<< DE ENIGMAS ANTIGOS A ALGORITMOS MODERNOS: A EVOLUÇÃO DA CRIPTOGRAFIA >>

Nome do Autor(es)
LUIZA MENDES SOUZA
MYCKAEL PEDRO DA SILVA SANTOS
OTAVIO DOS SANTOS SILVA

Nome do Orientador(es)
HUMBERTO ALVES DUTRA

Instituição de Ensino
E.E. PEI Prof° Plínio Paulo Braga

1. Resumo

O projeto *"De Enigmas Antigos a Algoritmos Modernos: A Evolução da Criptografia"* explora a trajetória histórica e tecnológica da criptografia, desde seus métodos rudimentares na antiguidade até as soluções avançadas dos dias atuais. Começamos abordando a origem da criptografia, destacando técnicas como a cifra de César e a famosa máquina Enigma, usadas em tempos de guerra. Em seguida, o projeto explora conceitos de criptografia simétrica e assimétrica, além de discutir as inovações na criptografia quântica e blockchain, ambas essenciais para a segurança digital contemporânea. Também são abordados os avanços na criptografia biométrica, uma tecnologia emergente que promete redefinir a proteção de dados. Através de uma reflexão sobre um cenário sem criptografia, o projeto demonstra os potenciais riscos para a privacidade e a segurança dos dados pessoais, seja em redes sociais, transações financeiras ou comunicações digitais. Por fim, relacionamos os estudos com o **ODS 16 – Paz, Justiça e Instituições Eficazes**, destacando a relevância da criptografia para a promoção de sociedades seguras e justas, onde a privacidade e a proteção da informação são fundamentais para o bem-estar de todos. Concluímos que compreender a evolução da criptografia e suas aplicações é essencial para conscientizar a sociedade sobre a importância de proteger informações no ambiente digital. Dessa forma, o projeto busca não apenas ilustrar a história e a tecnologia por trás da criptografia, mas também incentivar um uso mais seguro e responsável das ferramentas digitais, promovendo a construção de um espaço virtual mais seguro para todos.

Palavras-chave: Criptografia. Blockchain. Segurança Digital. Criptografia Biométrica.

2.Introdução

Imagine um mundo onde suas mensagens privadas, transações bancárias e até suas conversas nas redes sociais estivessem expostas a qualquer um. Sem códigos secretos, sem barreiras de proteção. Um cenário caótico onde a privacidade seria uma ilusão e a segurança digital, uma ideia distante. O que impede que isso aconteça? A criptografia.

Desde a antiguidade, a humanidade tem buscado maneiras de ocultar suas informações mais valiosas. De mensagens escondidas por generais em tempos de guerra até os complexos sistemas digitais que usamos todos os dias, a criptografia sempre foi a linha de defesa entre o público e o privado. Mas o que poucos percebem é que, hoje, ela é a única coisa que separa nossos dados pessoais de cair nas mãos erradas.

Neste projeto, vamos explorar os enigmas do passado, como a cifra de César, e avançar até as tecnologias de ponta, como a criptografia quântica. Descobriremos como simples códigos mudaram o curso de guerras, e como, nos dias atuais, algoritmos invisíveis mantêm seguras as informações que compartilhamos a cada clique. Será possível imaginar um mundo sem criptografia? E se isso acontecesse, o quão vulneráveis estaríamos?

Prepare-se para uma viagem fascinante pela história e pelos bastidores da segurança digital, onde cada código revela uma história e cada descoberta nos lembra da importância de manter nossos segredos bem guardados.

3.Objetivo

Explicar a evolução histórica da criptografia — Mostrar como os métodos de criptografia evoluíram desde a antiguidade até os tempos modernos, abordando desde a Cifra de César e a Máquina Enigma até a criptografia simétrica, assimétrica, a criptografia quântica e a Biometria.

Demonstrar a importância da criptografia no dia a dia — Apresentar como a criptografia está presente nas nossas atividades cotidianas, como conversas online, transações bancárias e até na proteção das redes sociais, destacando como ela impacta a segurança dos alunos e de suas famílias.

Conscientizar sobre os riscos de um mundo sem criptografia — Explicar como seria um mundo sem criptografia e quais seriam os impactos na privacidade, segurança e exposição a crimes cibernéticos.

Propor práticas para aumentar a segurança digital — Mostrar estratégias e medidas simples que todos podem adotar para proteger melhor suas informações online, como uso de senhas fortes, autenticação de dois fatores e estar atento a possíveis golpes.

Relacionar o estudo da criptografia com o ODS 16 – *Paz, Justiça e Instituições Eficazes*, enfatizando o papel da criptografia na promoção de sociedades pacíficas e inclusivas, garantindo segurança, justiça e proteção de dados pessoais.

4.Metodologia

4.1.Materiais:

Computadores e Internet: Usados para pesquisar informações e criar apresentações.

Slides e Vídeos: Para ajudar a explicar a criptografia de forma simples.

4.2.Métodos:

Pesquisa na Internet: Encontrar informações sobre a história da criptografia e como ela é usada hoje.

Criação de Atividades: Fazer jogos e programas (Através da linguagem de programação Scratch) que ajudem a entender como a criptografia funciona.

4.3Procedimentos:

Montar a Equipe: Escolher os alunos que vão ajudar no projeto.

Pesquisar e Estudar: Coletar informações sobre criptografia e criar as atividades.

Criar e Testar: Desenvolver e testar os jogos e programas.

Fazer as Aulas: Apresentar o conteúdo para os colegas.

Coletar Feedback: Perguntar o que os alunos acharam e ver o que aprenderam.

Escrever o Relatório: Resumir o que foi feito e o que aprendemos com o projeto.

5.Desenvolvimento

O projeto sobre a evolução da criptografia começou porque queríamos mostrar para os jovens como a criptografia, que é usada para proteger informações, mudou com o tempo. Vamos falar desde os códigos antigos até as tecnologias modernas que mantêm nossos dados seguros hoje em dia.

Primeiro, montamos uma equipe com os alunos que estão a fim de estudar o assunto. Conversamos sobre as principais ideias e decidimos que iríamos explorar a história da criptografia, incluindo coisas legais como a Cifra de César e a Máquina Enigma, além de explicar conceitos mais modernos, como criptografia simétrica e assimétrica, blockchain e criptografia biométrica.

A apresentação vai ser dividida em três partes.

5.1 Parte Histórica.

A criptografia (que vem do grego 'kryptos', que significa escondido, e 'graphein', que significa escrita) é o estudo de técnicas para esconder informações. A primeira vez que sabemos que usaram criptografia foi no Egito, há cerca de 4.000 anos, e depois na Mesopotâmia, Grécia e Roma.

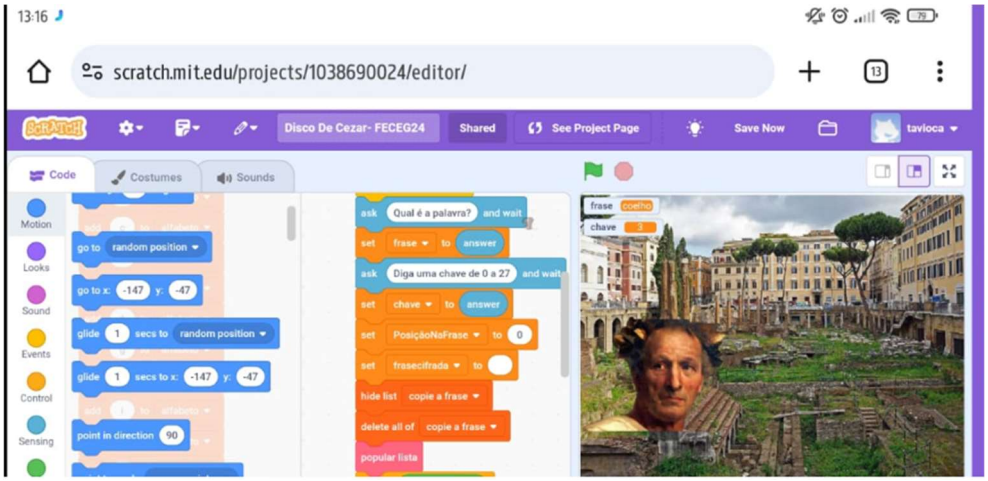
Um dos primeiros métodos de criptografia que conhecemos é a Cifra de César. Ela foi criada cerca de um século antes de Cristo, e Júlio César usou esse tipo de criptografia para mandar mensagens secretas para seus generais durante a guerra. Esse método é chamado de Cifra de Substituição, onde cada letra do texto original é trocada por outra letra, formando um texto cifrado. Por exemplo, A vira D, B vira E, C vira F – isso significa que estamos mudando as letras 3 posições para frente na cifra de César.

Figura 1 – Representação do disco de César.

Fonte: https://mylinuxbr.wordpress.com/wp-content/uploads/2016/10/logo.jpg

Para deixar a apresentação mais legal, os alunos usaram a plataforma Scratch para criar um programa que simula como codificar palavras. O programa muda as letras de acordo com a quantidade de posições que a gente escolhe, fazendo com que a palavra pareça não ter sentido.

Figura 2. Imagem da tela de Programação do Scratch.



Fonte Própria.

Em 1918, a Máquina Enigma foi criada pelo engenheiro alemão Arthur Scheribus. Na Segunda Guerra Mundial, foi usado regularmente pelos militares alemães nazistas.

Figura 3 – Máquina Enigma

Fonte: https://s1.static.brasilescola.uol.com.br/be/conteudo/images/c17da4f5560cfc61c4d5625a5dd27ca2.jpg

A máquina usava três ou mais rotores para embaralhar o alfabeto de 26 letras, girando em diferentes velocidades e gerando texto cifrado. A Máquina Enigma acabou sendo quebrada pela Polônia, o que levou os britânicos a criar o Bombe, um dispositivo que ajudava a identificar a ordem das rodas da máquina Enigma e as configurações iniciais dos rotores.

5.2 A criptografia no pós Guerra

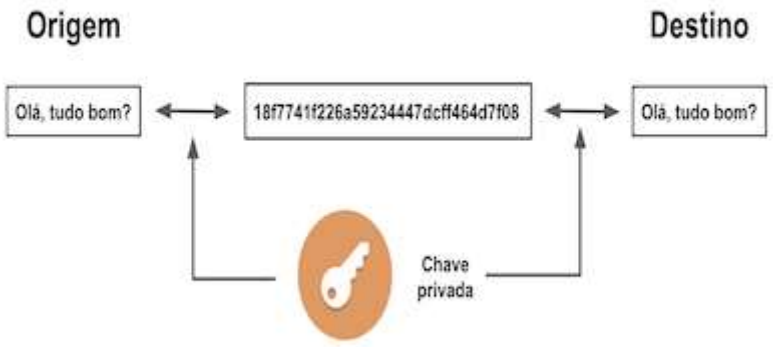
O uso de criptografia até este ponto foi usado principalmente para fins de guerra. No entanto, isso mudou quando as empresas viram o potencial comercial da criptografia para proteger os dados dos concorrentes.

Criptografia Simétrica

Nos anos 1970, a IBM percebeu que seus clientes precisavam de mais segurança para proteger seus dados e criou uma cifra chamada Lúcifer. Em 1973, o governo dos EUA

procurava um padrão de criptografia mais seguro, pois muitos produtos não protegiam bem as informações. A cifra Lúcifer foi escolhida, renomeada para DES (Data Encryption Standard) e se tornou um padrão nacional. Porém, em 1997, o DES começou a falhar, pois a chave usada para criptografar era muito curta, facilitando ataques que testavam todas as combinações possíveis. Então, o NIST propôs a criação de um novo padrão e, após receber várias propostas, escolheu a cifra Rijndael, que passou a se chamar AES (Advanced Encryption Standard). Com uma chave mais segura, o AES se tornou o padrão mundial de criptografia simétrica, utilizado até hoje para proteger dados em redes e dispositivos digitais.

Figura 4: Esquema representativo para a criptografia simétrica.



Fonte: https://www.universidadejava.com.br/images/2020-05-22-teaser-criptografia-simetrica.png

Criptografia Assimétrica

Em 1976, os pesquisadores Diffie e Hellman revolucionaram a criptografia ao criar a criptografia assimétrica, também conhecida como criptografia de chave pública. Nesse método, são usadas duas chaves diferentes: uma pública, que pode ser compartilhada com qualquer pessoa, e uma privada, que deve ser mantida em segredo. O interessante é que, se você criptografar uma mensagem com uma dessas chaves, apenas a outra chave poderá decifrá-la.

Por ser mais lenta e complexa, a criptografia assimétrica não substitui a criptografia simétrica. Em vez disso, é usada para enviar as chaves simétricas com segurança, que são mais rápidas para criptografar mensagens grandes. Funciona assim: primeiro, quem envia a mensagem cria uma chave simétrica e a criptografa com a chave pública do destinatário. Assim, apenas a pessoa com a chave privada correspondente poderá decifrar e acessar a chave simétrica para começar a troca de mensagens.

Em 1977, três pesquisadores chamados Rivest, Shamir e Adleman criaram um dos algoritmos mais famosos de criptografia assimétrica, chamado RSA. Esse método usa chaves de tamanhos variados (de 512 até 2048 bits) e é muito seguro. Hoje, a criptografia assimétrica é usada em muitos sistemas, como para garantir a segurança de e-mails, transações bancárias e sites na internet.

Figura 5: Esquema representativo para a criptografia assimétrica.

Fonte: https://www.researchgate.net/profile/Arthur-Teodoro/publication/332948161/figure/fig5/AS:756324753211396@1557333281925/Figura-7-Esquema-da-criptografia-assimetrica.ppm

Criptografia quântica

A criptografia quântica foi pensada pela primeira vez em 1984 por dois pesquisadores chamados Charles Henry Bennett e Gilles Brassard. Diferente da criptografia tradicional, que usa matemática para proteger informações, a criptografia quântica utiliza as leis da física. Ela se baseia em princípios da mecânica quântica para garantir a segurança das comunicações de uma forma que, teoricamente, é praticamente impossível de ser quebrada.

Apesar de ser muito segura, ainda é difícil usar a criptografia quântica em larga escala. Mas ela tem um grande potencial para proteger informações sensíveis, como dados financeiros ou segredos de governos. Em 1994, um matemático chamado Peter Shor mostrou que os computadores quânticos poderiam quebrar rapidamente os sistemas de criptografia que usamos hoje, descobrindo senhas complexas em minutos. Isso é um problema, porque computadores comuns levariam anos para fazer o mesmo.

Embora, no passado, a ideia de computadores quânticos parecesse algo distante, hoje os cientistas acreditam que, em 20 a 50 anos, esses computadores vão se tornar reais. Isso mudaria completamente a forma como protegemos nossos dados, tornando muitos métodos de segurança obsoletos. Por isso, precisamos desenvolver novos tipos de criptografia que possam resistir a essas máquinas superpoderosas e manter nossas informações seguras no futuro.

Blockchain.

O blockchain foi criado em 1991 por Stuart Haber e W. Scott Stornetta para garantir que documentos digitais tivessem marcas de tempo seguras e que ninguém pudesse alterá-los depois. No entanto, o blockchain só ficou famoso em 2008, quando alguém usando o nome Satoshi Nakamoto criou o Bitcoin e usou o blockchain para registrar todas as suas transações.

Basicamente, o blockchain é como um banco de dados, mas com uma diferença importante: não é controlado por uma única pessoa ou empresa. Isso significa que ele é descentralizado e mais seguro. As informações são organizadas em "blocos" que formam uma cadeia. Cada bloco tem dados de transações, uma marca de tempo e um código único (chamado de hash) que o liga ao bloco anterior. Isso impede que os dados sejam alterados, porque, se

alguém tentar mudar um bloco, teria que alterar todos os blocos seguintes, o que é praticamente impossível.

No início, o blockchain era usado apenas para registrar as transações do Bitcoin, mas hoje ele é aplicado em várias áreas, como contratos digitais, sistemas de votação e até mesmo para rastrear produtos, como alimentos. Isso mostra como a tecnologia é versátil e pode ser usada para tornar muitos processos mais seguros e transparentes.

Figura 6: Esquema representativo de um blockchain.

Fonte: https://101blockchains.com/wp-content/uploads/2018/09/Como-funciona-a-BlockChain-Passo-a-Passo-702x336.png.webp

Biometria.

A biometria é uma tecnologia de segurança usada para identificar pessoas e proteger informações em locais como caixas eletrônicos, aeroportos e dispositivos como celulares. O termo vem do latim e significa "medição da vida", referindo-se ao estudo de características físicas (como impressões digitais) e comportamentais (como a forma de andar).

Na segurança, a biometria ajuda a controlar acessos, localizar criminosos e garantir que apenas pessoas autorizadas acessem informações sigilosas. Por ser única para cada pessoa, a biometria é uma forma eficiente de proteger dados, superando o uso de senhas.

Quais são os tipos de biometria mais populares?

Existem vários tipos de biometria. Aqui estão seis tipos populares de biometria que estão sendo usados em diversas soluções. Alguns são mais seguros e já têm estudos mais avançados, e é possível que no futuro se tornem padrões de segurança.

Impressão Digital

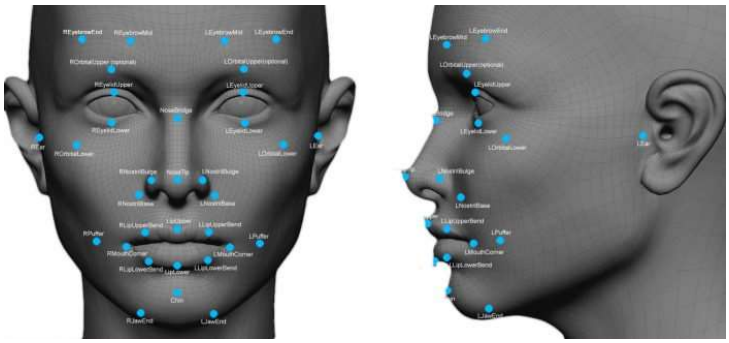
Figura 7

Fonte: https://files.tecnoblog.net/wp-content/uploads/2019/01/thedigitalway-fingerprint-pixabay-700x473.jpg

O reconhecimento biométrico por impressão digital é um dos métodos mais antigos e fáceis de usar. Ele é confiável porque as impressões digitais não mudam com o tempo. Essa tecnologia ajudou na transição do mundo analógico para o digital, mas o único problema é que a pessoa pode perder as digitais. Por isso, o método ainda é amplamente utilizado, sozinho ou em combinação com outras formas de segurança.

Reconhecimento Facial

Figura 8



Fonte: https://files.tecnoblog.net/wp-content/uploads/2019/01/fbi-facial-recognition-700x323.jpg

O reconhecimento facial, comum em celulares, mapeia rostos em 3D (como o Face ID da Apple) ou em 2D (como na maioria dos smartphones) para desbloquear dispositivos e identificar pessoas. No entanto, essa técnica tem desvantagens, como a possibilidade de o rosto mudar com o tempo, imprecisões na coleta de dados e erros que podem resultar em falsos positivos. Além disso, o reconhecimento facial pode ser invasivo, pois empresas e governos podem coletar dados faciais sem o consentimento das pessoas em locais públicos para diversos fins.

Reconhecimento de Íris

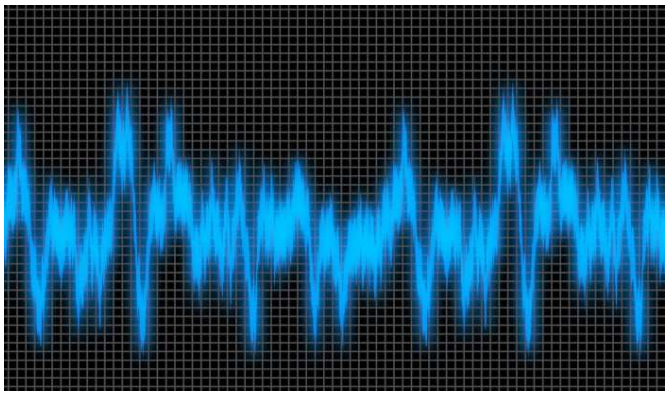
Figura 9

Fonte: https://files.tecnoblog.net/wp-content/uploads/2019/01/tbit-iris-scanning-pixabay-700x422.jpg

A biometria por íris é confiável porque a íris não muda ao longo da vida e é difícil de enganar. Embora seja menos invasiva do que a leitura da retina, sua implementação pode ser cara. Apesar disso, muitos acreditam que a leitura da íris se tornará o método biométrico mais popular, superando a impressão digital. Já há celulares, especialmente os mais caros, que possuem scanners de íris embutidos na câmera, oferecendo essa opção de segurança.

Reconhecimento de Voz

Figura 10

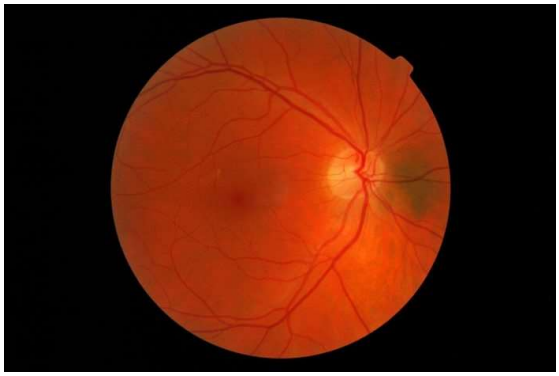


Fonte: https://files.tecnoblog.net/wp-content/uploads/2019/01/thedigitalartist-sound-wave-pixabay-700x408.jpg

O reconhecimento por voz analisa características físicas, como cordas vocais e laringe, e fatores comportamentais, como sotaques e entonações, criando um perfil sonoro único, semelhante a uma assinatura biométrica. Embora seja barato de implementar, sua confiabilidade é baixa, pois ruídos podem interferir na análise e mudanças na voz, devido à saúde ou envelhecimento, podem causar erros nas identificações.

Reconhecimento de Retina

Figura 11



Fonte: https://files.tecnoblog.net/wp-content/uploads/2019/01/rdowns-retina-pixabay-700x465.jpg

A leitura da retina é uma das biometrias mais seguras, pois a disposição dos vasos sanguíneos na retina é única e imutável. Esse método requer equipamentos especiais, dificultando a falsificação. O usuário apenas precisa olhar para um dispositivo, onde uma luz infravermelha faz a leitura. No entanto, apesar de sua segurança, esse método é invasivo e pode ser desconfortável.

Reconhecimento pela Digitação

Figura 12

Fonte: https://files.tecnoblog.net/wp-content/uploads/2019/01/picjumbo-com-woman-typing-pixabay-700x466.jpg

Esse método é pouco invasivo e analisa como a pessoa digita. Cada um tem seu próprio jeito de digitar, como quantos dedos usa, a velocidade e a pressão que faz nas teclas. Ele é barato, mas a captura dos dados não é tão fácil e não é muito confiável, porque alguém pode mudar seu estilo de digitação sem querer ou até de propósito.

5.3 Os perigos de um mundo sem criptografia e como se proteger corretamente para evitar cair em golpes.

Sem criptografia, a internet seria extremamente perigosa, permitindo que qualquer pessoa tivesse acesso a informações pessoais, como senhas, fotos e mensagens. Isso significaria que estranhos poderiam ver conversas privadas, dados bancários e bisbilhotar documentos importantes, tornando a vida online comparável a viver em uma "casa de vidro". Empresas, como bancos e hospitais, também estariam em risco, com hackers capazes de roubar segredos e manipular informações, ameaçando a saúde e a segurança financeira das pessoas. Além disso, compras online seriam inseguras, com dados de cartão de crédito vulneráveis a roubo. Governos

enfrentariam grandes problemas, pois documentos secretos e informações de segurança ficariam expostos, possibilitando invasões de comunicação e revelações de estratégias militares. Em suma, um mundo sem criptografia comprometeria a privacidade e a segurança de todos, destacando a importância desse "escudo invisível" que protege nossas atividades online.

Dicas para se proteger com mais eficiência

Senhas Fortes e Diferentes para Cada Conta: Sem criptografia, seria super fácil para hackers descobrirem nossas senhas. Por isso, ter uma senha longa e única para cada site seria essencial. Algo como misturar letras maiúsculas, minúsculas, números e símbolos. E nada de usar datas de aniversário ou nomes fáceis de adivinhar!

Evitar Redes Wi-Fi Públicas: Essas redes são um prato cheio para espiões digitais. Alguém poderia se conectar à mesma rede e ver tudo o que você está fazendo. Então, seria melhor usar uma conexão de dados segura ou pelo menos evitar acessar informações pessoais quando estiver em lugares como cafeterias ou shoppings.

Cuidado com Links e E-mails Suspeitos: Sem a proteção da criptografia, golpes online seriam ainda mais comuns. A gente teria que ficar de olho em mensagens e links esquisitos que parecem ser de empresas conhecidas, mas que na verdade são truques para roubar informações.

Não Compartilhar Informações Privadas em Mensagens: Evitar ao máximo mandar senhas, números de documentos ou qualquer informação pessoal em mensagens, mesmo que pareça uma conversa segura. Sempre que possível, prefira conversar sobre essas coisas pessoalmente.

Usar Programas e Apps de Segurança: Mesmo sem a criptografia, alguns programas como antivírus, firewalls e aplicativos de segurança poderiam ajudar a impedir que hackers invadissem seu computador ou celular.

Manter o Sistema Atualizado: Os sistemas operacionais (Windows, Android, iOS) sempre lançam atualizações para corrigir falhas de segurança. Manter seus dispositivos atualizados ajuda a reduzir as brechas que hackers poderiam explorar.

Autenticação em Duas Etapas: Quando possível, usar a autenticação em duas etapas (2FA) seria crucial. Mesmo que alguém conseguisse descobrir sua senha, precisaria de um segundo código enviado para o seu celular ou e-mail.

Usar Nomes de Usuário Criativos: Não usar o próprio nome, apelidos conhecidos ou informações pessoais nos nomes de usuário. Quanto mais diferente, mais difícil seria para alguém adivinhar.

Desconfiar de Tudo Que Parece Bom Demais para Ser Verdade: Ofertas superbaratas, promessas de prêmios e mensagens urgentes para clicar em um link são quase sempre armadilhas. Se parece muito bom, vale a pena pesquisar e desconfiar.

Falar com Alguém de Confiança: Se você acha que está sendo espionado ou suas informações foram vazadas, o melhor é conversar com alguém que entenda de segurança digital. Isso ajuda a tomar as medidas certas antes que os danos sejam maiores.

ODS 16

A **ODS 16** fala sobre justiça, paz e a construção de instituições que funcionem de forma justa e transparente. Mas o que isso tem a ver com criptografia? Muito! Se a gente parar para

pensar, a segurança digital é um pilar importante para que a justiça e a transparência existam. Por exemplo, se nossas informações pessoais não estiverem protegidas, qualquer um poderia roubar identidades, vazar documentos ou manipular dados. Isso abriria espaço para corrupção e vários crimes digitais.

A criptografia ajuda a garantir que nossos dados, sejam eles conversas, documentos ou transações, sejam sigilosos e acessíveis apenas para quem tem autorização. Isso é essencial para proteger a nossa privacidade e permitir que a justiça e a confiança nas instituições sejam mantidas. Ou seja, sem criptografia, o mundo digital se tornaria um lugar muito mais perigoso e injusto.

6.Resultados e Discussões

Evolução Histórica da Criptografia

Durante o desenvolvimento do projeto, os autores compreenderam a evolução da criptografia ao longo dos séculos, explorando exemplos como a Cifra de César, usada por Júlio César, e a Máquina Enigma da Segunda Guerra Mundial. Eles estudaram criptografia simétrica e assimétrica, destacando a importância do algoritmo RSA, e debateram o impacto da criptografia quântica no futuro. Os resultados mostraram que os estudantes passaram a reconhecer a criptografia como um campo dinâmico e essencial para a segurança.

Importância da Criptografia no Dia a Dia

Nas apresentações e discussões, os autores foram incentivados a identificar situações cotidianas onde a criptografia está presente, como em aplicativos de mensagens e redes sociais. Muitos se surpreenderam ao perceber que atividades simples, como desbloquear o celular com reconhecimento facial, dependem de criptografia. Isso os ajudou a entender a relevância prática do estudo e a importância de manter esses mecanismos de segurança. Os feedbacks indicaram que a maioria começou a valorizar mais o papel da criptografia no cotidiano.

Conscientização Sobre um Mundo sem Criptografia

Para entender como seria a ausência de criptografia, os autores realizaram discussões em grupo, tentando prever como seria viver em um ambiente onde qualquer pessoa pudesse acessar informações sigilosas ou realizar transações bancárias em nome de outra. Eles chegaram à conclusão de que, sem a criptografia, a privacidade estaria comprometida e os crimes cibernéticos aumentariam. A atividade gerou bastante debate, reforçando a percepção de que a proteção dos dados não é apenas uma questão técnica, mas também um direito.

Propostas para Aumentar a Segurança Digital

Com base no conteúdo apresentado, os estudantes elaboraram listas de recomendações práticas para proteger suas próprias informações, como criar senhas mais complexas, habilitar a autenticação de dois fatores e reconhecer sinais de tentativas de phishing. Eles também discutiram a importância de usar redes seguras e de não compartilhar dados pessoais sem verificar a fonte. Muitos relataram que, após o projeto, começaram a aplicar essas práticas, mostrando que o conhecimento adquirido impactou positivamente seu comportamento digital.

Relação com o ODS 16 – Paz, Justiça e Instituições Eficazes

A conexão com o ODS 16 foi explorada ao relacionar a criptografia com a promoção de uma sociedade mais segura e justa. Os alunos entenderam que a proteção de informações não é apenas uma medida de segurança pessoal, mas também um pilar para garantir a privacidade, a proteção de direitos e a prevenção de abusos. Isso gerou reflexões sobre o uso ético da tecnologia e como a criptografia pode apoiar governos e instituições a protegerem dados sensíveis e promoverem a confiança no ambiente digital. Os debates ampliaram o entendimento dos alunos sobre como a criptografia contribui para uma sociedade mais inclusiva e segura, alinhada aos objetivos globais de desenvolvimento sustentável.

7.Considerações Finais

O projeto começou com a hipótese de que a falta de criptografia moderna tornaria as pessoas mais vulneráveis a ataques cibernéticos, e, ao longo do trabalho, constatou-se que essa afirmação é verdadeira. O estudo de diferentes tipos de criptografia revelou que essa tecnologia é fundamental para proteger dados digitais, pois sem ela, informações sensíveis estariam expostas a invasões e manipulações por criminosos virtuais. Ao discutir um mundo sem criptografia, os alunos refletiram sobre os riscos à privacidade individual e à confiança em serviços digitais, além da importância da criptografia como um direito essencial à segurança. A evolução das técnicas, desde a Cifra de César até algoritmos complexos, reforçou a necessidade de proteger dados em uma sociedade tecnológica. O projeto também relacionou a criptografia ao ODS 16, mostrando como ela contribui para um ambiente mais seguro e justo. Além das discussões teóricas, serão realizados experimentos práticos na FECEG, onde os alunos apresentarão simulações para ilustrar a importância da criptografia na segurança digital.

8.Referências Bibliográficas

- ARANHA, Christian. Bitcoin, Blockchain e muito dinheiro: uma nova chance para o mundo. 3. ed. Rio de Janeiro: Valentina, 2021.
- JORNAL DA USP, Odemir M. Bruno. Critografia: de arma de guerra a pilar da sociedade moderna, 09/jan/2017. Disponível em: <https://jornal.usp.br/artigos/criptografia-de-arma-de-guerra-a-pilar-da-sociedade-moderna/> . Acesso em: 03 jun. 2024.
- SIDHPURWALA, H. Uma breve história da criptografia. Disponível em: <https://www.redhat.com/pt-br/blog/brief-history-cryptography> Acesso em: 06 jun. 2024.
- IBM. Disponível em: <https://www.ibm.com/br-pt/topics/quantum-cryptography> Acesso em: 06 jun. 2024.
- BRASIL ESCOLA, Máquina enigma. Disponível em: <https://brasilescola.uol.com.br/historiag/maquina-enigma.htm> Acesso em: 13 jun. 2024.
- DOC9, Criptografia assimétrica: saiba o que é, como funciona e vantagens. Disponível em: <https://doc9.com.br/blog/criptografia-assimetrica-o-que-como-funciona-e-vantagens/> Acesso em: 20 jun. 2024.

- MEDIUM. Criptografia simétrica. Disponível em: <https://medium.com/prognosys/criptografia-sim%C3%A9trica-6b4271ff697c> Acesso em: 20 jun. 2024.
- TECNOBLOG. O que é biometria? Os 6 tipos mais usados na tecnologia. Disponível em: <https://tecnoblog.net/responde/o-que-e-biometria-tecnologia/> Acesso em: 05 set. 2024.
- SERASA PREMIUM. Proteção de dados. Disponível em: <https://www.serasa.com.br/premium/blog/protecao-de-dados-4-razoes-para-se-preocupar/> Acesso em: 12 set. 2024.