EUROPEAN INFORMATION TECHNOLOGIES CERTIFICATION INSTITUTE, ASBL.

Brussels, Belgium, European Union

# CERTIFICATE

## Gorazd Planinc

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

### EITC/IS/ACC Advanced Classical Cryptography

**Certification Programme examination result:** 60%

**Certification Programme description:**

Diffie-Hellman cryptosystem: Diffie-Hellman key exchange and the discrete log problem; generalized discrete log problem and the security of Diffie-Hellman; Encryption with Discrete Log Problem: Elgamal encryption scheme; Elliptic Curve Cryptography: introduction to elliptic curves, elliptic curve cryptography (ECC); Digital Signatures: digital signatures and security services, Elgamal digital signature; Hash Functions: introduction to hash functions, SHA-1 hash function; Message Authentication Codes: MAC (Message Authentication Codes) and HMAC; Key establishing: symmetric Key Establishment and Kerberos; Man-in-the-middle attack: man-in-the-middle attack, certificates and PKI

**Certificate Programme version/revision: EITC/IS/ACCv1r1**

CERTIFICATE ID: **EITC/IS/ACC/FXR24005184**

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

DATE OF ISSUE:
December 2024
Brussels, Belgium
**European Union**