**Ficha 5**

**Aluno:** Adilson Alves Neves Junior

1. (\*) O que é confidencialidade dos dados em Internet das Coisas.

R: A confidencialidade dos dados na Internet das Coisas (IoT) se refere à proteção dos dados para garantir que eles sejam acessíveis apenas por entidades autorizadas. Isso envolve a criptografia dos dados durante a transmissão e armazenamento, autenticação dos dispositivos para garantir sua legitimidade, controle de acesso para limitar o acesso apenas a usuários autorizados, segurança de rede para evitar ataques indesejados, atualizações regulares de segurança e proteção física dos dispositivos. Essas medidas ajudam a preservar a privacidade dos usuários, proteger informações sensíveis e manter a integridade dos sistemas IoT.

1. (\*) O que é integridade dos dados em Internet das Coisas.

R: A integridade dos dados na Internet das Coisas (IoT) refere-se à garantia de que os dados permaneçam completos, precisos e não sejam alterados sem autorização. Isso é alcançado por meio de mecanismos de detecção de alterações, assinaturas digitais, controles de acesso, monitoramento de intrusões, segurança de rede e atualizações de segurança. Essas medidas ajudam a assegurar que os dados da IoT sejam confiáveis, protegendo a precisão das informações e evitando alterações não autorizadas.

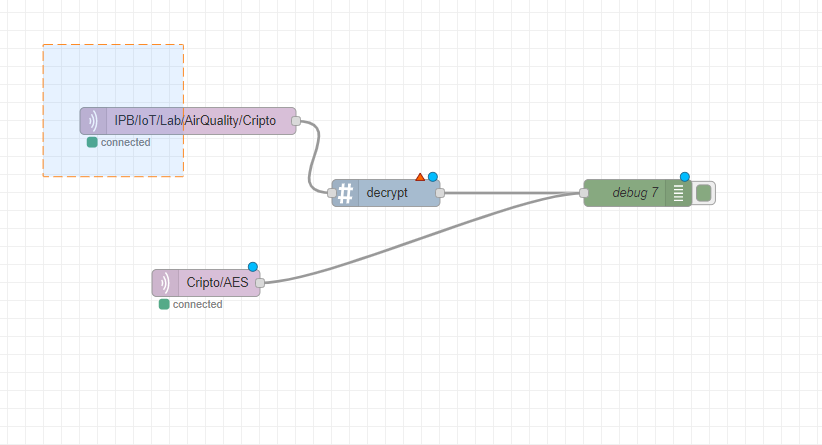
1. (\*) O que é disponibilidade dos dados em Internet das Coisas.

R: A disponibilidade dos dados na Internet das Coisas (IoT) refere-se à capacidade de acessar e utilizar os dados dos dispositivos conectados de forma confiável e contínua. Para garantir a disponibilidade dos dados na IoT, são adotadas medidas como infraestrutura robusta, backup e recuperação de dados, tolerância a falhas, monitoramento contínuo, segurança cibernética e atualizações de software. Essas medidas asseguram que os dados estejam disponíveis quando necessários, evitando interrupções e garantindo o bom funcionamento dos sistemas conectados.

**2. (\*)** Utilizando a biblioteca do Node-RED “Node-RED-contrib-crypto-js”, faça: Subscreva ao tópico MQTT (IPB/IoT/Lab/AirQuality/Cripto) e verifique se é possível interpretar os dados que obtém. Subscreva ao Tópico (Cripto/AES) para descobrir qual a secret-key está sendo utilizada para criptografar a mensagem. Utilize o node do Node-RED decrypt com o algoritmo AES para analisar o valor correto. Apresente os valores criptografados e descriptografados bem como a secret-key obtida. Confira se o valor corresponde ao dado obtido do tópico (IPB/IoT/Lab/AirQuality)

**R:** Utilizando a biblioteca que mensagem que vem criptografada vai ser descripta a partir da key que vem do topo (Cripto/AES), inserido manualmente no decrypt

**.**

****

**3. (\*)** Utilizando a biblioteca do Node-RED “sense-rsa”, faça: Crie uma chave publica e uma chave privada. Então, criptografe e descriptografe a mensagem. Qual a função da chave pública? Qual a função da chave privada? Porque é uma abordagem relevante em Internet das Coisas?

R: A criptografia assimétrica envolve o uso de um par de chaves: uma chave pública para criptografar e uma chave privada para descriptografar. A chave pública é compartilhada amplamente e usada para criptografar os dados, enquanto a chave privada é mantida em segredo e usada para descriptografar. Essa abordagem é relevante na IoT para garantir a segurança e autenticidade das comunicações entre dispositivos.

