

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

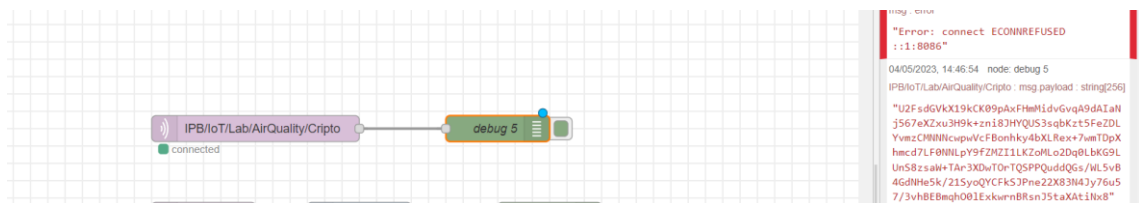
Disponibilidade de dados refere-se à acessibilidade que se tem dos mesmos. Os dados devem estar disponíveis a todo o momento para serem consultados. Em caso de falhas ou ataques, os dados devem ser recuperados rapidamente.

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:

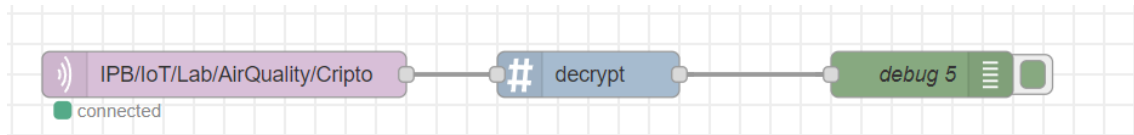


- **Subscreva ao Tópico (Cripto/AES) para descobrir qual a secret-key está sendo utilizada para criptografar a mensagem:**



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

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



Propriedades colocadas no node “decrypt”:

Edit decrypt node

Delete Cancel Done

Properties

Name: Name

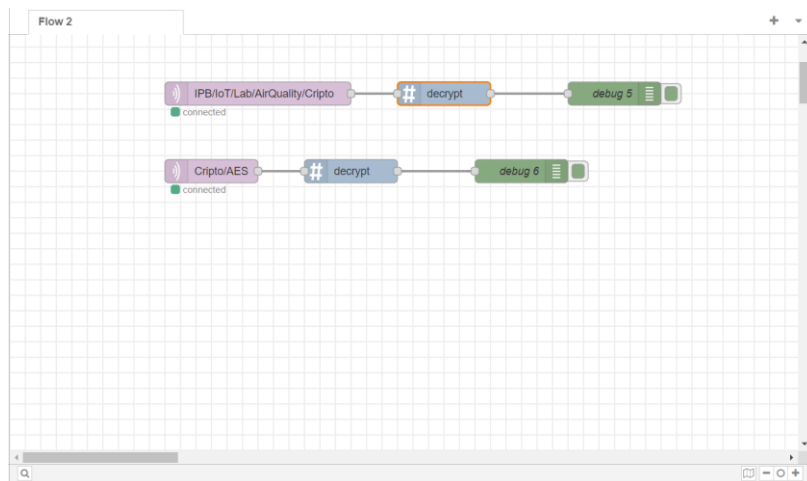
Algorithm: AES

Secret Key: ReAu+O0WLFzsqkG/0JeQ3y/HfzKM42LFQKYc1F

Enabled

```
04/05/2023, 14:49:50 node: debug 5
IPB/IoT/Lab/AirQuality/Cripto : msg.payload : string[162]
"
{"r_temp":26.79,"temp":26.73,"r_hum":
40.51,"hum":40.69,"press":94134,"gas_
res":1238404,"iaq":249.11,"iaq_accu
r":2,"s_iaq":186.47,"co2_eqv":1864.66,"
voc_eqv":5.74}"
```

- 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):



```

msg - error
"Error: connect ECONNREFUSED
::1:8086"

04/05/2023, 14:46:54 node: debug 5
IPB/IoT/Lab/AirQuality/Cripto : msg.payload : string[256]
"U2FsdGVkX19kCK09pAxFmM1dvGvqA9dAIaN
j567eXZnu3H9k+znI83HYQU53sqbKzt5FeZDL
YvmzCHNNncupwVcFBonhky4bXlRex+7wnTDpX
hmc7LF0NnLpY9fZM2I1LKZoHLo2Dq0LbKG9L
Un58zsaW+TAr3XDwT0rTQ5PPQddQGs/WL5vB
4GdNHe5k/21SyoQYCFk5JPne22X83N4Jy76u5
7/3vh8EBeqh001ExkwnnBRcn35taXAtiNx8"

```

```

04/05/2023, 14:49:50 node: debug 5
IPB/IoT/Lab/AirQuality/Cripto : msg.payload : string[162]
"
{"r_temp":26.79,"temp":26.73,"r_hum":
40.51,"hum":40.69,"press":94134,"gas_
res":1238404,"iaq":249.11,"iaq_accu
r":2,"s_iaq":186.47,"co2_eqv":1864.66,"
voc_eqv":5.74}"

```

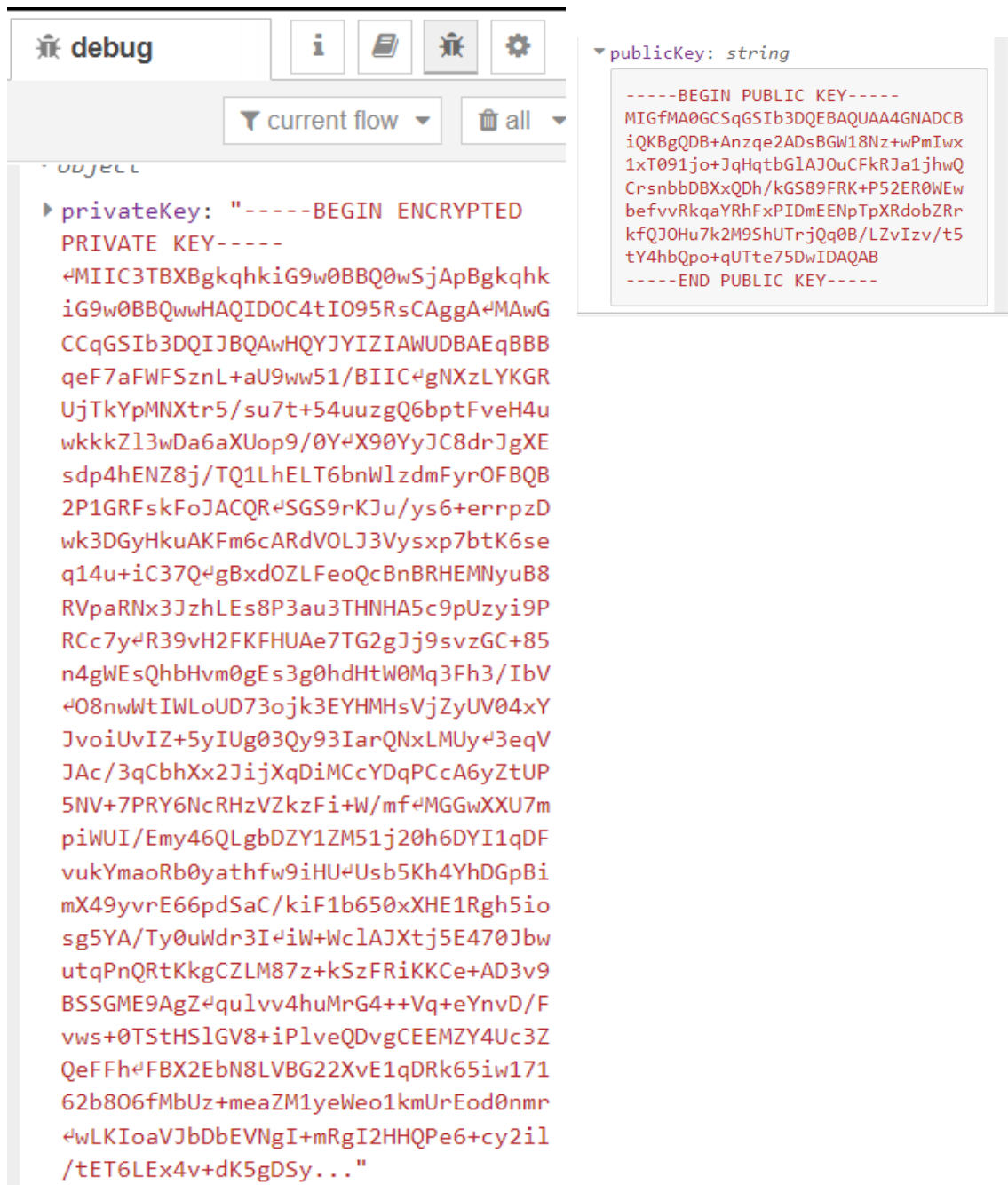
3. Crie uma chave pública e uma chave privada. Então, criptografe e descriptografe a mensagem. Qual a função da chave pública? Qual a função da chave privada? Porque é uma abordagem relevante em Internet das Coisas?

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).

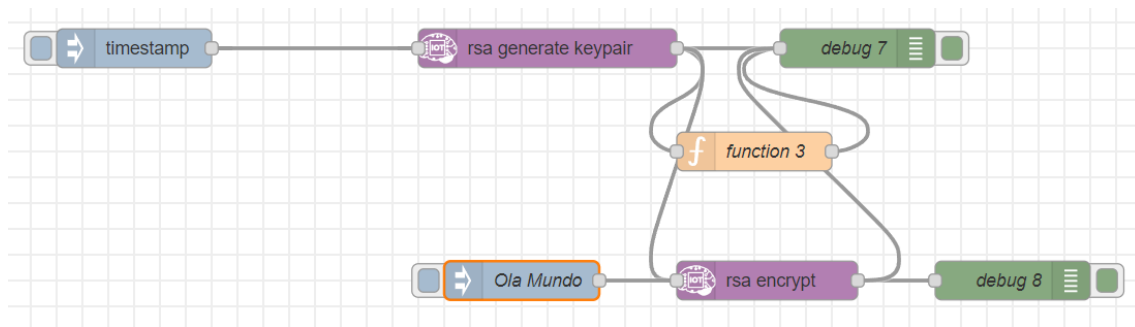
A chave pública é usada para criptografar informações antes de serem enviadas, garantindo que somente o destinatário pretendido possa descriptografá-las usando a chave privada correspondente. Por sua vez, a chave privada é usada para descriptografar informações recebidas, garantindo que apenas o destinatário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



```
04/05/2023, 15:20:03 node: debug 8
```

```
msg.payload : string[172]
```

```
"FE7KQDjcBKiYYpsIqC0/l+oFW0y+ie5SxNl4Vf  
uDDiO80tdQuHGlhI8/kYjiPGk7+SK1omYL6VS+x  
Ju/ctGjC7MF3k/6Jm1BDZIVF4skxuuI0pagUzVY  
IZIuxEmuDEoDcfdPEjUEvz53zX7obrI7rodDo1i  
eMkcgN1CxAXiXsM="
```

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

```
04/05/2023, 15:41:51 node: rsa decrypt
```

```
msg.payload : string[9]
```

```
"Olá Mundo"
```