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

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

CURSO – DESENVOLVIMENTO DE SISTEMAS

PROFESSORA: Mizael

Aluno: Gustavo Zanini Marques Soares - 304

**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?
2. Qual a diferença entre PGP e GNU GPG?
3. O que é uma chave pública e uma chave privada no contexto do GPG?
4. Explique como funciona a criptografia assimétrica. Dê um exemplo de uso no cotidiano.
5. Explique como funciona a criptografia simétrica. Dê um exemplo de uso.
6. Quais são as vantagens e desvantagens da criptografia assimétrica em relação à simétrica?
7. Qual o papel do GPG na comunicação segura por e-mail?
8. O que é criptografia de disco? Cite dois softwares usados para isso e explique brevemente como funcionam.
9. Compare o BitLocker (Windows) e o FileVault (macOS). Quais suas semelhanças e diferenças?
10. O que significa criptografia de ponta a ponta em uma conversa por aplicativo de mensagem?
11. Qual a importância da criptografia de ponta a ponta em aplicativos como WhatsApp e Signal?
12. Cite dois riscos de armazenar dados importantes em um computador sem qualquer tipo de criptografia.
13. Como a criptografia ajuda a proteger dados em caso de roubo de notebook ou celular?
14. Qual a diferença entre o uso legítimo da criptografia e a criptografia usada em ataques de ransomware?
15. O ransomware criptografa os dados da vítima. Como essa técnica é diferente da criptografia usada por softwares como GPG ou BitLocker?

**Respostas:**

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

O Pretty Good Privacy (PGP) é um sistema de criptografia utilizado para proteger comunicações digitais, principalmente e-mails. Seu objetivo principal é garantir a confidencialidade, a integridade e a autenticidade das informações por meio da criptografia assimétrica e da assinatura digital (STALLINGS, 2021).

**2. Qual a diferença entre PGP e GNU GPG?**

O PGP é um software proprietário desenvolvido por Phil Zimmermann em 1991. Já o GNU Privacy Guard (GPG) é uma implementação livre e compatível com o padrão OpenPGP, permitindo a realização das mesmas funções criptográficas sem custos de licenciamento (KOCH, 2023).

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

No GPG, a chave pública é usada para criptografar mensagens, podendo ser compartilhada livremente. A chave privada, mantida em segredo pelo proprietário, é utilizada para descriptografar mensagens recebidas e assinar digitalmente documentos (STALLINGS, 2021).

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

A criptografia assimétrica utiliza um par de chaves — pública e privada — para proteger dados. Por exemplo, em um e-mail criptografado, o remetente usa a chave pública do destinatário para codificar a mensagem, que só poderá ser lida com a chave privada correspondente. Um exemplo cotidiano é o uso em transações bancárias online seguras.

**5. Explique como funciona a criptografia simétrica. Dê um exemplo de uso.**

Na criptografia simétrica, uma única chave é utilizada tanto para criptografar quanto para descriptografar dados. Um exemplo de uso é a proteção de arquivos compactados com senha (ZIP, RAR), onde a mesma senha é necessária para abrir o arquivo (TANENBAUM; WETHERALL, 2011).

**6. Quais são as vantagens e desvantagens da criptografia assimétrica em relação à simétrica?**

A principal vantagem da criptografia assimétrica é a eliminação da necessidade de trocar chaves secretas entre as partes. Entretanto, ela é mais lenta e consome mais recursos computacionais em comparação com a criptografia simétrica. Já a simétrica é mais rápida, porém exige métodos seguros para a troca da chave (STALLINGS, 2021).

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

O GPG assegura a confidencialidade e autenticidade das mensagens por meio da criptografia de conteúdo e da assinatura digital. Assim, garante que apenas o destinatário possa ler a mensagem e que o remetente possa ser autenticado com segurança.

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

Criptografia de disco é o processo de codificação de todos os dados armazenados em um disco rígido, tornando-os inacessíveis sem a chave ou senha correta. Dois softwares populares são:

**BitLocker (Windows)**: utiliza o módulo TPM para criptografar o disco de forma transparente ao usuário.

**VeraCrypt**: permite a criação de volumes criptografados ou a criptografia de discos inteiros, exigindo senha na inicialização.

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

Ambos realizam criptografia de disco completo, utilizando algoritmos robustos (como AES). O BitLocker se integra ao TPM e ao Active Directory, enquanto o FileVault utiliza a conta iCloud para recuperação de chave. A principal diferença está na integração com os respectivos sistemas operacionais e na forma de gerenciamento das chaves.

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

Criptografia de ponta a ponta significa que apenas o remetente e o destinatário podem ler as mensagens trocadas. Nem mesmo os servidores do aplicativo têm acesso ao conteúdo, pois a descriptografia só é possível nos dispositivos envolvidos (SCHNEIER, 2020).

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

Ela garante a privacidade e a segurança das conversas, protegendo contra interceptações por terceiros, inclusive pelo próprio serviço de mensagens. Isso é essencial para jornalistas, ativistas e qualquer cidadão preocupado com sua privacidade digital.

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

Os principais riscos são:

Acesso não autorizado por invasores ou em caso de roubo do equipamento;

Exposição de dados sensíveis, como informações financeiras e pessoais, comprometendo a privacidade e podendo levar a fraudes.

**13. Como a criptografia ajuda a proteger dados em caso de roubo de notebook ou celular?**

Mesmo que o dispositivo físico seja roubado, os dados permanecem inacessíveis sem a chave ou senha de descriptografia. Isso impede que o invasor leia ou copie os arquivos armazenados.

**14. Qual a diferença entre o uso legítimo da criptografia e a criptografia usada em ataques de ransomware?**

O uso legítimo da criptografia visa proteger dados contra acesso indevido, sendo autorizado e controlado pelo proprietário. Já no ransomware, a criptografia é aplicada maliciosamente por criminosos, que bloqueiam o acesso aos dados da vítima e exigem resgate para a liberação (CERT.br, 2024).

**15. O ransomware criptografa os dados da vítima. Como essa técnica é diferente da criptografia usada por softwares como GPG ou BitLocker?**

A principal diferença está no controle da chave. Em softwares legítimos como o GPG ou o BitLocker, o usuário possui e controla a chave. No ransomware, a chave de descriptografia fica em posse do criminoso, sendo negado o acesso ao usuário até o pagamento do resgate.

**Referências:**

STALLINGS, W. Cryptography and Network Security: Principles and Practice. 8. ed. Pearson, 2021.

TANENBAUM, A. S.; WETHERALL, D. J. Redes de Computadores. 5. ed. Pearson, 2011.

KOCH, W. The GNU Privacy Handbook. Free Software Foundation, 2023.

SCHNEIER, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company, 2020.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: https://www.cert.br. Acesso em: maio 2025.

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.

SECURITY AFFAIRS. *Social Engineering*. [S. l.], 2023.