



# CERTIFICATE

## Laimis Paskauskas

Has successfully completed test requirements of  
The European Information Technologies Certification Programme

### EITC/IS/CCF Classical Cryptography Fundamentals

**Certification Programme examination result:**

 73.33%

**Certification Programme description:**

Introduction to cryptography; History of cryptography; modular arithmetic and historical ciphers; Stream ciphers: stream ciphers, random numbers and the one-time pad, stream ciphers and linear feedback shift registers; DES block cipher cryptosystem: Data Encryption Standard (DES) " encryption, Data Encryption Standard (DES) - key schedule and decryption; AES block cipher cryptosystem: introduction to Galois Fields for the AES, Advanced Encryption Standard (AES); Applications of block ciphers: modes of operation for block ciphers; Conclusions for private-key cryptography: multiple encryption and brute-force attacks; Introduction to public-key cryptography: number theory for PKC " Euclidean Algorithm, Euler's Phi Function and Euler's Theorem, the RSA cryptosystem and efficient exponentiation

**Certificate Programme version/revision:** EITC/IS/CCFv1r1



**CERTIFICATE ID: EITC/IS/CCF/FXR25004606**

To validate authenticity of this certificate or review its  
programme and test results scan/click QR code or visit:  
[www.eitci.org/validate](http://www.eitci.org/validate)



**DATE OF ISSUE:**  
April 2025  
Brussels, Belgium  
European Union