que impedissem que essas mensagens aparecessem claras ao atacante e, até mesmo, para o mensageiro, tornando-as inúteis a ele sem a chave para quebrar o enigma que envolvia o processo. Uma das criptografias mais antigas e, também, mais populares, sem dúvidas é a **Cifra de César**.

Cifra de César

A Cifra de César foi um método extremamente usado pelo exército romano para decodificar mensagens e compartilhar informações com a infantaria e generais. O processo é o seguinte: Cada letra que for escrita deve ser substituída pela 3° letra posterior. Por exemplo, a letra “A”, seria substituída pela letra “D”.

Veja abaixo uma tabela que mostra o alfabeto e as letras já alteradas pela cifra.

Alfabeto normal:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Alfabeto cifrado:
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Ao utilizarmos a Cifra de César para criptografar uma frase, ficará desta forma:

"EU ESTUDO NA ESCOLA TECNICA" – Texto claro.
"HX HVWXGR QD HVFROD WHFQLFD" – Texto criptografado pela Cifra de César.
"EU ESTUDO NA ESCOLA TECNICA" – Texto Decifrado.

As letras do alfabeto são equiparadas de acordo com a sua posição na ordem alfabética. O valor da letra "A" é D, o valor da letra "B" é E, e assim por diante. Isso significa que a letra "Z" tem o valor 26.Quando a tabela chega à última letra "Z", ela retorna à letra "A" e continua seguindo a sequência alfabética.
Com o passar do tempo e o surgimento das tecnologias de maquinários eletromecânicos, os métodos de criptografia cresceram junto, e tornaram-se cada vez mais competentes e difíceis de serem decifrados. No século XX e, mais precisamente, na Segunda Guerra Mundial, aumentou mais ainda a popularidade dos métodos de criptografia, já que houve um alto investimento em tecnologia neste período.
Uma das ferramentas mais utilizadas pelo exército alemão, sem dúvidas, foi a máquina comumente chamada de Enigma.

Enigma

Definitivamente o maior desafio de encriptação naquela época, a Enigma era uma máquina capaz de criptografar e descriptografar informações através de seus **rotores eletromecânicos**. Foi desenvolvida pelo holandês Hugo Alexander Koch e aprimorada por Ritter e Scherbius.
A Enigma se assemelhava a uma máquina de escrever, porém, não era todo mundo capaz de operá-la. O técnico deveria ser cauteloso ao manuseá-la, já que era necessário alterar sua chave todos os dias e ser configurada exatamente de acordo com os manuais. O rotor no seu interior armazenava a mensagem anteriormente digitada em seu teclado, depois, outra pessoa deveria selecionar quais luzes iriam acender caso alguma tecla seja pressionada.
Posteriormente, na era da Computação, já com toda sua bagagem milenar, inicia-se o período da Criptografia Moderna.

https://www.youtube.com/watch?v=rID250fN1Mk

Criptografia Moderna

Com o surgimento dos computadores e sua ampla acessibilidade, a criptografia passa a ser utilizada para fins cotidianos, e **deixa de ser de uso exclusivo para militares ou de cunho governamental**.
A criptografia é hoje o **braço direito da S.I.**, sendo a ferramenta principal contra o vazamento dos ativos de informação, o que contribuiu ao impedimento de fraudes e demais usos inapropriados.
É aplicável desde para **proteger uma troca de mensagens até mesmo a transações que envolva criptomoedas**.
Partindo agora para este contexto do Cyber Security, a criptografia é aplicada praticamente em todos os ambientes informáticos, tanto empresariais, quanto em nossas casas, navegando pela internet e respondendo e-mails. Veja **abaixo alguns exemplos em que a criptografia é aplicada atualmente**:

Criptografia SSL (Secure Sockets Layer – Camada de Soquete Seguro)

É um **protocolo de criptografia utilizado em certificados digitais** (chamado de Certificado SSL) de um site publicado na Web e cria uma conexão entre o servidor que comporta a aplicação e o navegador de internet. Ele criptografa os dados compartilhados pelo usuário e serviço por meio de algoritmos, o *que impede que agentes mal-intencionados em potencial tentam interceptar a comunicação*.

HTTP + SSL = HTTPS

Assinaturas digitais

As assinaturas digitais são **encarregadas por autenticar que uma pessoa está assinando de maneira virtual um documento**, o que possibilita que arquivos críticos e demais contratos possam ser reconhecidos juridicamente, sem a necessidade da assinatura ser física em um papel. Por estarem relacionados a uma identidade real, a *criptografia está presente para legitimar que a pessoa realmente deseja assinar o documento e visa proteger os dados e informações contidas nessa assinatura*, o que dificulta que ela sofra alterações e fraudes.

Aplicativos de troca de mensagens

Os *apps* mensageiros mais utilizados no Brasil não poderiam ficar de fora. O **Whatsapp e Telegram**, por exemplo, usam um método de **criptografia chamado de "ponta a ponta"**. *Este codifica a mensagem antes de enviá-la. Assim que a mensagem chega ao destinatário, é decifrada e libera a leitura*. A **mensagem só pode ser decifrada e lida por este destinatário**.

VPN

As **VPN's (*Virtual Private Network*)** são conexões de rede privadas criadas a partir de redes públicas com o intuito de aprimorar a segurança. *A criptografia entra codificando o tráfego de internet do usuário, aumentando sua privacidade enquanto navega*.

Métodos de Criptografia

Existem **três tipos de criptografia**, sendo que dois deles se baseiam pelas **chaves**. As chaves são os métodos específicos dos algoritmos utilizados para realizar o embaralhamento e a resolução.

São elas:

1) Funções *Hash*

A criptografia do tipo *Hash* emprega algoritmos matemáticos que realizam a função de transformar o dado ou informação em um conjunto de caracteres alfanuméricos de comprimento fixo, e resume consideravelmente seu tamanho. É **mais utilizado em métodos de autenticação por possuir alta complexidade**.

Veja abaixo três dos algoritmos *Hash* mais utilizados mundialmente:

- MD (*Message Digest*) – É o algoritmo responsável por checar a integridade dos dados. A mais comum é a MD5, que trabalha com 128 bits. Porém, nos dias atuais, não é mais utilizado para criptografia, pois apresenta muitas vulnerabilidades para este fim.
- RIPEMD – É considerado a evolução do MD, isso porque apresenta uma quantidade de bits maior (160).
- SHA (*Secure Hash Algorithms*) – Função criptográfica encarregada por mediar a transmissão de dados e informações entre um servidor de aplicações e um cliente.

* SHA é usado para assegurar que os dados não foram alterados durante a transmissão, oferecendo um mecanismo robusto para verificar a integridade e autenticidade das informações transmitidas entre um servidor e um cliente.

2) Chave Simétrica/Privada

A chave simétrica usa apenas uma chave para criptografar e descriptografar um dado ou informação dentro do algoritmo, e apresenta uma cadeia de bits proprietária.
Possui um bom desempenho, no entanto, precisa-se substituir a chave caso ocorra alguma implicação, já que tanto o remetente, quanto o destinatário da transmissão usam a mesma chave, além de não possuir uma maneira de autenticar as pessoas envolvidas. Por isso, não é uma alternativa recomendada nos dias de hoje para encriptação de informações críticas.

DES

O algoritmo de encriptação simétrico do tipo DES (*Data Encryption Standard*), foi um dos primeiros a serem incluídos na programação de modo geral e instituído nos anos 70. Ele trabalha com uma chave de apenas 56 bits, atualmente, **é considerado inseguro, isso porque é facilmente quebrado**.

AES

AES (*Advanced Encryption Standard*) foi uma evolução perante o DES, uma vez que permite a escolha do tamanho da chave. Esta poderia ser de 128, 192 e 256 bits, muito além dos anteriores 56 do DES.

3) Chave Assimétrica/Pública

No método de chave assimétrica, a criptografia utiliza duas chaves diferentes: uma pública e outra privada. A **chave pública se destina a criptografar a informação** e a **privada decodificar**. Não há necessidade do emissor da mensagem compartilhar e/ou distribuir outras chaves para que o destinatário consiga abrir. Este é o tipo de criptografia mais complexo, porém é o mais seguro e utilizado atualmente.

RSA

O RSA (**R**ivest, **S**hamir, **A**ndleman) é uma das referências de chave assimétrica, pois é extremamente poderosa. **Funciona com a multiplicação de dois números primos para gerar as chaves privadas e públicas.** Como resultado, é elaborado um número extenso que dificulta imensamente o processo de decifragem por algum agente externo.

Diffie-Hellman

Este tipo de criptografia assimétrica foi criado por **Whitfield Diffie e Martin Hellman**, baseado na confiança da **troca de chaves entre o emissor e destinatário de maneira não tradicional**, ou seja, ambos sabem a estrutura das chaves.

RESUMO

A criptografia é uma ferramenta essencial à segurança da informação. Funcionando como uma camada protetora contra invasões, codifica dados para que sejam compreendidos apenas por quem possui a chave de decodificação. Desta maneira, é possível prevenir a violação da privacidade, fraudes e outros tipos de ataques cibernéticos, o que torna-se fundamental em um mundo cada vez mais digital e interconectado.A elaboração do pensamento lógico é uma habilidade vital para compreender e utilizar criptografia, e envolve a capacidade de pensar de maneira estruturada e racional para resolver problemas complexos. As cifras são um componente central da criptografia, que abrange técnicas de codificação e decodificação. Além disso, a compreensão dos sistemas de defesa e de como resolver falhas, tanto digitais quanto humanas, é básica para manter a segurança

da informação. Esse conhecimento possibilita identificar vulnerabilidades, desenvolver estratégias de proteção eficazes e, em caso de falhas, aplicar soluções apropriadas para minimizar danos e restabelecer a segurança.

ATIVIDADES

1. O que é criptografia?
2. Qual é a finalidade da criptografia na segurança da informação?
3. Cite um exemplo de uso comum da criptografia no cotidiano.
4. Explique a diferença entre criptografia simétrica e criptografia assimétrica. Quais são as vantagens e desvantagens de cada abordagem?
5. Descreva o que é uma chave de criptografia e por que é importante para garantir a segurança dos dados criptografados.

GLOSSÁRIO:

ECC:

A criptografia de curva elíptica (ECC, do inglês Elliptic Curve Cryptography) é um método de criptografia baseado na matemática das curvas elípticas. Este tipo de criptografia utiliza as propriedades dos pontos sobre uma curva elíptica para criar chaves criptográficas. Aqui estão os principais pontos sobre ECC:

1. Definição e Fundamentos Matemáticos:

- ECC usa equações algébricas de curvas elípticas sobre campos finitos.
- A equação típica de uma curva elíptica é $y^2 = x^3 + ax + b$, onde a e b são constantes que definem a forma da curva.

2. Chaves Menores e Segurança:

- ECC pode fornecer o mesmo nível de segurança que outros sistemas de criptografia (como RSA) usando chaves de tamanho muito menor.
- Por exemplo, uma chave de 256 bits no ECC oferece uma segurança comparável a uma chave de 3072 bits no RSA.

3. Eficiência:

- Devido ao uso de chaves menores, ECC requer menos poder de processamento e recursos computacionais, tornando-o ideal para dispositivos com recursos limitados, como smartphones e dispositivos IoT.

4. Aplicações:

- ECC é amplamente usado em vários protocolos de segurança, incluindo SSL/TLS para a segurança das comunicações na internet, e na criptografia de chaves para criptomoedas como o Bitcoin.

5. Vantagens:

- **Desempenho**: ECC é mais rápido e eficiente em termos de uso de recursos.
- **Segurança**: Oferece alta segurança com chaves menores.
- **Escalabilidade**: Adequado para uma ampla gama de dispositivos, especialmente aqueles com limitações de recursos.

6. Implementação:

- ECC é implementado em vários padrões e protocolos de criptografia, incluindo ECDSA (Elliptic Curve Digital Signature Algorithm) para assinaturas digitais, ECDH (Elliptic-curve Diffie–Hellman) para troca de chaves seguras, e outras variantes.

Resumo:
A criptografia de curva elíptica (ECC) é uma forma avançada de criptografia que utiliza as propriedades matemáticas das curvas elípticas para criar chaves criptográficas. É altamente eficiente e segura, oferecendo os mesmos níveis de segurança que outros métodos tradicionais, mas com chaves menores, o que a torna ideal para aplicações modernas e dispositivos com recursos limitados.

COMPARATIVO
Aqui está uma tabela comparativa entre os diferentes tipos de criptografia mencionados, incluindo segurança e desempenho. Além disso, mencionarei outros métodos de criptografia que são considerados seguros atualmente e que não foram listados no texto.

Tipo de Criptografia	Algoritmo	Segurança	Desempenho	Notas
Funções Hash	MD5	Baixa	Alta	Vulnerável a ataques de colisão; não recomendado para segurança crítica.
	RIPEMD-160	Moderada	Moderada	Mais seguro que MD5, mas menos popular que SHA-256.
	SHA-256	Alta	Moderada	Muito usado para verificar integridade e autenticidade de dados.
	SHA-3	Alta	Moderada	Mais recente, alternativa ao SHA-2, oferece segurança robusta.
	Bcrypt	Alta	Baixa	Usado para hashing de senhas, inclui um fator de custo ajustável para aumentar a segurança.
	Argon2	Muito Alta	Baixa	Vencedor do PHC (Password Hashing Competition), muito seguro para hashing de senhas.
Chave Simétrica	DES	Baixa	Alta	Obsoleto, facilmente quebrado; não recomendado.
	AES-128	Alta	Muito Alta	Muito usado, seguro e eficiente.
	AES-256	Muito Alta	Alta	Muito usado, mais seguro que AES-128, mas com desempenho um pouco menor.
Chave Assimétrica	RSA	Alta	Baixa	Amplamente usado, seguro, mas lento; ideal para troca de chaves e assinatura digital.

	Diffie-Hellman	Alta	Moderada	Usado para troca de chaves segura; requer implementação cuidadosa.
	ECC (Curve25519)	Muito Alta	Alta	Baseado em criptografia de curva elíptica; oferece alta segurança com chaves menores.

Outros Métodos de Criptografia

1. Elliptic Curve Cryptography (ECC):
- **Segurança:** Muito Alta
- **Desempenho:** Alta
- **Notas:** Usa curvas elípticas para fornecer segurança equivalente ao RSA com chaves menores e maior eficiência. Exemplos incluem Curve25519 e P-256.

2. ChaCha20:
- **Segurança:** Alta
- **Desempenho:** Muito Alta
- **Notas:** Alternativa ao AES para criptografia simétrica, especialmente em dispositivos com recursos limitados. Usado no protocolo TLS.

Resumo

- **Funções Hash:** SHA-256 e SHA-3 são atualmente as mais seguras e amplamente utilizadas para garantir a integridade dos dados.
- **Chave Simétrica:** AES-256 é uma escolha sólida para segurança e desempenho, superando o DES.
- **Chave Assimétrica:** RSA e ECC são os métodos mais seguros para criptografia de chave pública, com ECC sendo mais eficiente.

Para garantir a máxima segurança, especialmente em novas implementações, recomenda-se o uso de algoritmos modernos como SHA-3, AES-256, e ECC.