CERTIFICATE SUPPLEMENT
EITCA/IS/FXR23004672

EITCI

EITCA IT SECURITY PROGRAMME

EITCA

Certificate ID:	EITCA/IS/FXR23004672
Certificate type:	The European Information Technologies Certification Academy Programme
Academy name:	EITCA Information Technologies Security Programme (EITCA/IS)
Issue date:	October 2023 (updated in October 2023)
Holder's name:	Viacheslav Vietluzhskykh
Holder's country:	Ukraine
Examination center:	EITCA Academy, Brussels, Belgium

EUROPEAN IT CERTIFICATION INSTITUTE · ASBL · BRUSSELS · EU · EITCI

EITCA/IS Programme (version/revision: v2r1) component EITC Certificates:

Result:

EITC/IS/CCTF Computational Complexity Theory Fundamentals

EITC Certificate number: EITC/IS/CCTF/FXR23004672

80%

Certificate Programme description: Theoretical introduction; Finite State Machines (FSMs): introduction to FSMs, examples of FSMs, operations on regular languages, introduction to nondeterministic FSMs, formal definition of nondeterministic FSMs, equivalence of deterministic and nondeterministic FSMs; Regular languages: closure of regular operations, regular expressions, equivalence of regular expressions and regular languages, pumping lemma for regular languages, summary of regular languages; Context free grammars and languages (CFGs and CFLs): introduction to CFGs and CFLs, examples of CFGs, kinds of CFLs, facts about CFLs; Context Sensitive Languages: Chomsky normal form, Chomsky hierarchy and context sensitive languages, pumping lemma for CFLs; Pushdown Automata (PDA): introduction to PDAs, Equivalence of CFGs and PDAs, conclusions from equivalence of CFGs and PDAs; Turing machines (TMs): introduction to TMs, TM examples, definition of TMs and related language classes, the Church-Turing thesis, TM programming techniques, multitape TMs, nondeterminism in TMs, TMs as problem solvers, enumerators; Decidability: decidability and decidable problems, more decidable problems For DFAs, problems concerning CFLs, universal TM, infinity - countable and uncountable, languages that are not Turing recognizable, undecidability of the halting problem, language that is not Turing recognizable, reducibility - a technique for proving undecidability, halting problem - a proof by reduction, computable functions, equivalence of TMs, reducing one language to another, the post correspondence problem, undecidability of the PCP, linear bound automata; Recursion: program that prints itself, TM that writes a description of itself, recursion theorem, results from the recursion theorem, the fixed point theorem; Logic: first-order predicate logic - overview, truth (meaning and proof), true statements and provable statements, Godel`s incompleteness theorem; Complexity: time complexity and big-O notation, computing an algorithm`s runtime, time complexity with different computational models, time complexity classes P and NP, definition of NP and polynomial verifiability, NP-completeness, proof that SAT is NP complete, space complexity classes
Certificate Programme version/revision: EITC/IS/CCTFv1r1

EITC/IS/CCF Classical Cryptography Fundamentals

EITC Certificate number: EITC/IS/CCF/FXR23004672

73%

Certificate 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) â€" 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 â€" Euclidean Algorithm, Eulerâ€™s Phi Function and Euler`s Theorem, the RSA cryptosystem and efficient exponentiation
Certificate Programme version/revision: EITC/IS/CCFv1r1

EITC/IS/ACC Advanced Classical Cryptography

EITC Certificate number: EITC/IS/ACC/FXR23004672

93%
(updated in July 2023)

Certificate 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

EITC/QI/QIF Quantum Information Fundamentals

EITC Certificate number: EITC/QI/QIF/FXR23004672

73%
(updated in September 2023)

Certificate Programme description: Introduction to Quantum Mechanics: introduction to double slit experiment, double slit experiment with waves and bullets, conclusions from the double slit experiment; Introduction to Quantum Information: qubits, geometric representation, photon polarization, uncertainty principle; Quantum Entanglement: k-level system and bra-ket notation, systems of two qubits, entanglement, EPR paradox, Bell and EPR, rotational invariance of Bell state, CHSH inequality, Bell and local realism; Quantum Information processing: time evolution of a quantum system, unitary transforms, single qubit gates, two qubit gates; Quantum Information properties: no-cloning theorem, Bell state circuit, quantum teleportation, quantum teleportation using CNOT, quantum measurement; Introduction to Quantum Computation: n-qubit systems, universal family of gates, reversible computation, conclusions from reversible computation; Quantum Algorithms: Fourier sampling, applying Fourier sampling, Simon`s algorithm, conclusions from Simon`s Algorithm; Simon`s algorithm in terms of the double slit experiment, extended Church-Turing thesis; Quantum Fourier Transform: QFT overview, n-th roots of unity, discrete Fourier Transform, n-th dimensional Quantum Fourier Transform, properties of Quantum Fourier Transform; Shor`s Quantum Factoring Algorithm: period finding, Shor`s factoring algorithm, QFT circuit; Grover`s Quantum Search Algorithm: needle in a haystack, Grover`s algorithm, implementing Grover`s Algorithm; Observables and Schrodinger`s equation: introduction to observables, observables properties, Schrodinger`s equation; Introduction to implementing qubits: continous quantum states, Schrodinger`s equation for a 1D free particle, particle in a box, implementing qubits; Introduction to Quantum Complexity Theory: limits of quantum computers, adiabatic quantum computation, BQP; Introduction to spin: spin as a qubit, Bloch sphere, Stern-Gerlach experiment, Pauli spin matrices; Manipulating spin: Larmor precession, spin resonance, classical control
Certificate Programme version/revision: EITC/QI/QIFv2r1

EITC/IS/QCF Quantum Cryptography Fundamentals

EITC Certificate number: EITC/IS/QCF/FXR23004672

73%

Certificate Programme description: Introduction: Introduction to Quantum Key Distribution; Quantum information carriers: quantum systems, composite quantum systems; Entropy: classical entropy, quantum entropy; Quantum Key Distribution: prepare and measure protocols; Entanglement based Quantum Key Distribution: entanglement based protocols; Error correction and privacy amplification: classical post-processing; Security of Quantum Key Distribution: security definition, eavesdropping strategies, security of BB84, security via entropic uncertainty relations; Practical Quantum Key Distribution: QKD - experiment vs. theory, Introduction to experimental quantum cryptography, quantum hacking

Certificate Programme version/revision: EITC/IS/QCFv2r1

EITC/IS/CNF Computer Networking Fundamentals

EITC Certificate number: EITC/IS/CNF/FXR23004672

80%

Certificate Programme description: Introduction to networking; Physical networks: cabling devices; OSI Model: introduction to the OSI Model; Internet protocols: introduction to IP addresses, IP addressing in depth, TCP/IP - Internet Protocol Suite, how TCP and UDP protocols work, establishing connections with TCP`s three way handshake, how TCP handles errors and uses windows; Practical networking: introduction to Cisco CLI; Switching: how switching works; Virtual local area network (VLAN): how VLANs work, VLAN trunk links; Access Control Lists: understanding Access Control Lists; Address Resolution Protocol (ARP): introduction to ARP; Dynamic Host Configuration Protocol (DHCP): introduction to DHCP; Domain Name System (DNS): introduction to DNS; Routing: static route configuration, dynamic routing protocols and traffic forwarding, how Routing Information Protocol RIP works, how to use Network Address Translation NAT; time in networks; Logging: sending logs to a Syslog Server; Network management: introduction to Simple Network Management Protocol SNMP, Spanning-Tree protocol, how Spanning-Tree works

Certificate Programme version/revision: EITC/IS/CNFv1r1

EITC/IS/CSSF Computer Systems Security Fundamentals

EITC Certificate number: EITC/IS/CSSF/FXR23004672

73%
(updated in October 2023)

Certificate Programme description: Architecture: security architecture; Authentication: user authentication; Buffer overflow attacks: introduction to buffer overflows; Security vulnerabilities damage mitigation in computer systems: privilege separation, Linux containers, software isolation; Secure enclaves: enclaves

Certificate Programme version/revision: EITC/IS/CSSFv1r1

EITC/IS/ACSS Advanced Computer Systems Security

EITC Certificate number: EITC/IS/ACSS/FXR23004672

80%

Certificate Programme description: Mobile security: mobile device security, mobile app security; Security analysis: symbolic execution; Network security: web security model, network security, secure channels, certificates; Implementing practical information security: information security in real life; Messaging: messaging security; Security of storage: untrusted storage servers; Timing attacks: CPU timing attacks

Certificate Programme version/revision: EITC/IS/ACSSv1r1

EITC/IS/WSA Windows Server Administration

EITC Certificate number: EITC/IS/WSA/FXR23004672

80%

Certificate Programme description: Introduction; Virtual Machine for Windows Server: downloading and installing Virtual Box, downloading Windows Server, what is a Virtual Machine, creating a Virtual Network with Virtual Box, configuring the Virtual Machine; Working with Windows Server: installing Windows Server, basic Windows Server configuration, launching Windows Server, adding the Active Directory domain services role in Windows Server, joining our workstation to our domain in Windows Server; Deploying Windows: downloading Windows 10, installing Windows 10, introduction to Windows Domain and Domain Controller; Configuring DHCP and DNS Zones in Windows Server: adding the DHCP Server Role in Windows Server, DHCP scopes and exclusions, how DHCP works in Windows Server, DHCP Reservations in Windows Server, DNS Zones in Windows Server, creating a DNS Zone; System administration in Windows Server: resource record types, understanding Active Directory, understanding organizational units and containers in Windows Server, creating and managing user accounts, groups and memberships, saved queries in Windows Server, Group Policy, creating and managing Group Policy Objects, Group Policy precedence in Windows Server; Working with PowerShell: storing user input into variables with PowerShell, creating Active Directory user accounts with Powershell, creating users accounts from a CSV Spreadsheet with PowerShell; DNS and hosts in Windows Server: creating DNS resource records in Windows Server, understanding Domain Name System in Windows Server, the hosts file in Windows Server

Certificate Programme version/revision: EITC/IS/WSAv1r1

EITC/IS/LSA Linux System Administration

EITC Certificate number: EITC/IS/LSA/FXR23004672

87%
(updated in October 2023)

Certificate Programme description: Introduction: Setting up a Linux Virtual Machine; Linux command-line: introduction to Linux command-line, Linux basic commands, Linux system awareness, Linux text editors; Linux shell features: pipes and redirection, filtering output and searching; Basic Linux sysadmin tasks: package management, Linux file permissions, basic Linux access control, user account management; Linux processes: processes overview, process signals, state, niceness and processes monitoring; Linux filesystem: the /proc filesystem, filesystem and absolute/relative pathnames, filesystem layout overview, filesystem layout continued, Linux file types; Advancing in Linux sysadmin tasks: scheduling tasks with cron, Linux bash shortcuts, introduction to tmux - windows, panes, and sessions over SSH, advancing in tmux - shared sessions, archiving and compression on Linux; Bash scripting: introduction to bash scripting, bash basics, bash variables and quoting, how bash scripts work, arguments in bash scripting, if conditions and testing in bash scripting, bash scripting functions; Advanced sysadmin in Linux: the $PATH variable in bash, the Linux script command - recording shell sessions, Linux shell aliases, basic lsof commands, monitoring Linux systems and services with Monit, advancing in Monit - SSH local forwarding for a web dashboard, service management with systemd, Linux documentation, sublime Text basics, the tee command - watch and log command output, MySQL/MariaDB database backup and restore, MySQL/MariaDB basics, Vim basics, creating a systemd Linux service, Linux inodes explained, deleting Linux system logs, how to tail Linux service logs; Working with systemd on Linux: introduction and unit files, systemctl commands, targets, dependencies and ordering

Certificate Programme version/revision: EITC/IS/LSAv1r1

EITC/IS/WASF Web Applications Security Fundamentals

EITC Certificate number: EITC/IS/WASF/FXR23004672

73%

Certificate Programme description: Introduction to Web Security, HTML and JavaScript Review; Web protocols: DNS, HTTP, Cookies, Sessions; Session attacks: cookie and session attacks; Same Origin Policy: cross-site request forgery, exceptions to the same origin policy; Cross-site scripting: cross-site scripting (XSS), cross-site scripting defenses; Web fingerprinting: fingerprinting and privacy on the web; Denial-of-service (DoS), phising and side channels; Injection attacks: code injection; TLS attacks: transport layer security; HTTPS in the real world; Authentication: introduction to authentication, WebAuthn; Managing web security: managing security concerns in Node.js project; Server security: server security: safe coding practices, local HTTP server security; DNS attacks: DNS rebinding attacks; Browser attacks: browser architecture, writing secure code

Certificate Programme version/revision: EITC/IS/WASFv1r1

EITC/IS/WAPT Web Applications Penetration Testing

EITC Certificate number: EITC/IS/WAPT/FXR23004672

73%

(updated in October 2023)

Certificate Programme description: Introduction to Burp Suite; Spidering: spidering and DVWA; Brute force testing: brute force testing with Burp Suite; Firewall detection: web application firewall detection with WAFW00F; Target scope: target scope and spidering; Hidden files: discovering hidden files with ZAP; WordPress: WordPress vulnerability scanning and username enumeration; Load balancing: load balancer scan; Cross-site scripting: XSS - reflected, stored and DOM; Proxy attacks: ZAP - configuring the proxy; Files and directories attacks: file and directory discovery with DirBuster; Web attacks practice: installing OWASP Juice Shop, CSRF - Cross Site Request Forgery, cookie collection and reverse engineering, HTTP Attributes - cookie stealing, OWASP Juice Shop - SQL Injection, DotDotPwn - Directory Traversal Fuzzing, Iframe injection and HTML injection, Heartbleed Exploit - discovery and exploitation, PHP code injection, bWAPP HTML injection (reflected POST, stored - blog), bWAPP (OS command injection with Commix, Server-Side include SSI injection); Pentesting in Docker: Docker for pentesting, Docker for pentesting on Windows; OverTheWire Natas (Level 0-10, LFI and command injection); Google hacking for pentesting: Google Dorks for penetration testing; ModSecurity: Apache2 ModSecurity, Nginx ModSecurity

Certificate Programme version/revision: EITC/IS/WAPTv1r1