UNIVERSIDADE ESTADUAL DE MONTES CLAROS – UNIMONTES
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS – CCET
DEPARTAMENTO DE CIÊNCIAS DA COMPUTAÇÃO – DCC

ATIVIDADE 6 - CRIPTOGRAFIA E SEGURANÇA

ERIC SILVA GUSMÃO
JOÃO PEDRO ARANTES MONTEIRO
LINCON AQUINO SOARES
RAMON LOPES DE QUEIROZ
YURI MARQUES DE AGUIAR

MONTES CLAROS – MG
OUTUBRO/2025

ERIC SILVA GUSMÃO
JOÃO PEDRO ARANTES MONTEIRO
LINCON AQUINO SOARES
RAMON LOPES DE QUEIROZ
YURI MARQUES DE AGUIAR

ATIVIDADE 6 - CRIPTOGRAFIA E SEGURANÇA

Atividade avaliativa apresentada para atendimento de requisito parcial para aprovação na disciplina Matemática Computacional do Curso de Graduação em Bacharelado em Sistemas de Informação – 1º período

Professor: Dr. Reginaldo Morais de Macedo

MONTES CLAROS – MG
OUTUBRO/2025

Exercício 6:

1) “universidade estadual de montes claros departamento de ciências da computação curso de graduação em bacharelado em ciências da computação disciplina matemática computacional

por tres anos, onde quer que os marines aterrissarem, os japoneses recebiam uma enxurrada de estranhos ruidos gorgolejo antes entremeados com outros sons que lembravam o clamor de um monge tibetano e o som de uma bolsa de agua quente sendo esvaziada”.

2) A segurança é um conjunto de medidas e técnicas que garantem a proteção de informações.
Ela busca garantir quatro princípios:

- **Confidencialidade:** Apenas pessoas autorizadas têm acesso.
- **Autenticidade:** Confirmar a identidade de quem acessa e impedir que negue uma ação realizada.
- **Integridade:** A informação não pode estar inacessível ou corrompida.
- **Disponibilidade:** Os dados têm que estar acessíveis sempre que necessário.

A segurança é crucial para os sistemas de informação por:

- Proteger dados sensíveis e importantes.
- Prevenir ataques e fraudes.
- Manter a confiança.
- Evitar prejuízos.
- Assegura a continuidade dos serviços.

3) A segurança em sistemas de informação envolvem diferentes atores com motivações próprias, que alteram o como as medidas de segurança são implementadas ou atacadas.

Usuários finais

- Motivações positivas

Algumas das motivações positivas deles são: Ter confiança de que seus dados pessoais estarão seguros e que seja garantido o acesso contínuo do serviço sem interrupção.

- Possíveis conflitos

Os usuários podem ter preferência de conforto e facilidade sobre a segurança, colocando senhas fáceis e compartilhamentos de logins.

Administradores e equipes de TI

- Motivações positivas

Eles prezam por manter integridade e disponibilidade do sistema, evitar falhas que possam prejudicar a organização e cumprir normas e regulamentos de segurança.

- Possíveis conflitos

Equilibrar facilidade de uso e custo e podem ser pressionados por conta de prazos curtos que diminuem o investimento na segurança.

Gestores e executivos da organização

- Motivações positivas

Estar em conformidade com a legislação, proteger ativos estratégicos importantes e evitar danos à reputação.

- Possíveis conflitos

A segurança é vista como custo invisível, tendo seu investimento reduzido por causa de reduções de custos e negligência.

Atacantes (hackers, criminosos)

- Motivações negativas

Roubos de contas bancárias, protestos digitais, obter vantagens competitivas

4) A criptografia, que vem do grego e significa "escrita secreta", transforma informações para torná-las ilegíveis a pessoas não autorizadas.Ela tem sido utilizada por militares e diplomatas, pois muitas informações secretas não podem ser acessadas por qualquer pessoa.

O modelo básico de criptografia envolve a transformação de uma mensagem por meio de uma função parametrizada por uma chave, onde o resultado é um texto cifrado, que é transmitido,além disso,um intruso pode interceptar o texto cifrado, mas, sem a chave, não consegue descriptografá-lo.

5) Cifra é a transformação caractere por caractere ou bit a bit, já o Código substitui uma palavra por outra palavra ou símbolo.
Exemplo de Cifra: Cifra de César, onde cada letra é substituída por outra letra a uma distância fixa no alfabeto.
Exemplo de Código: Código Navajo, Guerreiros Navajo se comunicavam usando palavras específicas em sua língua para termos militares.

6) Técnicas fundamentais da Criptografia ao longo do tempo:
Cifras de Substituição: Cada letra ou grupo de letras é substituído por outra.
Cifras de Transposição: Reordenam as letras da mensagem.
Chave Única: Sequência de bits aleatórios usada para codificar o texto simples.
Algoritmos de Base Simétrica: Utilizam a mesma chave para codificação e decodificação.
Algoritmos de Chave Pública: Utilizam chaves diferentes para a codificação e decodificação.
Funções de Hash: Utilizadas na criptografia para garantir a integridade e autenticidade da mensagem.
Criptografia Quântica: Promete uma solução para a transmissão de chaves únicas pela rede, potencialmente tornando os sistemas criptográficos invioláveis.

7) Criptoanálise: É a arte de solucionar mensagens cifradas.
Exemplos- Adivinhação de palavras ou frases prováveis: Usada para quebrar cifras de substituição, procurando por padrões de letras repetidas em palavras comuns.
Ataque à cifra de transposição: Analisar a frequência das letras para confirmar que é uma cifra de transposição, e estimar o número de colunas e ordenar as colunas com base em diagramas e trigramas.

Criptologia: Engloba a criptografia e a criptoanálise.

8) É uma estratégia que se baseia em tentar manter o algoritmo de criptografia secreto para garantir a segurança. Porém, o princípio de Kerckhoff afirma que essa abordagem nunca funciona, pois ele estabelece que todos os algoritmos devem ser públicos.

9) É a medida da dificuldade computacional de “quebrar” uma cifra, e é diretamente influenciado pelo tamanho da chave utilizada.

10) O primeiro tipo de problema de criptoanálise é o problema do texto cifrado disponível. Esse tipo específico acontece quando existe o texto cifrado mas sem exemplos de textos simples, assim como sem a chave usada, um exemplo são as palavras cruzadas. Outra variação é o texto simples conhecido, que acontece quando existem exemplos do texto cifrado e de textos simples que correspondem, sendo necessário então entender a chave que foi usada no processo. Esse tipo de problema ocorre em mensagens que possuem trechos repetitivos, são padronizadas, como em algumas comunicações militares. O terceiro problema é o do texto simples disponível. Nesse tipo de problema, o criptoanalista consegue criptografar textos simples e analisar o texto cifrado gerado, possibilitando assim uma análise para descobrir a chave. Um exemplo seria o atacante ter acesso a máquina ou software que gera o texto cifrado.

11) As cifras por substituição são um tipo de cifra em que cada letra do texto simples é substituído por outra letra ou grupo de letras para codificar a mensagem. Dentre os exemplos de cifras de substituição é possível citar a cifra de César, em que as letras do alfabeto movem-se três posições para a frente, sendo substituídas pelas letras da posição selecionada, podendo ser descriptografadas realizando o movimento oposto das letras. Outro exemplo é a própria generalização da cifra de César, em que o carácter é deslocado k vezes de maneira circular pelo alfabeto, sendo possível de ser descriptografado caso se saiba a chave k. Outro sistema de substituição é a cifra de substituição monoalfabética, em que se usa uma palavra chave para substituir as letras do alfabeto. A palavra escolhida (que não deve apresentar repetição) é colocada no início do “novo” alfabeto e os caracteres que não a formam aparecem

em seguida. O texto cifrado pode ser descriptografado caso quem o receba possua a palavra chave.

12) As cifras de transposição são um tipo de método de cifragem em que os caracteres, ou bits, de um texto simples são reordenados, a ordem é embaralhada. O método contrasta com as cifras de substituição que mudam os símbolos. Um exemplo de cifra de transposição é a cifra de colunas. Nesse método existe uma palavra chave que indicará como o texto simples será embaralhado, em formato de linhas e colunas. A palavra chave representa as colunas e o texto simples compõe as linhas escritas abaixo. A ordem em que as letras da chave aparecem no alfabeto é o que indica como as colunas serão embaralhadas. O destinatário do texto cifrado pode descriptografá-lo realizando o processo oposto, desde que saiba a palavra chave. Um exemplo parecido é a cifra de Myszkowski. Nesse método a palavra chave pode possuir repetição de letras, porém, os caracteres abaixo de letras repetidas são lidos como um bloco, na horizontal. Outro exemplo de transposição é o método “Rail Fence” em que os caracteres são escritos em uma matriz em um padrão de ziguezague, que deve ser conhecido por quem tentará descriptografar.

13) Uma chave única em criptografia é uma cifra considerada inquebrável. O seu funcionamento é simples, porém, muito eficaz. O primeiro passo é converter um texto simples, a mensagem a ser criptografada em um sequência de bits. Em seguida, é criada uma chave, outra sequência de bits, que tem o exato comprimento que o texto simples. A chave é então usada em um operação XOR com o texto simples transformado em sequência de bits, criando um texto cifrado, resultando em bits que parecem ser completamente aleatórios e não relacionados ao texto simples. Tanto o emissor, quanto o destinatário da mensagem necessitam da chave única para criptografar e descriptografar a mensagem (utilizando também a operação XOR). Para que a chave seja considerada inviolável ela tem de ser utilizada apenas uma vez e tem de ser tão longa quanto o texto simples, a mensagem a ser transmitida. O método é considerado inquebrável pois não existe nenhuma informação na mensagem cifrada, todos os textos possíveis com o mesmo tamanho são igualmente possíveis.

14) A criptografia quântica é uma área ainda incipiente da criptografia que busca resolver o desafio de como trocar uma chave única de maneira segura. Um dos exemplos desse tipo de criptografia é o BB84. Este protocolo baseia-se no fato da luz ser transmitida em formato de fótons e que pode ser polarizada ao passar por um filtro de polarização. Em uma conexão de fibra óptica, os dois protagonistas usam filtros polarizados para transmitir, codificar, decodificar e receber bits. Para cada bit enviado, o emissor usa duas bases de polarização, a base padrão e a base vertical, que podem ser trocadas rapidamente no feixe de luz transmitido. Do mesmo modo, receptor da mensagem escolhe também aleatóriamente uma das duas bases para medir o fóton, um qubit (um bit quântico). Se ambos os lados da comunicação escolherem a mesma base para um fóton específico, o bit será recebido de maneira correta. Por outro lado, se escolherem uma base diferente, o bit se torna inútil e a mensagem é perdida, ou seja, alguns fótons foram lidos corretamente e outros não. Em seguida, através de uma comunicação de texto simples, ambos trocam a informação de que base usaram para enviar e ler os qubits, e os lidos de maneira correta compõem a chave única. Caso um intruso tenta interceptar a mensagem e usar uma base incorreta para decodificá-la, a polarização do fóton será alterada e é possível perceber que existe uma tentativa de invasão. As perspectivas para o futuro da criptografia quântica são promissoras, mas esbarram na complexidade e nos custos desse tipo de tecnologia. Além disso, a tecnologia pode ser usada em curtas distâncias de cabos de fibra óptica.

15) A criptografia possui dois princípios fundamentais. O primeiro deles é a redundância, que diz que todas as mensagens criptografadas devem ter alguma informação adicional que não seja necessária para a sua compreensão, mas que permita ao receptor verificar se a mensagem é válida. Essa redundância é importante para impedir que intrusos ativos enviem lixos ou mensagens inválidas, enganando o receptor. O segundo princípio é a atualidade. Cada mensagem recebida precisa ser confirmada como uma mensagem atual. Essa medida é necessária para que intrusos ativos não reutilizem mensagens antigas e, assim, impedir ataques de repetição.

16) Algoritmo de chave simétrica é um método de criptografia que utiliza a mesma chave para codificação e decodificação de uma mensagem. Esse algoritmo de

criptografia funciona através do processamento por blocos. Se opera com blocos de bits ou bytes. Um bloco de entrada, de tamanho fixo, é transformado usando a chave secreta em um bloco de saída criptografado. Essa transformação é feita através de operações de substituição, transposição ou combinações mais complexas dessas operações.

17) 1. Criptoanálise diferencial

Essa técnica pode ser usada para atacar qualquer cifra de bloco. Ela analisa pares de blocos e textos simples que diferem apenas por um pequeno número de bits e observa a mudança nas mensagens cifradas resultantes dessa diferença. Essa observação pode levar a ataques probabilísticos.

2. Criptoanálise linear

Essa técnica funciona através da aplicação de cálculos XOR entre certos bits do texto cifrado e do texto simples, procurando por padrões de inclinação.

3. Uso da análise do consumo de energia elétrica

Essa técnica analisa o consumo de energia elétrica para encontrar chaves secretas. Através de algoritmos criptográficos de leitura dos bits de uma chave, é possível medir e monitorar a energia consumida por cada instrução da máquina e, assim, deduzir a chave.

4. Análise de sincronismo

Essa técnica explora as pequenas diferenças no tempo necessário para executar certas operações de cifragem, especialmente aquelas que envolvem testes condicionais (ifs). Se essas diferenças de tempo forem medidas com precisão, é possível deduzir informações sobre as chaves de rodadas e, assim, calcular a chave original.

18) RSA é um sistema de criptografia de chave pública descoberto por um grupo de pesquisadores do MIT e o seu nome é formado pelas iniciais dos sobrenomes dos três estudiosos que o criaram: Ron Rivest, Adi Shamir, Leonard Adleman. Os três

receberam o ACM Turing Award, prêmio concedido a grandes contribuições à computação, devido à segurança e força do algoritmo.

19) O funcionamento desse algoritmo envolve a geração de um par de chaves – uma pública e uma privada – que são usadas para criptografar e descriptografar mensagens. De forma simplificada, o funcionamento de RSA ocorre da seguinte maneira:

1. Geração das chaves

- Selecione dois números primos grandes, *p* e *q*, geralmente com pelo menos 1024 bits cada.
- Calcule $n = p \times q$ e $z = (p-1) \times (q-1)$
- Selecione um número *d* tal que *z* e *d* sejam primos entre si.
- Por fim encontre *e* tal que $e \times d = 1 \bmod z$.

2. Distribuição das chaves

- **Chave pública:** É composta por (*e*, *n*). Pode ser divulgada livremente.
- **Chave privada:** É composta por (*d*, *n*). Deve ser mantida em segredo.

3. Criptografia

- Dada uma mensagem P, representada como um número inteiro $0 \leq P < n$, a mensagem cifrada C é calculada por:

$C = P^e \pmod n$

Ou seja, elevando-se *P* a *e*, e calculando o resto da divisão por *n*.

4. Decriptação

- Para recuperar a mensagem original *P*, o destinatário utiliza sua chave privada (*d*, *n*) e calcula:

$P = C^d \pmod n$

As operações de encriptação e de decriptação são inversas entre si e a segurança do RSA baseia-se na dificuldade de fatorar números extensos.

20) O ataque do aniversário é um método que explora a matemática por trás da teoria da probabilidade para encontrar "colisões" em funções de hash criptográfico, ou seja, encontrar duas mensagens diferentes que produzem o mesmo resumo (hash). O problema questiona quantas pessoas são necessárias em uma sala para que a probabilidade de duas delas compartilharem o mesmo aniversário seja superior a 50%. A resposta, surpreendentemente, é de apenas 23 pessoas.

A explicação para este resultado está no número de pares que podem ser formados:

- Com 23 pessoas, é possível formar (23×22)/2=253 pares diferentes.
- Cada um desses pares tem uma chance em 365 de corresponder (ter o mesmo aniversário). A probabilidade de haver pelo menos uma correspondência se torna alta.

Aplicado à criptografia, onde as mensagens são as "entradas" e os resumos de hash são as "saídas": Usando o ataque do aniversário, um invasor só precisa gerar cerca de n=k=(2^64)^1/2=2^32 mensagens diferentes para ter uma alta probabilidade de encontrar duas com o mesmo resumo.

21) O funcionamento do PGP (Pretty Good Privacy) para enviar uma mensagem segura e assinada de Alice para Bob. O PGP combina criptografia de chave pública (RSA) e de chave simétrica (IDEA) para fornecer privacidade, autenticação, assinatura digital e compactação.

O processo de envio da mensagem por Alice é:

1. **Assinatura Digital:**

Primeiramente, o PGP calcula um resumo (hash) da mensagem original (P) usando o algoritmo MD5. Esse hash é então criptografado com a chave RSA privada de Alice (DA). O resultado é a assinatura digital, que garante a autoria e a integridade da mensagem.

2. **Compactação:**

A mensagem original (P) é concatenada com a sua assinatura digital, formando uma nova mensagem (P1). Essa mensagem P1 é então compactada com o programa ZIP para reduzir seu tamanho e aumentar a segurança, gerando a saída P1.Z.

3. **Criptografia (Confidencialidade):**

O PGP gera uma chave de sessão de 128 bits, única e aleatória (KM), para o algoritmo de cifra de bloco IDEA. A mensagem compactada (P1.Z) é criptografada usando essa chave de sessão IDEA (KM). Como o IDEA é muito mais rápido que o RSA, ele é usado para criptografar o corpo da mensagem. Para que Bob possa descriptografar a mensagem, a chave de sessão (KM) é criptografada com a chave RSA pública de Bob (EB).

4. **Formatação para Envio:**

A mensagem principal (já criptografada com IDEA) e a chave de sessão (criptografada com RSA) são concatenadas. O resultado final é convertido para o formato Base64. Isso garante que a mensagem contenha apenas caracteres de texto padrão e possa ser enviada por qualquer sistema de e-mail sem ser corrompida.

Ao receber a mensagem, Bob reverte o processo. Após a reversão, um novo hash MD5 da mensagem recebida é comparado com o hash que ele descriptografou. Se os dois forem idênticos, Bob tem a certeza de que a mensagem veio de Alice e não foi alterada no caminho.

22) A esteganografia é a ciência de ocultar mensagens, de modo que o próprio fato de haver uma comunicação secreta seja escondido. Diferente da criptografia, que codifica uma mensagem para torná-la ilegível, a esteganografia oculta a mensagem dentro de outro arquivo ou meio, de forma que sua existência seja imperceptível.
Funcionamento:

- **Meio de Cobertura:** Utiliza-se um arquivo de mídia, como uma fotografia colorida, que é composta por pixels. Cada pixel é definido por três valores numéricos de 8 bits que representam a intensidade das cores primárias: vermelho, verde e azul (RGB).

- **Canal Oculto:** O método de codificação aproveita o bit de menor ordem (o menos significativo) de cada um desses valores de cor. Alterar este bit causa uma mudança tão sutil na cor que é invisível ao olho humano, que não consegue distinguir facilmente entre cores de 21 bits e de 24 bits.
- **Processo de Codificação:**

1. A mensagem secreta é primeiramente compactada para reduzir seu tamanho e, em seguida, criptografada para maior segurança.
2. Os bits da mensagem criptografada são inseridos, um a um, nos bits de menor ordem de cada valor de cor (vermelho, verde e azul) dos pixels da imagem.
3. Dessa forma, uma imagem de 1024×768 pixels pode ocultar até 294.912 bytes de informação secreta sem que haja alteração visual perceptível.

23) A tecnologia de segurança da Internet converge com importantes questões sociais, políticas e legais. Na área da privacidade, existe um conflito entre o direito dos cidadãos de usar criptografia forte, como o PGP, para proteger suas comunicações e os esforços de governos para monitorar o tráfego em nome da segurança. Ferramentas como repostadores anônimos e o roteamento cebola surgiram para permitir a comunicação e a navegação sem revelar a identidade do usuário, protegendo dissidentes e delatores.

Quanto à liberdade de expressão, a natureza global da web gera conflitos sobre censura, pois as leis de um país podem ser aplicadas a sites de outras nações. Em resposta, foram desenvolvidas tecnologias para contornar a censura, como sistemas de armazenamento persistente e a esteganografia, que oculta a existência de mensagens dentro de arquivos de mídia.

Por fim, os direitos autorais representam uma batalha entre os detentores de propriedade intelectual e o público, intensificada por redes de compartilhamento de arquivos. Leis como o DMCA (Digital Millennium Copyright Act) criminalizam a quebra de proteções contra cópia, o que pode restringir o uso legal (fair use) e a pesquisa científica. A discussão sobre o equilíbrio entre os interesses dos criadores e do público continua, com novas tecnologias como a "computação confiável" prometendo um controle ainda mais rígido sobre o conteúdo.

Referências Bibliográficas:

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011.