Q PROJECT - TECHEQUATION.ORG

FRIDAY WRAP UP & UPDATES

Week 2 Part 3 | Presented by Solomon Denning

TODAY'S OVERVIEW

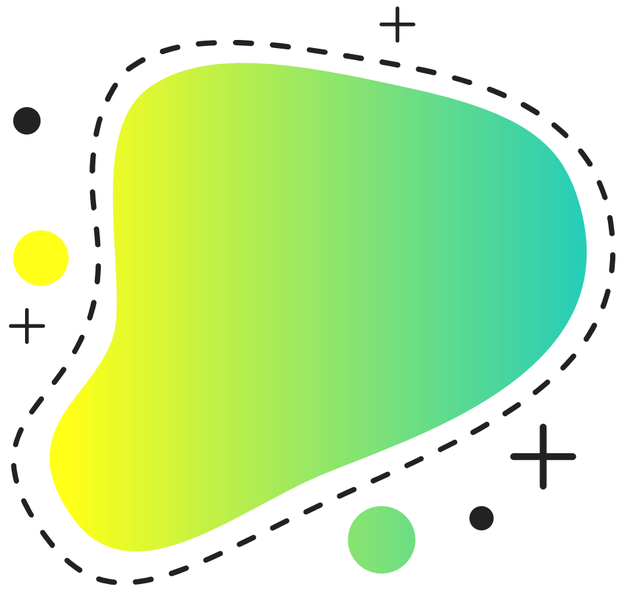
Check your Emails

Encryption

LoRaWAN Security

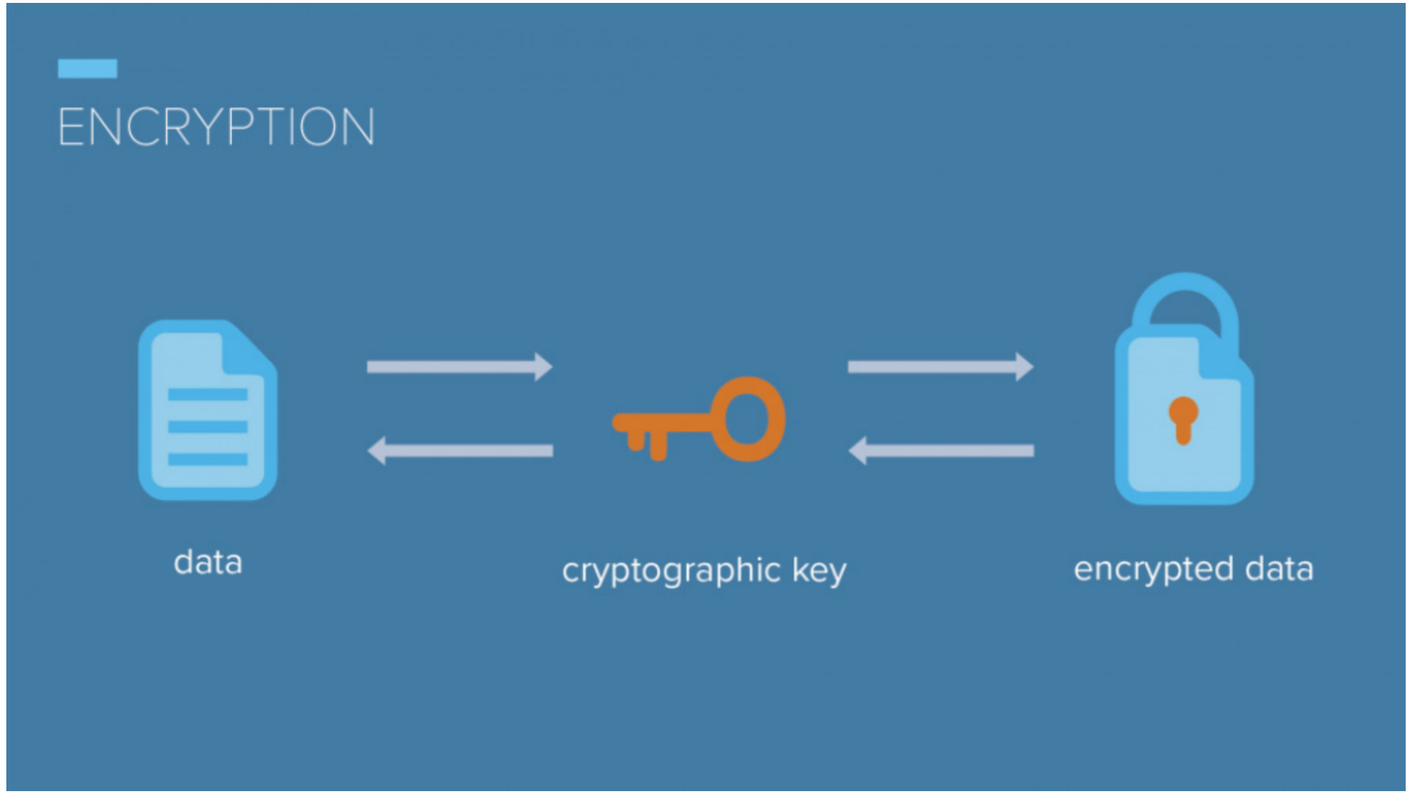
Questions

ENCRYPTION



Encoding and Decoding

Encryption is the process of encoding data into a non-readable form. The user that receives the message also knows how to decoded the message.



Encryption Key

Keys are a string of random bits used to scramble and unscramble data.

Encryption using a longer key length is generally more secure.

PRIVATE & PUBLIC KEYS

Private Key (Symmetric Key)

The two users share the same key, one key encodes and decodes.
LoraWAN security uses this type of encryption key.
The common key length for private key encryption is 128 bits.

Public Key

One key is public knowledge for everyone to see, used to encode.
A private key for the end user is used to decode.
The common key length for public key encryption is 2048 bits

LORAWAN SECURITY

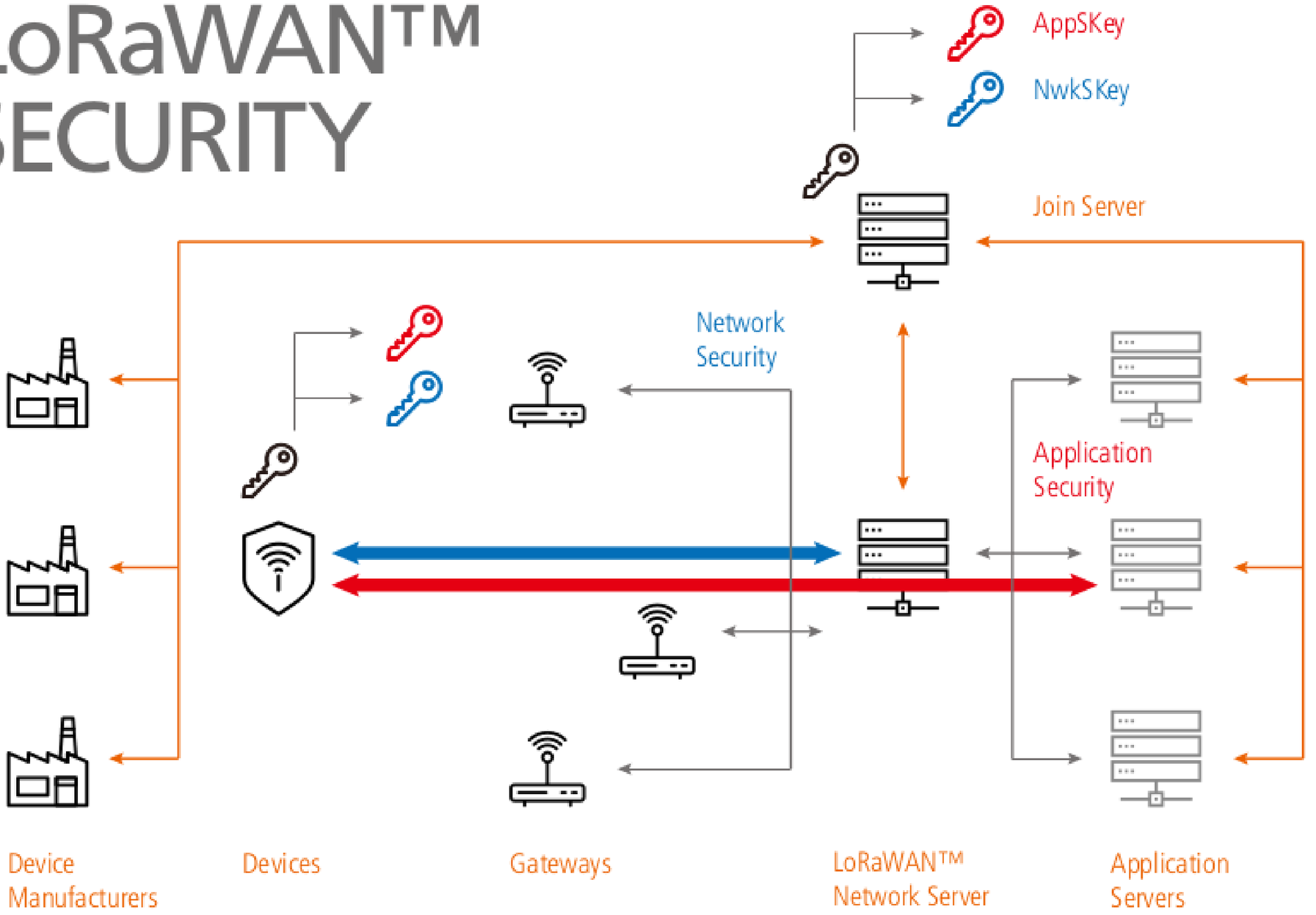
AES-128 bit Encryption

More details later.

End-to-End Encryption

No point in data transfer where data is not encrypted

LoRaWAN™ SECURITY



AES - ADVANCED ENCRYPTION STANDARD

LoRaWAN

LoRaWAN uses the AES-128 encryption, which means it uses a 128 bit long key.

Symmetric Key

AES uses a symmetric encryption key. Server and End Device use same 128 bit key.

Very Secure

AES has never been cracked. Brute-forcing can take years.

QUESTIONS?

SOURCES

LoRaWAN Security

Encryption

AES-128