Segurança na Internet das Coisas

Ficha 5

Assunto: Segurança | MQTT

ALUNOS:

A48530 -Diogo Brandão Ferreira

A48542-José Nuno Marinho Carvalho

Segurança na Internet das Coisas

1)

a) O que é confidencialidade dos dados em Internet das Coisas.

A confidencialidade dos dados está relacionada com a privacidade dos mesmos. Estes devem ser acedidos apenas por entidades autorizadas. No caso de um protocolo de troca de mensagens, como por exemplo o MQTT, o subscriber só poderia aceder aos dados caso tivesse autorização para tal.

b) O que é integridade dos dados em Internet das Coisas.

Integridade dos dados consiste na manutenção e garantia da consistência de dados durante todo o ciclo de vida dos mesmos. Desde a sua conceção até à sua análise, garantindo que estes não são indevidamente alterados.

c) O que é disponibilidade em Internet das Coisas

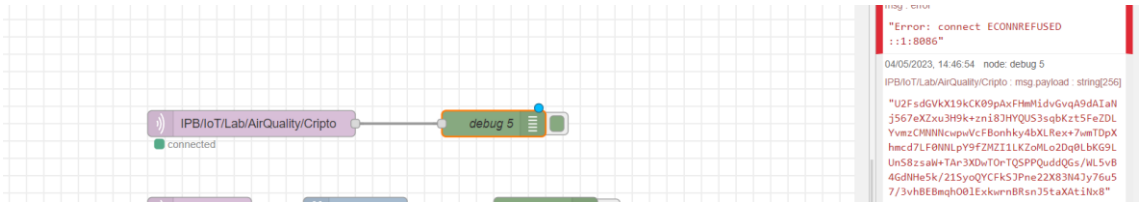
Disponibilidade de dados refere-se à acessibilidade que se tem dos mesmos. Os dados devem estar disponíveis a todo o momento para serem consultados. Em caso de falhas ou ataques, os dados devem ser recuperados rapidamente.

Dados. Criptografados

2)

- **Subscreva ao tópico MQTT (IPB/IoT/Lab/AirQuality/Cripto) e verifique se é possível interpretar os dados que obtém:**

Como se pode visualizar pela imagem, a mensagem aparece criptografada:

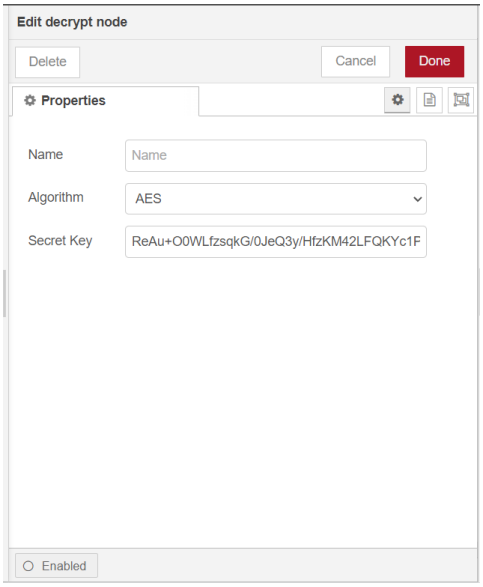


- **Subscreva ao Tópico (Cripto/AES) para descobrir qual a secret-key está sendo utilizada para criptografar a mensagem:**

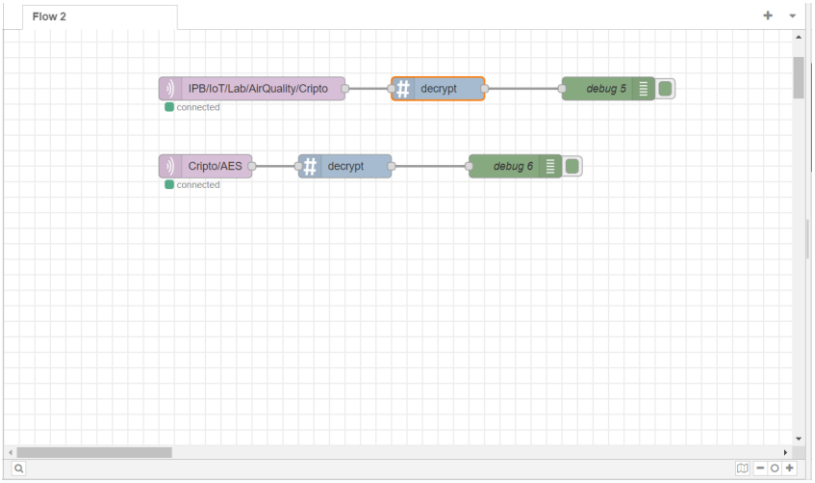
Com a chave fornecida pelo tópico “Cripto/AES” conseguimos finalmente desencriptar a mensagem anterior.

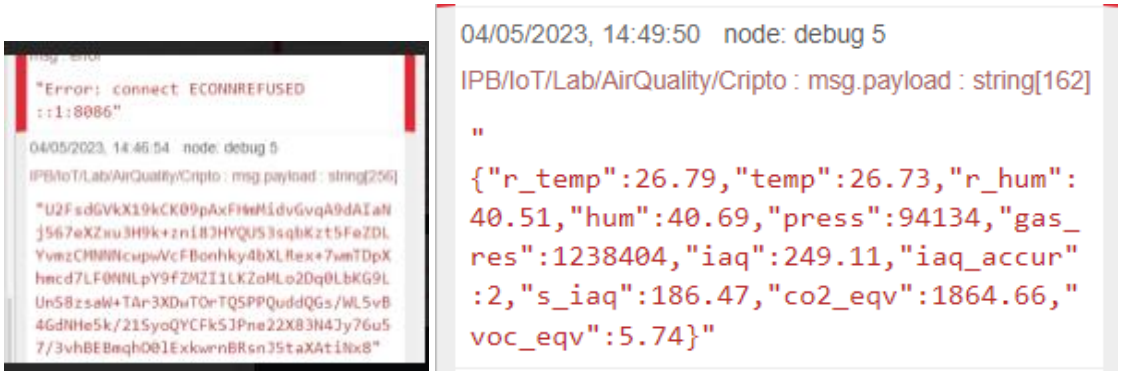
- **Utilize o node do Node-RED decrypt com o algoritmo AES para analisar o valor:**

Propriedades colocadas no node “decrypt”:



- **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):**





3. 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?

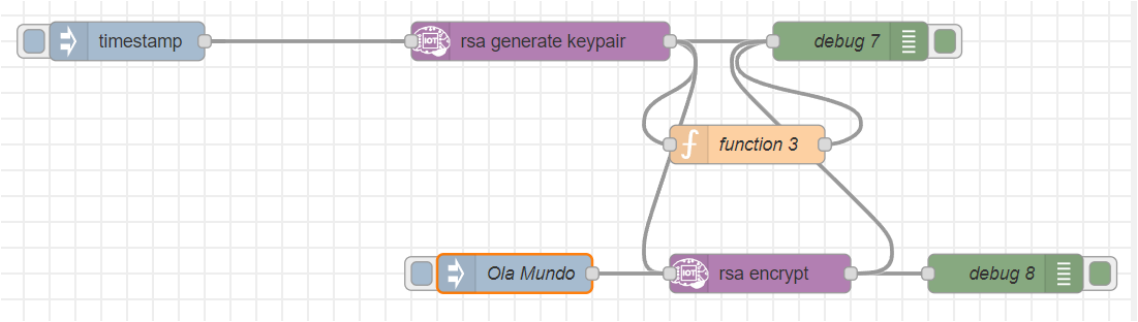
A chave pública e privada são componentes essenciais da criptografia de chave assimétrica, que é uma técnica amplamente utilizada para proteger a segurança de dados em sistemas de Internet das Coisas (IoT).

A chave pública é usada para criptografar informações antes de serem enviadas, garantindo que somente o destinatário pretendido possa descriptografá-las usando a chave privada correspondente. Por sua vez, a chave privada é usada para descriptografar informações recebidas, garantindo que apenas o destinatário pretendido possa acessar essas informações.

Esta abordagem é extremamente importante em sistemas de IoT, pois os dispositivos conectados geralmente lidam com informações críticas, como dados de saúde, informações financeiras e informações pessoais. A criptografia de chave assimétrica ajuda a garantir que essas informações sejam transmitidas com segurança, sem o risco de que terceiros mal-intencionados possam interceptá-las ou acessá-las indevidamente.

Em resumo, a criptografia de chave assimétrica com chaves públicas e privadas é fundamental para garantir a confidencialidade e segurança dos dados em sistemas de IoT, ajudando a proteger a privacidade e a segurança dos usuários finais.

De seguida, com a chave pública gerada anteriormente encriptámos a mensagem “Olá Mundo”:



Por último desencriptamos a mensagem através do node “rsa decrypt”: