EUROPEAN INFORMATION TECHNOLOGIES CERTIFICATION INSTITUTE, ASBL.

Brussels, Belgium, European Union

CERTIFICATE

Michal Klos

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

EITC/IS/CF Cryptography fundamentals

Certification Programme examination result: 60%

Certification Programme description:

Introduction to cryptology, cryptography and cryptoanalysis: Basic definitions, Ciphering and deciphering techniques, Symmetrical and asymmetrical cryptosystems, Cryptographical algorithms classification, Authorization and authentication techniques, Methods of ensuring data integrity; Data privacy: history of symmetrical ciphers, Transposition ciphers, Substitution ciphers, Permutation and translation ciphers - matrices, Keys, XOR operation and modulo 2 bit-sum, Vernam cipher, One-time pad, Shannon's proof of OTP unconditional security, Credibility and authentication: Authentication techniques, Hash functions, MD5 implementation, Discrete logarithm, Pseudorandom sequences, Data integrity; Cryptology: cryptography, cryptoanalysis, Steganography, Cryptography formalization; Cryptosystems: asymmetrical, (public key cryptography, NP-difficult problems, asymmetrical algorithms, Public Key Infrastructure, PKI certification, digital signature), symmetrical (private key cryptography, algorithms, private key distribution, QKD - quantum cryptography); practical implementations of algorithms (symmetrical - Vernam cipher, DES, IDEA, RC5, 3DES, AES, Rijndael, NASZ; asymmetrical - RSA, Diffie-Hellman key distribution, El-Gamal); Authorization: Techniques of authorization and authentication (passwords, biometrical systems)

Certificate Programme version/revision: EITC/IS/CFv1r2

CERTIFICATE ID: **EITC/IS/CF/LEH/18004658**

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:
October 2018
Brussels, Belgium
European Union