|  |  |  |
| --- | --- | --- |
|  |  |  |

**Criptografia: Sua Aplicação e Importância na Segurança da Informação**

CURSO – DESENVOLVIMENTO DE SISTEMAS

PROFESSORA: Mizael

Aluno: Daniel Natan Maurício Lapa e João Vitor Souza

**BELO HORIZONTE**

***MAIO/ 202***5

#### 

#### Instruções:

Pesquise nos sites confiáveis, manuais oficiais ou materiais educacionais para responder às questões abaixo. Use fontes como:

* [https://gnupg.org](https://gnupg.org/)
* Artigos de segurança da informação
* Vídeos e manuais técnicos do BitLocker e FileVault

### Questões

1. O que é PGP e qual seu objetivo principal na criptografia de dados?

O Pretty Good Privacy (PGP) é um software de criptografia utilizado em e-mails e arquivos confidenciais. Desde que foi criado em 1991, o PGP se tornou o padrão de fato em relação à segurança de e-mails. O PGP tem alguns recursos em comum com outros softwares de criptografia que você talvez conheça, como [criptografia para protocolo Kerberos](https://www.varonis.com/blog/kerberos-authentication-explained/?hsLang=pt-br) (usada para autenticar usuários em uma rede) e [criptografia SSL](https://www.thesslstore.com/blog/understanding-the-encryption-technology-behind-ssl/) (usada para proteger sites). O principal objetivo do **PGP (Pretty Good Privacy)** na criptografia de dados é **garantir a confidencialidade, integridade e autenticidade das informações trocadas entre usuários.**

1. Qual a diferença entre PGP e GNU GPG?

A diferença entre PGP e [GPG](https://www.goanywhere.com/blog/the-ultimate-checklist-for-purchasing-file-encryption-software) é que o PGP (Pretty Good Privacy) é um software de criptografia proprietário, enquanto o GPG (GNU Privacy Guard) é uma implementação de código aberto do padrão OpenPGP. Ambos são usados ​​para criptografar e descriptografar e-mails, arquivos e comunicações digitais, mas o GPG oferece maior flexibilidade, suporta mais algoritmos de criptografia (como RSA, AES e Twofish) e é disponível gratuitamente. O PGP, por outro lado, requer uma licença proprietária para sua versão comercial. O GPG é amplamente preferido para criptografia moderna devido à sua segurança, manutenção ativa e desenvolvimento orientado pela comunidade.

1. O que é uma chave pública e uma chave privada no contexto do GPG?

Chaves matemáticas que funcionam em conjunto para criptografar e descriptografar dados, bem como assinar e verificar assinaturas digitais. A chave pública pode ser compartilhada com outras pessoas, enquanto a chave privada deve ser mantida em segredo, se alguém quer enviar uma mensagem secreta para outra pessoa, basta usar a do destinatário para codificar a mensagem e somente o destinatário poderá decodificar a mensagem usando sua chave privada.

Esse sistema garante a confidencialidade e a autenticidade das comunicações, pois evita que terceiros interceptem ou alterem as mensagens sem ter acesso às chaves privadas dos envolvidos.

1. Explique como funciona a criptografia assimétrica. Dê um exemplo de uso no cotidiano.

é um método de [criptografia](https://www.ibm.com/br-pt/topics/encryption) que usa duas chaves diferentes — uma chave pública e uma chave privada — para criptografar e descriptografar dados. Em geral, ela é considerada mais segura, embora menos eficiente, do que a criptografia simétrica, Outro exemplo está nos e-mails. A união da tecnologia de proteção de dados garante que o conteúdo dos e-mails fique protegido de qualquer um que não faça parte da conversa.

Se alguém de fora, um terceiro, procura ler o conteúdo de um e-mail que não faz parte, ele apenas vai acessar uma forma criptografada do mesmo – que não é legível por um humano.

1. Explique como funciona a criptografia simétrica. Dê um exemplo de uso.
2. Um método de criptografia que usa uma única chave para criptografar e descriptografar dados. Embora geralmente seja menos segura do que a criptografia assimétrica, é considerada mais eficiente porque exige menos capacidade de processamento, ao receber o documento criptografado, Bob usa a mesma chave secreta para descriptografá-lo de volta à sua forma original, garantindo a confidencialidade durante a transmissão.
3. Quais são as vantagens e desvantagens da criptografia assimétrica em relação à simétrica?

Vantagem principal: É mais segura que a criptografia simétrica, pois a chave pública é conhecida por todos, e o receptor da mensagem não precisa revelar a sua chave privada

Desvantagem: É mais lenta que a criptografia simétrica.

1. Qual o papel do GPG na comunicação segura por e-mail?

oferecendo **criptografia de ponta a ponta** e **assinaturas digitais**. Ele é uma implementação livre do padrão OpenPGP (RFC 4880),

| **Função** | **Benefício** |
| --- | --- |

|  |  |
| --- | --- |
| Criptografia | Confidencialidade |

|  |  |
| --- | --- |
| Assinatura digital | Autenticidade e integridade |

|  |  |
| --- | --- |
| Web of trust | Confiança sem autoridade central |

1. O que é criptografia de disco? Cite dois softwares usados para isso e explique brevemente como funcionam.

processo de criptografar todos os dados no disco rígido de um computador, incluindo o sistema operacional, permitindo o acesso somente após autenticação bem-sucedida no produto de criptografia. É comumente usada em computadores desktop e laptops para proteger dados contra acesso não autorizado, software FDE funciona redirecionando o registro mestre de inicialização (MBR) do computador, que é um setor reservado na mídia inicializável que determina qual software (por exemplo, sistema operacional, utilitário) será executado quando o computador inicializar a partir da mídia. Antes de o software FDE ser instalado em um computador, o MBR geralmente aponta para o sistema operacional principal do computador.

1. Compare o BitLocker (Windows) e o FileVault (macOS). Quais suas semelhanças e diferenças?

Um dos recursos de segurança integrados do Windows, a Criptografia de Unidade de Disco [BitLocker](https://www.donemax.com/wiki/bitlocker.html) , embaralha todos os dados na unidade do sistema. Criptografar os dados no seu dispositivo é uma precaução útil. Uma chave de descriptografia, como uma senha ou PIN, deve ser lida, Um dos recursos de segurança integrados do Windows, a Criptografia de Unidade de Disco [BitLocker](https://www.donemax.com/wiki/bitlocker.html) , embaralha todos os dados na unidade do sistema. Criptografar os dados no seu dispositivo é uma precaução útil. Uma chave de descriptografia, como uma senha ou PIN, deve ser lida.

1. O que significa criptografia de ponta a ponta em uma conversa por aplicativo de mensagem?

são criptografadas no dispositivo do remetente e só podem ser decifradas no dispositivo do destinatário, e não em nenhum ponto intermédio. Isso garante que o conteúdo das mensagens seja confidencial e que apenas o remetente e o destinatário possam lê-las, mesmo que os servidores do aplicativo ou outras partes possam ter acesso às mensagens durante o transporte,

1. Qual a importância da criptografia de ponta a ponta em aplicativos como WhatsApp e Signal?

proteger a privacidade das conversas, garantindo que apenas o remetente e o destinatário possam ler as mensagens, mesmo que as mensagens passem pelos servidores do aplicativo, quando você envia uma mensagem no WhatsApp, ela é criptografada no seu dispositivo e só pode ser descriptografada no dispositivo do destinatário, sem que o WhatsApp tenha acesso ao conteúdo. Isso garante que a mensagem seja segura e privada, mesmo que o WhatsApp armazene a mensagem em seus servidores.

1. Cite dois riscos de armazenar dados importantes em um computador sem qualquer tipo de criptografia

**Acesso não autorizado**: Se alguém obtiver acesso físico ou remoto ao computador (por exemplo, por meio de um ataque hacker ou roubo do dispositivo), os dados poderão ser lidos facilmente, já que não estão protegidos por nenhuma forma de codificação

**Vazamento de informações sensíveis**: Sem criptografia, dados confidenciais como senhas, informações bancárias, dados pessoais ou corporativos podem ser expostos ou roubados, resultando em prejuízos financeiros, danos à reputação ou violação de leis de proteção de dados, como a LGPD ou o GDPR.

1. .

4o

1. Como a criptografia ajuda a proteger dados em caso de roubo de notebook ou celular?
2. Qual a diferença entre o uso legítimo da criptografia e a criptografia usada em ataques de ransomware?
3. O ransomware criptografa os dados da vítima. Como essa técnica é diferente da criptografia usada por softwares como GPG ou BitLocker?

### 

Após realizar a pesquisa, e disponibilizar o seu arquivo em seu github, que escolham uma ferramenta (GPG,RSA, BitLocker,FileVault) e façam uma breve EM GRUPO apresentação em sala de aula de 7 minutos explicando como ela protege os dados do usuário.

**Referências: ( NA NORMA DA ABNT)**

MITNICK, K. D.; SIMON, W. L. *The art of deception: controlling the human element of security*. Indianapolis: Wiley Publishing, 2011.

OLIVEIRA, R. *Segurança da informação para leigos*. 3. ed. Rio de Janeiro: Brasport, 2012.

PETERSON, Z. *Pretexting*: social engineering's greatest weapon. *Infosecurity Magazine*, [S. l.], 2010. Disponível em: [Inserir link se houver]. Acesso em: [Inserir data de acesso].

SECURITY AFFAIRS. *Social Engineering*. [S. l.], 2023. Disponível em: [Inserir link se houver]. Acesso em: [Inserir data de acesso].