Cryptography

## Course for master's degree in EDGE COMPUTING

Michał Melosik, PhD

Scope

1. Introduction

2. Randomness, random number generators

3. Block ciphers - AES, encryption modes of operation

4. Stream cyphers, hash function

6. Asymmetric cryptography - RSA, ECC/ECDS

7. Security architecture

8. CA & Certificates

9. HW security

10. Supply chain security

11. Practical aspects of cryptography

12. Security and ethics

EDGE COMPUTING
Cryptography in EC
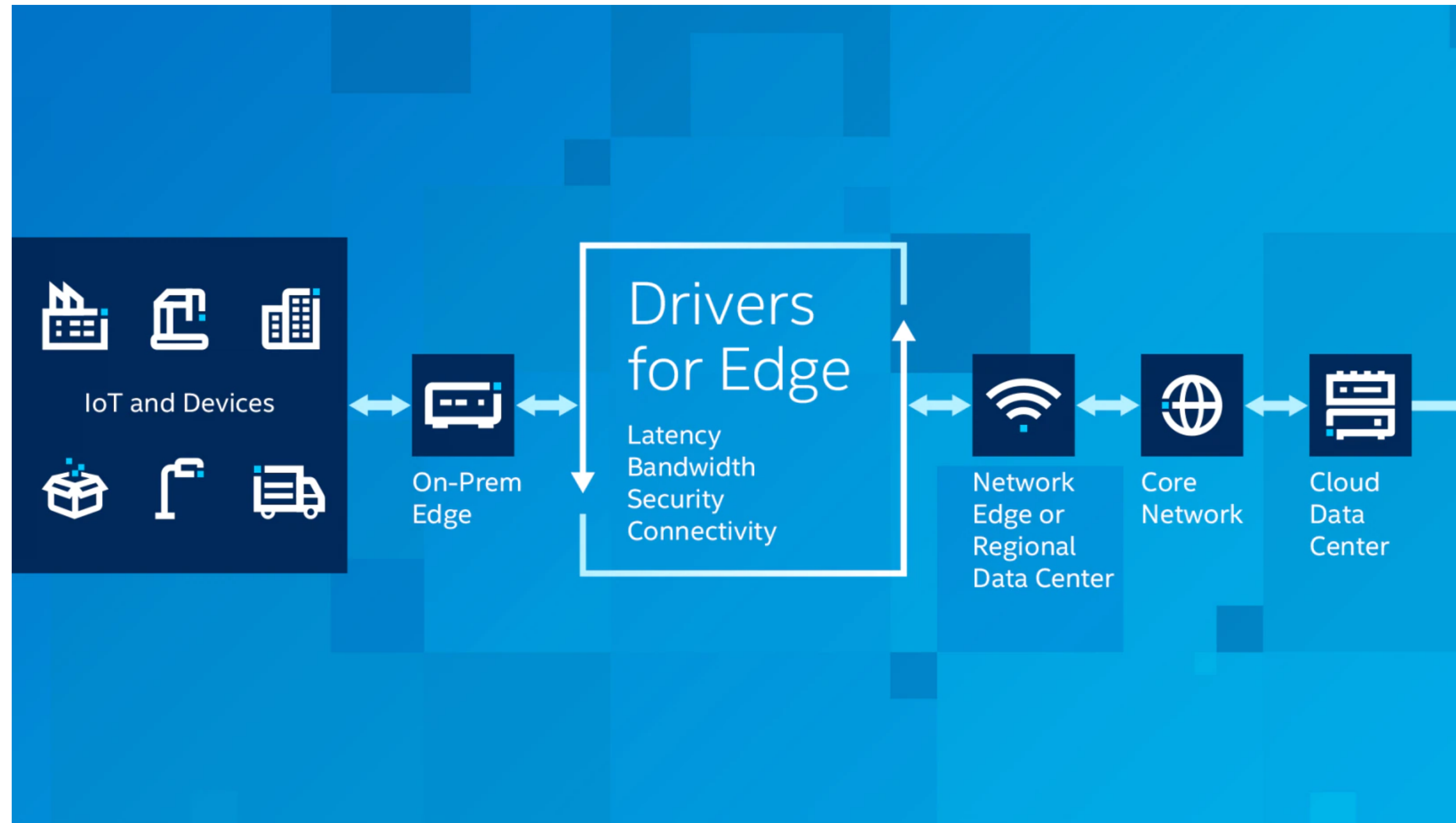
Cryptology

As a science

Cryptology is the science of encryption and ensuring data security.

There are two main areas in cryptology:

- cryptography (cryptographic cipher systems)

- cryptanalysis (techniques for breaking ciphers)

Openness and secretness of security methods

What's the most important thing in the practice of cryptographic solutions?

- security through obscurity

- full disclosure

- responsible disclosure