European Security and Defence College
Doc: ESDC/2023/055
Date: 16 February 2023
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	**Applied Cryptography**	ECTS
Feb. 2025	**211**		**1**

Target audience	Aim
The participants should be mid-ranking to senior military or civilian officials dealing with information security and cybersecurity from EU Institutions, Bodies and Agencies as well as EU Member States. Open to: • EU Member States / EU Institutions Bodies and Agencies	The aim of the course is to provide the main notions of applied cryptography, help the participants to familiarise with the use of hash functions, encryption algorithms and the available encryption tools. Furthermore, this course will allow the participants to exchange views, share best practices on applied cryptography topics by improving their knowledge, skills and competencies in this domain. By the end of this course, the participants will be familiar with the terminology, concepts and tools used in applied cryptography and share views on how to protect data in personal and business environment.

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber and the EU Policy on Cyber Defence	• *Specialised course, at tactical/operational level.* • *Linked with the strategic objectives of Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning Outcomes	
Knowledge	LO1. Define the basic notions, terminology and concepts of applied cryptography LO2. Define the basics of Randomness, Abstract Syntax Notation One (ASN.1), Hash functions, symmetric cryptography, asymmetric cryptography, public key infrastructure , public key certificates, digital signatures, transport layer security, cryptographic currency transactions LO3. Define how Blockchain and Cryptocurrency use cryptographic algorithms
Skills	LO4. Produce encrypted from plaintext and the opposite LO5. Produce ASN.1 description language code LO6. Compute bitwise operations LO7. Apply Hash functions, Encryption algorithms, Certificates, TLS LO8. Apply Pretty Good Privacy (PGP) to encrypt and decrypt data and emails

Responsibility and Autonomy	LO9. Create symmetric cryptosystem LO10. Generate Certificates, Public Private Key LO11. Create asymmetric encryption and signing utility

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of *level 1 evaluation* (*based on participants' satisfaction with the course*) and *level 3 evaluation* (*assessment of participants' long-term change in behaviour after the end of the course*). *Evaluation feed-back* is given in the level 1 evaluation on the residential modules.

In order to complete the course, the participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential modules, including their syndicate sessions and practical activities as well as on their completion of the eLearning phases: course participants must finalise the autonomous knowledge units (AKUs) and pass the tests (*mandatory*), scoring at least 80% in the incorporated out-test/quiz. **However, no formal verification of the learning outcomes is foreseen; proposed ECTS is based on participants' workload only**.

The Executive Academic Board takes these factors into account when considering the award of *Certificates* to participants. Module leaders provide an evaluation report for each residential module. The Course Director is responsible for overall coordination, with the support of the ESDC Secretariat, and drafts the *final evaluation report, which* is presented to the Executive Academic Board.

Course structure

The residential module is held over 3 days.

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. One Time Pad (OTP)	6(3)	• Pseudo-Random Number Generator (PRNG) • Bitwise operations • One-Time Pad (OTP)
2. Abstract Syntax Notation One (ASN.1)	10(4)	• Types • Encoding rules • Distinguished Encoding Rules (DER)
3. Hash functions	4(2)	• Data identification and integrity verification • Hash-based PRNG • Hash chain • Hash tree • Hash-based Message Authentication Code
4. Symmetric cryptography	5(2)	• AES • Block cipher • Password based
5. Asymmetric cryptography	5(2)	• RSA encryption • Hybrid encryption • RSA Public and Private key
6. Public Key Infrastructure (PKI) and certificates	10(4)	• Certificates • ElGamal encryption system • Payment Card Industry Data Security Standards (PCI-DSS) • Encryption in compliance with industry standards and GDPR
7. Transport Layer Security (TLS)	5(2)	• Transport Layer Security overview and characteristics
8. Email security	3	• Encrypting emails

9. Crypto Currencies	5	• Cryptocurrencies transactions (case study) • Blockchain and the transaction log • Anonymity
TOTAL	**48(19)**	

<u>Material</u>

Required:

- **AKU 104: Module 2 – Learn about Information Security**
- **ENISA, Algorithms, Key Sizes and Parameters Report, 2013 recommendations from October 2013, https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report?v2=1**
- **ENISA, Post-quantum cryptography, Current state and quantum mitigation from May 2021, https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation**

Recommended:

- *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union (**NIS 2**)*
- *EU Policy on Cyber Defence, JOIN(22) 49 final, 10.11.2022*
- *The EU's Cybersecurity Strategy for the Digital Decade (December 2020)*
- *The EU Cybersecurity Act (June 2019)*
- *The EU Cyber Diplomacy Toolbox (June 2017)*
- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*
- *Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)*

<u>Methodology</u>

The course is based on the following methodology: Presentations, Panels talks, Q&A and/or workshops

<u>Additional information</u>

Pre-course questionnaire on learning expectations and possible briefing topic from the specific area of expertise may be used.

All course participants have to prepare for the residential module by going through the relevant eLearning preparatory phase, which is mandatory. The materials proposed for supplemental (eLearning) study will reflect current developments in the field of cyber security/cyber defence in general and EU policies in particular.

The Chatham House Rule is applied during all residential phase of the course: "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".