IPSSI

criptografia

1. O que é Criptografia?
2. Como funciona a criptografia?
3. Quais as técnicas de criptografia mais comuns?
4. Cite exemplos de algoritmos de criptografia
5. Criptografia em trânsito versus em repouso: qual a diferença?
6. O que são dados criptografados de ponta a ponta?
7. Quais os usos mais populares da Criptografia e seus benefícios?

1.
Criptografia é um mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos e etc) ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem. É a conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados. A criptografia é um elemento fundamental da segurança de dados.

2.
Funciona enviando os dados originais (ou texto simples) por meio de um algoritmo (uma cifra), que criptografa os dados em texto cifrado. O texto resultante é ilegível, a menos que alguém use a chave de descriptografia correta para decodificá-lo.

3.

A criptografia é um conjunto de técnicas pensadas para proteger uma informação de modo que apenas o emissor e receptor consigam compreendê-la. É utilizada em comunicações digitais, como na troca de mensagens ou em pagamentos online.

- Chave simétrica

A chave simétrica é o modelo mais comum e simples. Nela, uma mesma chave é utilizada tanto pelo emissor como pelo receptor da mensagem – ou seja, ela é usada tanto para a codificação como para a descodificação dos dados.

- DES

Esse é um dos modelos mais básicos, tendo sido um dos primeiros a ser criados e implementados. Consequentemente, é um dos mais difundidos mundialmente, pois fornece uma proteção básica de apenas cerca de 56 bits, oferecendo até 72 quatrilhões de combinações.

- IDEA

Criada em 1991, essa é uma chave simétrica que opera em blocos de informações de 64 bits e utiliza chaves de 128 bits.

- SAFER

Nesse modelo, a criptografia é feita em blocos de 64 bits. Não raro, o usuário poderá encontrá-la pelo nome de SAFER SK-64.

- AES

É um dos algoritmos de criptografia mais seguros da atualidade, sendo utilizado até mesmo pelo Governo dos Estados Unidos e, também, por diversas organizações de segurança.

- Chave assimétrica

Também conhecida como «chave pública», trabalha tanto no modo privado quanto no público. No primeiro, a chave é secreta.

4.

Em criptografia existem dois tipos básicos de algoritmos: os de chave simétrica e assimétrica. Os primeiros utilizam uma única chave para cifrar e decifrar os dados, enquanto os segundos adotam par de chaves, sendo uma para cifrar e a outra para decifrar.

5.
Se você enviar mensagens não encriptadas (ou seja, se não criptografar seu dados em trânsito) por meio de um dispositivo móvel criptografado (ou seja, se criptografar seus dados em repouso), estas mensagens ainda vão estar vulneráveis a quem quiser bisbilhotar sua rede ou à interceptação por parte de governos, provedores ou adversários com habilidades técnicas. No entanto, o registro das mensagens que ficou no seu dispositivo móvel estará protegido contra aquelas pessoas que tiverem acesso físico a ele, caso elas não saibam a senha.
Por outro lado, se você enviar mensagens com encriptação ponta-a-ponta (ou seja, se criptografar seus dados em trânsito) por meio de um dispositivo não criptografado (ou seja, se não criptografar seus dados em repouso), estas mensagens vão ser impermeáveis a qualquer pessoa que esteja bisbilhotando ou espionando a sua rede. No entanto, se alguém tiver acesso físico ao seu dispositivo móvel, também será possível ter acesso às mensagens e lê-las.

6.
A criptografia de ponta a ponta é um método de segurança que protege a comunicação. Com ela, ninguém, nem mesmo o Google ou terceiros, pode ler as mensagens qualificadas enquanto elas são transmitidas entre seu smartphone e o smartphone do destinatário.

7.
A criptografia de dados também ajuda a resguardar arquivos de acesso indevido. O que é muito útil para casos de roubo de máquinas e dispositivos ou até mesmo de tentativa de vazamento de informações por hackers. Em smartphones e em computadores, você até consegue apagar aquilo que precisa remotamente. As principais aplicações da criptografia no mundo moderno: criptomoedas, uso pessoal e empresarial, trocas de informações, áreas de segurança, assinatura digital de documentos, criptografia simples (SSL), criptografia para e-mails, certificado codesign.

REFERÊNCIAS:

- https://www.avast.com/pt-br/c-encryption#:~:text=autorizado%20dos%20dados.-,Como%20a%20criptografia%20funciona%3F,descriptografia%20correta%20para%20decodific%C3%A1%2Dlo.
- https://www.kaspersky.com.br/resource-center/definitions/encryption
- https://www.significados.com.br/criptografia/
- https://ssd.eff.org/pt-br/module/o-que-%C3%A9-criptografia#:~:text=Isto%20garante%20que%20suas%20conversas,n%C3%A3o%20ir%C3%A1%20criptografar%20os%20metadados.
- https://docs.aws.amazon.com/pt_br/emr/latest/ManagementGuide/emr-data-encryption.html
- https://blog.rebel.com.br/criptografia-de-dados-saiba-quais-sao-suas-principais-aplicacoes-e-onde-usa-la/
- https://blog.tylermangroup.com/3-beneficios-da-criptografia-de-dados-na-empresa/