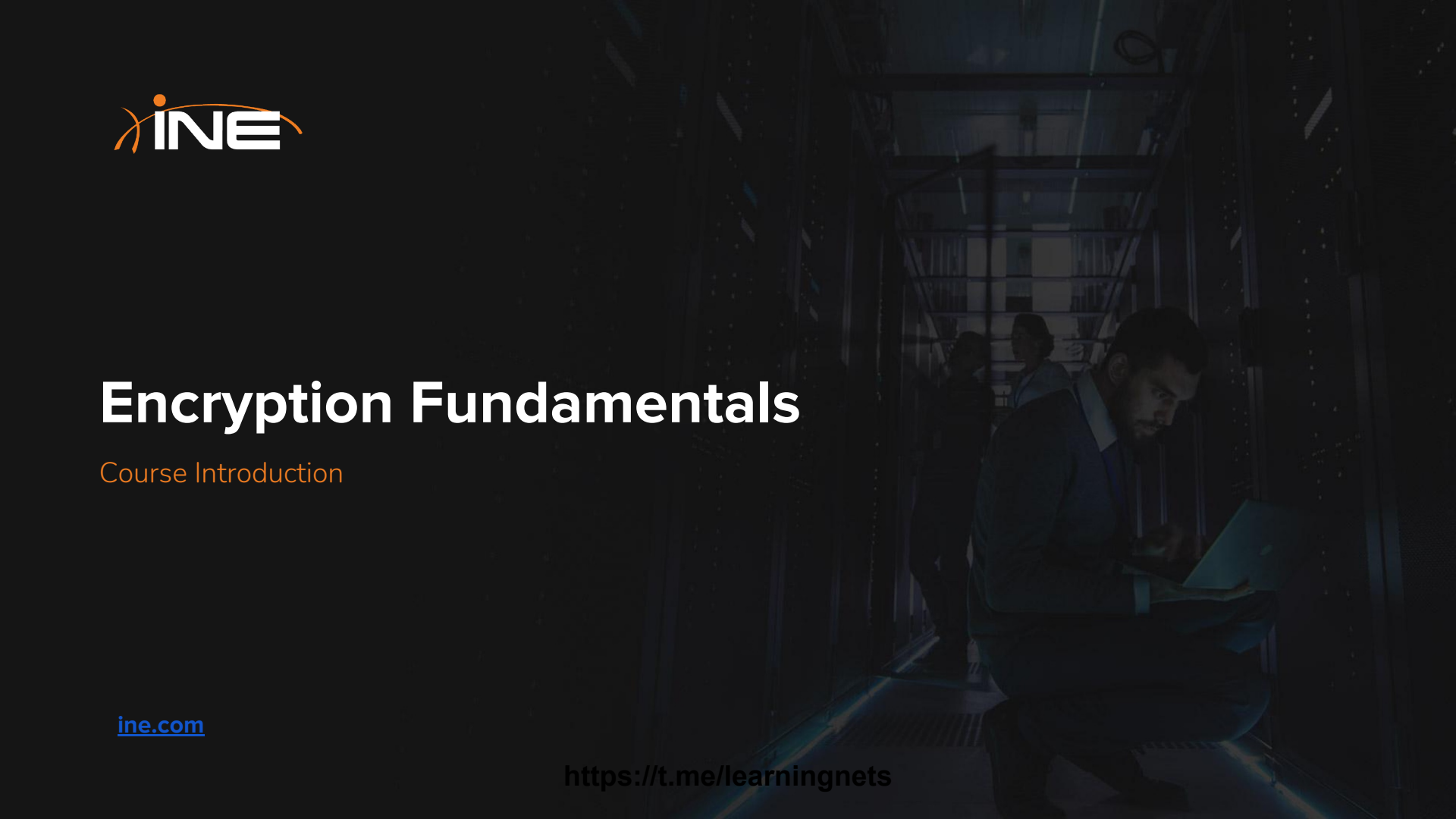


Encryption Fundamentals

Course Introduction

ine.com

Piotr Kaluzny

CCIE #25665

pkaluzny@ine.com

linkedin.com/in/piotrkaluzny

CCIE Security

Course Prerequisites

+ Elementary mathematics

Course Overview

- Module 1 Introduction to Encryption
- Module 2 Symmetric Encryption
- Module 3 Asymmetric Encryption
- Module 4 Data Encryption Standard
- Module 5 Advanced Encryption Standard
- Module 6 Asymmetric Algorithms

Encryption Fundamentals

Introduction to Encryption

ine.com

Module Overview

- Learning objectives
- Cryptography vs encryption
- Encryption characteristics
- Literature

Learning Objectives

- At the conclusion of this course you should be able to:
  - Define encryption
  - Explain the differences between the different encryption types
  - Describe encryption algorithms

Cryptography vs Encryption

- Cryptography is a science of protecting information & communications
  - Provides confidentiality, integrity, authentication & more
    - Encryption is just one of the techniques used to secure data

- Encryption is a process of concealing information
  - Converts plaintext into ciphertext
    - Plaintext (cleartext) refers to the original data
    - Ciphertext refers to the "hidden" data
      - Nonessential/meaningless to any third party
  - Decryption is the reverse of the encryption

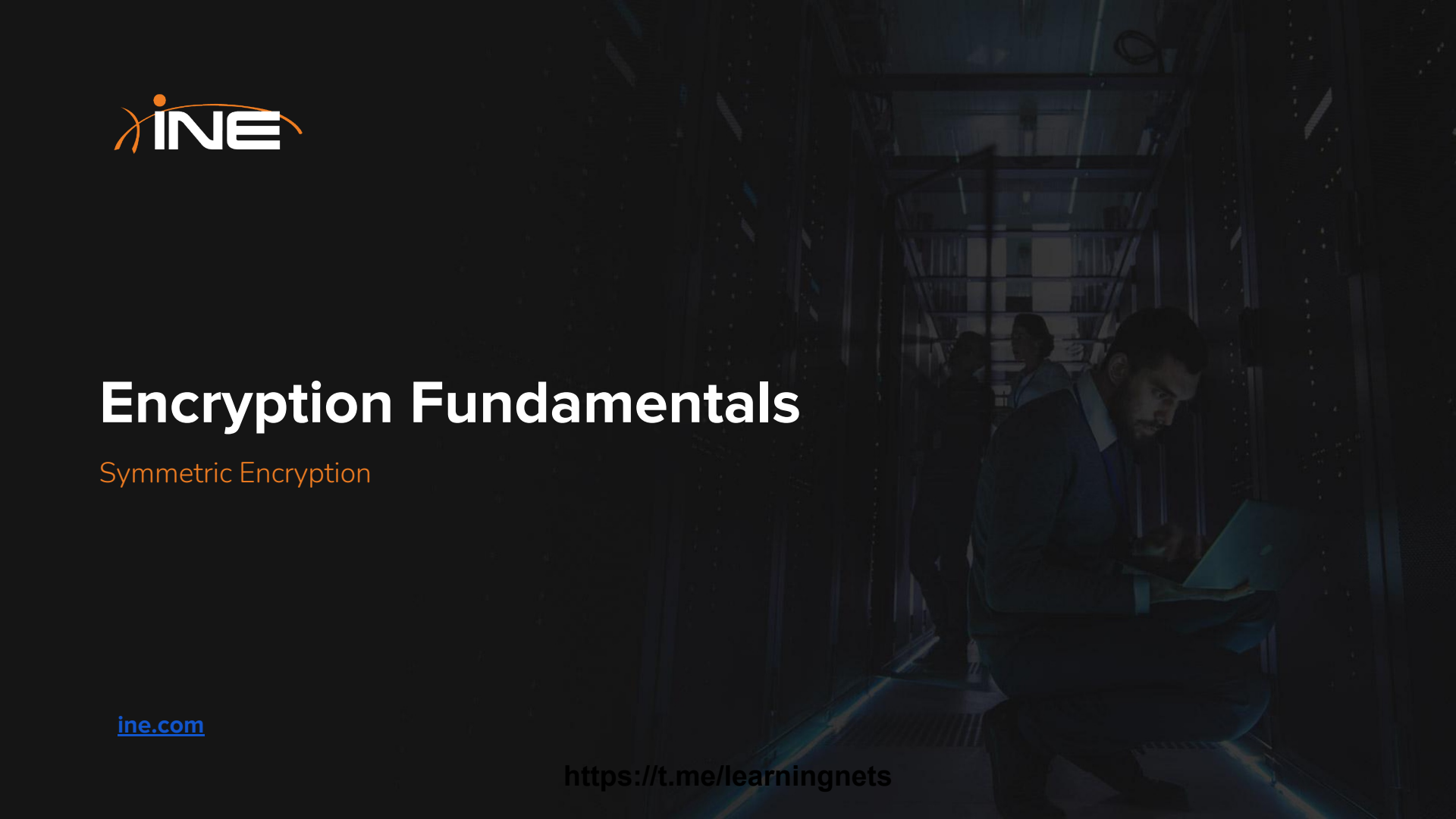
More on Encryption

- Encryption relies upon two basic components
  - Algorithm
    - Also known as Cipher
  - Key(s)
    - Set of characters (bits)

- Encryption Types
  - Symmetric
  - Asymmetric

Literature

- Applied Cryptography : Protocols, Algorithms, and Source Code in C
  - Bruce Schneier
    - https://www.amazon.com/Applied-Cryptography-Protocols-Algorithms-Source/dp/0471117099



Encryption Fundamentals

Symmetric Encryption

ine.com

Module Overview

- Overview
- Algorithm types & modes

Symmetric Encryption Overview

- Symmetric encryption uses a single key that is shared
  - Static vs Dynamic

- Security Factors
  - Algorithm & key length
    - For equally secure algorithms, the longer the key is, the more secure is the encryption
      - E.g. 8-bit key -> 256 possibilities
    - The underlying algorithm can be Stream or Block Cipher
      - Bits vs blocks
      - See https://www.convertbinary.com/

Stream Ciphers

- Rivest Cipher 4 (RC4)
  - Used with wireless encryption (WEP, WPA), BitTorrent, TLS, and more
  - Deemed insecure
    - Explicitly prohibited for TLS (see RFC 7465)

- Software Encryption Algorithm (SEAL)
  - Uses a 160-bit encryption key
  - Requires less CPU cycles than other software-based algorithms

Block Ciphers

- Data Encryption Standard (DES)
  - Avoid at all cost (56-bit key)
- Triple DES (3DES)
  - Legacy (168 bit key)
- Advanced Encryption Standard (AES)
  - Deemed a secure cryptographic standard available since 2002
  - Deployed with 128, 192 or 256 bit keys

Block Algorithm Modes

- Block Algorithms work in certain modes of operation
  - Control data processing and overall security

- Cipher Block Chaining (CBC)
  - Uses XOR to prevent two identical messages result in the same ciphertext
    - XORs plaintext with the previous ciphertext before encrypting it
      - First plaintext is XORed with random data
        - Initialization Vector (IV)
  - Performs poorly at high data rates

Block Algorithm Modes

- Counter Mode (CTR)
  - Makes use of a sequence number as an input to encryption
    - Sometimes combined with a nonce
  - Works well in high-speed implementations

- Galois/Counter Mode (GCM)
  - Provides encryption AND data origin authentication
  - Fast and efficient
  - Also offers authentication-only variant
    - Galois Message Authentication Code (GMAC)

Encryption Fundamentals

Asymmetric Encryption

ine.com

Module Overview

- Overview
- Asymmetric algorithm examples

Asymmetric Encryption Overview

- Involves two separate (but related) keys : “public” and “private”
  - Public key is „open”, private key must be kept secret

- Asymmetric encryption is performed with a public key
  - Anyone can do the encryption
    - No need for a secure channel and key exchange
      - Only the private key owner can decrypt the message
  - Slower and more CPU intensive than Conventional Encryption

Asymmetric Algorithm Examples

- Rivest Shamir Adelman (RSA)
  - Different variants : 512, 768, 1024, 2048 and 4096 bits
- Digital Signature Algorithm (DSA)
  - US Federal Government standard very similar to RSA
- Diffie-Hellman (DH)
  - A secure method of exchanging keys over public channels
  - Different groups (1, 2, 5, 14, 15) represent different key lengths

Encryption Fundamentals

Data Encryption Standard (DES)

ine.com

Module Overview

+ Overview
+ Encryption scheme
+ 3DES
+ DES today

Data Encryption Standard (DES) Overview

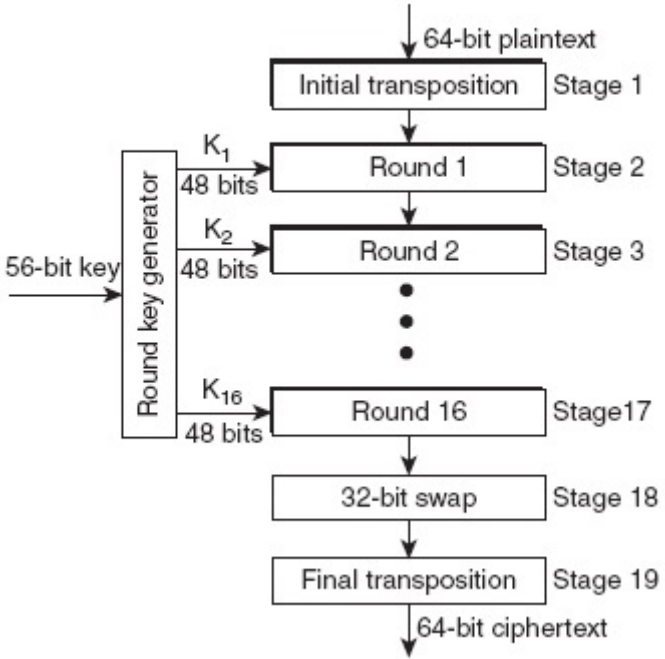
- Symmetric-key block cipher developed at IBM
  - NSA-approved and published in late 70s
  - Adopted by US government and various security products

- General Mechanics
  - Works on 64-bit blocks of data
    - Smaller blocks are "padded"
  - Uses a 56-bit key to derive a 64-bit output
    - Parity bits are dropped
  - Decryption follows a process reverse to encryption

Encryption Structure

- A single DES "cycle" consists of 19 stages
  - Initial transposition
    - Straight keyless permutations of the 64-bit data block
  - Encryption rounds (16)
    - The Feistel Function (F)
      - Splits 64-bit data into two 32-bit halves
      - Each round uses a different 48-bit round key derived from the 56-bit general (cipher) key & round key generator
  - Swap function
    - Swaps the two final 32-bit halves
  - Final transposition
    - Inverse of the initial transposition

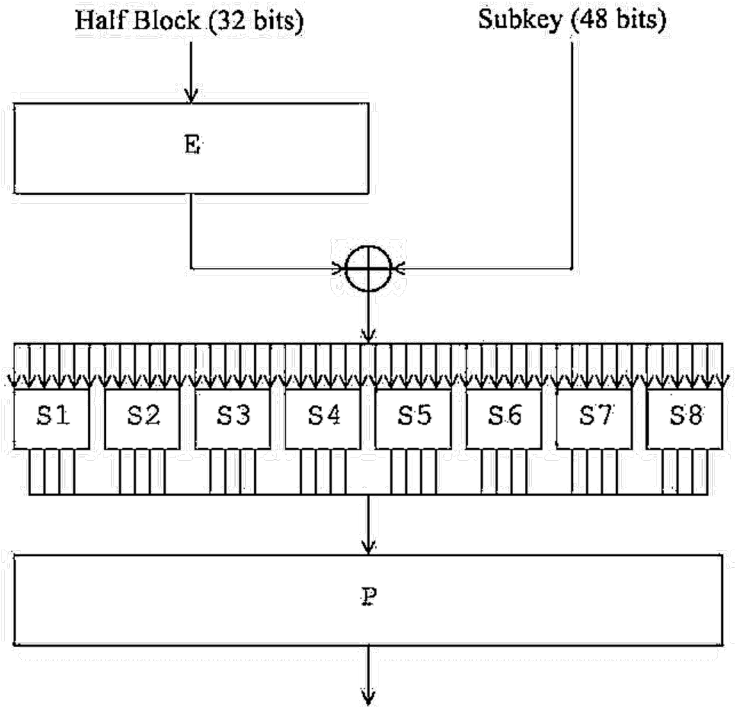
Encryption Structure



Encryption Function

- Each encryption (F) round comprises four steps
  - Expansion P-box
    - Expands the rightmost 32 data bits to 48 bits to match the round key
  - XOR
    - Bitwise XOR (48 bits) on the data & round key
  - S-boxes
    - Substitution "shrinks" the 48-bit XOR output to 32 bits
  - Straight P-box
    - Permutes the 32-bit S-box output to produce the "final" 32 bits
      - These bits will be XORed with the first half of the data (leftmost 32 bits)
        - Makes the new second half
        - The original second half is made the new first half

Encryption Function



Triple DES (3DES)

- DES quickly became insecure due to increasing computational power
  - The new algorithm - 3DES - runs DES three times
    - Encryption (k1) - decryption (k2) - encryption (k3)
      - The keys "add up" to 168 bits

- 3DES Variants
  - 3TDEA
    - Different keys
  - 2TDEA
    - Keys k1 & k3 are the same
  - Identical keys

DES Today

- Major security vulnerabilities have been found in DES and 3DES in 2016
  - DES became obsolete in early 2000s
  - NIST has deprecated the most secure 3DES variant (3TDEA) by 2023

Encryption Fundamentals

Advanced Encryption Standard (AES)

ine.com

Module Overview

+ Overview
+ Encryption scheme

Advanced Encryption Standard (AES) Overview

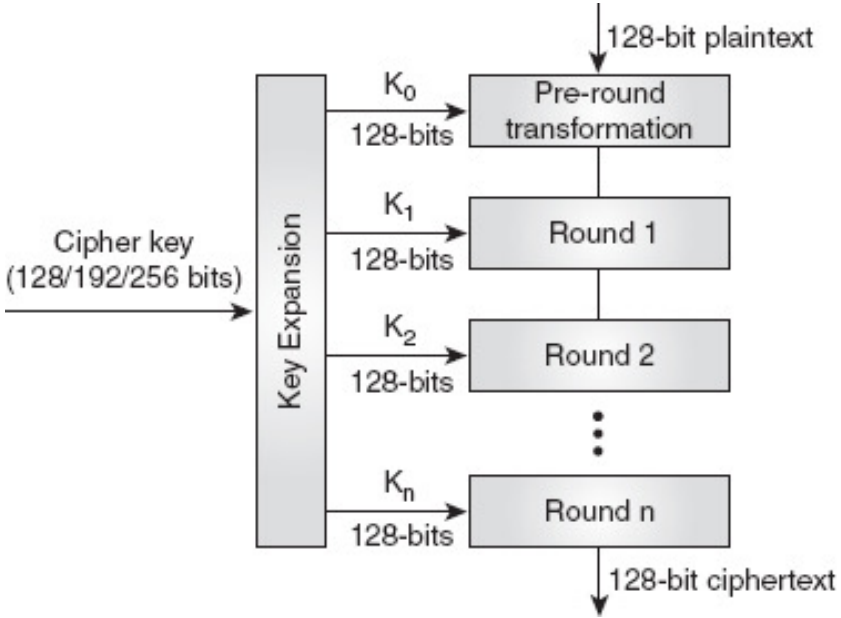
- Symmetric-key block cipher published in 2001 to replace DES/3DES
  - Made an official federal government standard in May 2002
  - Publicly adopted in many products (e.g. WinZip, RAR)

- General Mechanics
  - Works on 128-bit blocks of data
    - 4B x 4B matrix aka "state"
  - AES variants only differ in key size and affect number of encryption rounds
    - 128 bits (10 rounds)
    - 192 bits (12 rounds)
    - 256 bits (14 rounds)
  - Decryption generally follows a process reverse to encryption*

Encryption Structure

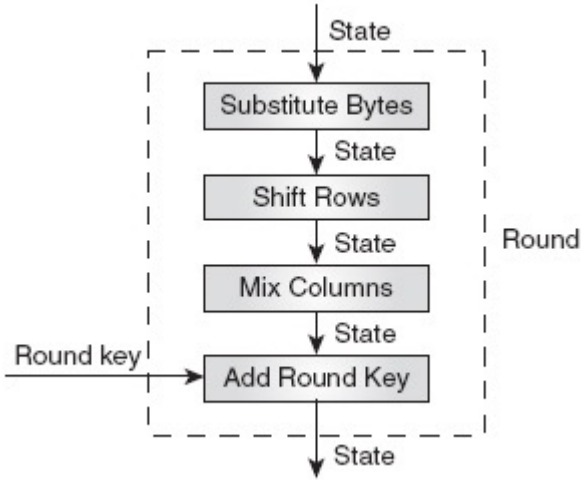
- A single encryption cycle requires several steps
  - Key Expansion
    - Creates a set of round keys (K0 through Kn) from the main cipher key
      - 128 bits long regardless of the AES variant
  - Initial Round Key Addition
    - Combines (XOR) the initial state with K0
  - Main Encryption Function (Rounds)
    - Sub Bytes
    - Shift Rows
    - Mix Columns
    - Add Round Key

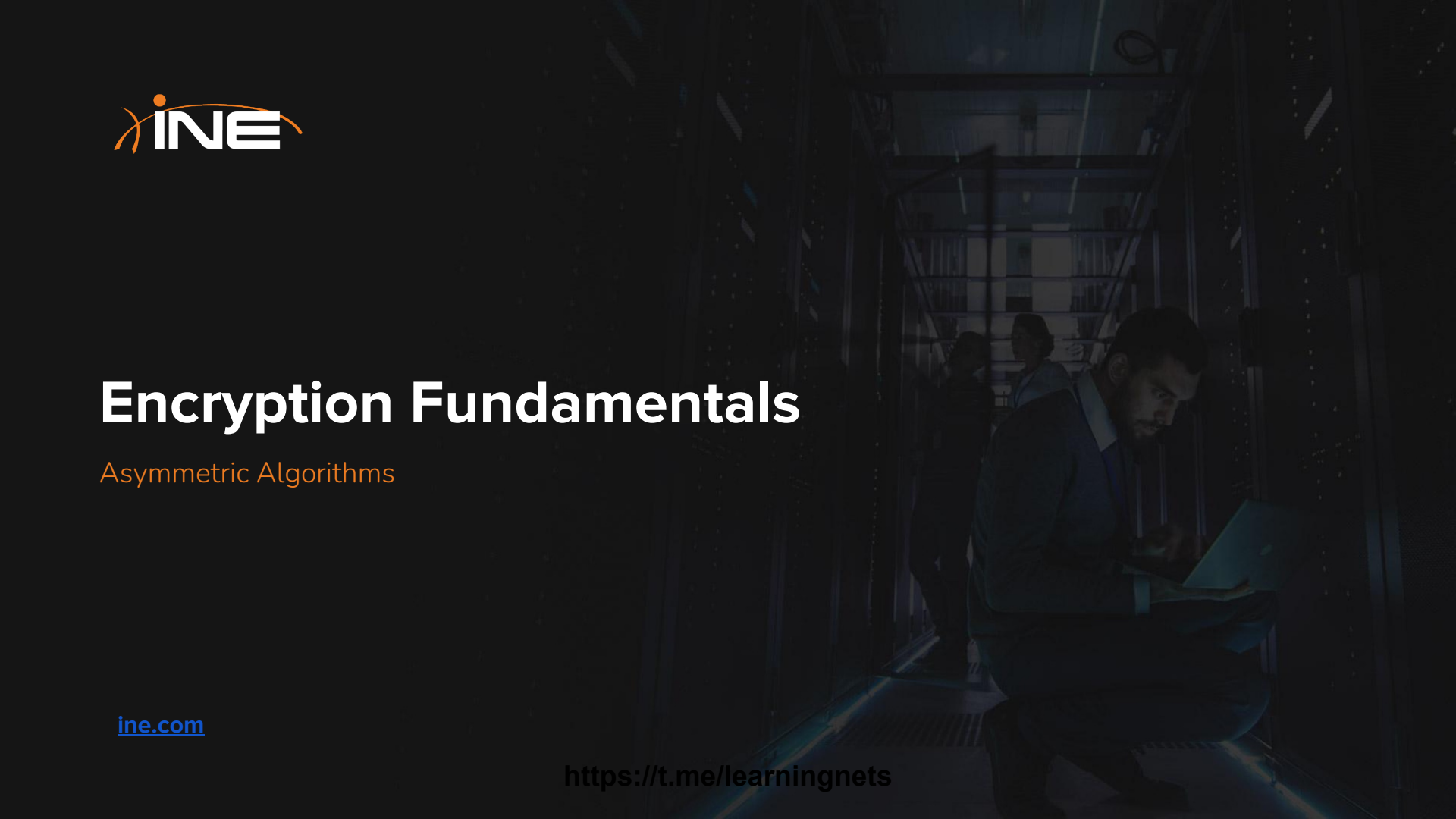
Encryption Structure



Encryption Function

- Each* encryption round involves four stages
  - Sub Bytes
    - Substitution for all bytes (S-boxes)
  - Shift Rows
    - Row-level transformation
  - Mix Columns
    - Column-level transformation
    - *Skipped during the last round
  - Add Round Key
    - Merges the corresponding round key with the current state
      - XOR





Encryption Fundamentals

Asymmetric Algorithms

ine.com

Module Overview

+ Rivest-Shamir-Adleman
+ Diffie-Hellman

Rivest-Shamir-Adleman (RSA)

- Public-key cryptosystem discovered at MIT in 1978
  - Based on large prime numbers & modular exponentiation
    - Public key encrypts, private key decrypts
  - Key Distribution
    - Public Announcement
      - Public broadcast is at risk of forgery
    - Digital Certificates
      - Link identity to the key
- Security
  - Possible threats include chosen-ciphertext or factorization attacks
    - Large keys are deemed secure

Diffie-Hellman (DH)

- First public-key algorithm published in 1976
  - Not used for regular data encryption/decryption
    - Allows for secure key exchange
      - No need for a pre-existing infrastructure
      - Results in symmetric key agreement
  - Exchanging parties are not authenticated

- Security
  - Vulnerable to MiTM
  - Vulnerable to Clogging Attacks
    - DoS

Elliptic Curve (EC)

- A newer alternative to traditional Public Key Cryptography
  - Created to replace traditional functions
  - Calculate on elliptic curves rather than large prime numbers
    - Shorter keys, better performance
  - Examples
    - Elliptic Curve DSA (ECDSA)
    - Elliptic Curve DH (ECDH)

Encryption Fundamentals

ine.com

Course Conclusion

- Encryption is a process of hiding information with the aid of a special algorithm and a key (or keys)
- It can be symmetric or asymmetric
- Symmetric encryption algorithms include DES, 3DES and AES (DES replacement)
- Examples of asymmetric encryption algorithms include RSA and DH

Thank You