**European Security and Defence College**
**Doc: ESDC/2021/073**
**Date: 17/03/2021**
**Origin:** Executive Academic Board

# Curriculum

| To be reviewed by | Activity Number | Applied Cryptography | ECTS |
|---|---|---|---|
| *February 2023* | ***211*** | | **2** |

## Target audience

Participants should be junior to mid-ranking (at technical level) officials dealing with aspects in the field of cyber security from Member States (MS) and EU Institutions and Agencies. They should have basic knowledge of IT systems and preferably Python programming language.

Course participants must be available during the entire course and should be ready to participate with their specific field of expertise and experience.

## Aim

This course aims to enable participants to comprehend the main notions of applied cryptography, help them build their own encryption utilities by using hash functions, encryption algorithms and widely available tools.

Furthermore, this course will allow the junior ranking to senior officials from MS and EU Institutions and Agencies to exchange their views, share best practices on applied cryptography topics by improving their knowledge, skills and competencies in the cyber 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.

| | | |
|---|---|---|
| **Learning outcomes** | Knowledge | K1 - Define the basic notions, terminology and concepts related to applied cryptography<br>K2 - Compute bitwise operations<br>K3 - Define the basics of Randomness, One Time Pad, Abstract Syntax Notation One (ASN.1), Hash functions, symmetric cryptography (Advanced Encryption Standard (AES)), Asymmetric Cryptography (RSA), Public Key Infrastructure (PKI), Public Key Certificates, Digital Signatures, Transport Layer Security (TLS), cryptographic currency transactions |
| | Skills | S1 - Produce ASN.1 description language code to define data structures<br>S2 - Produce cypher from plaintext and the opposite (decryption)<br>S3 - Outline the basic characteristics of Hash functions, Encryption algorithms and Certificates<br>S4 - Apply Hash functions, Encryption algorithms, Certificates, TLS<br>S5 - Apply Pretty Good Privacy (PGP) to encrypt and decrypt data |
| | Competences | C1 - Create symmetric cryptosystem<br>C2 - Generate Certificates, Public Private Key<br>C3 - 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 participant's satisfaction with the course).

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on the active contribution in the residential Module, including their syndicate sessions and practical activities as well as on the completion of the eLearning phases: course participants finalise the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated out-test/quiz. At the end of the course, there is active observation by the course director/lead instructor and a feedback questionnaire is filled by the course participants.

**However, no formal verification of learning outcome is foreseen; proposed ECTS is based on participants' workload only**

## Course Structure

| Main Topic | Recommended Working Hours (of that eLearning) | Contents |
|---|---|---|
| One Time pad | 6(3) | • Pseudo-Random Number Generator (PRNG)<br>• Bitwise operations<br>• One-Time Pad (OTP) |
| Abstract Syntax Notation One (ASN.1) | 10(4) | • Types<br>• Encoding rules<br>• Distinguished Encoding Rules (DER) |
| Hash functions | 4(2) | • Data identification and integrity verification<br>• Hash-based PRNG<br>• Hash chain<br>• Hash tree<br>• Hash-based Message Authentication Code |
| Symmetric cryptography | 5(2) | • AES<br>• Block cipher<br>• Password based |
| Asymmetric Cryptography (RSA) | 5(2) | • RSA encryption<br>• Hybrid encryption<br>• RSA Public and Private key |
| Public Key Infrastructure (PKI) and certificates | 10(4) | • Key management<br>• Certificate Authority (CA)<br>• Certificates |
| Transport Layer Security (TLS) | 5(2) | • Transport Layer Security overview and characteristics |
| Crypto Currencies | 6 | • Cryptocurrencies transactions (case study)<br>• Blockchain<br>• Blockchain (transaction log)<br>• Anonymity |
| **TOTAL** | 51(19) | |

Materials

*Essential eLearning:*

**AKU 104a:** Information Security Management Implementation Course
**AKU 104b:** Information Security Management Implementation Course
**AKU 104c:** Information Security Management Implementation Course

*Reading material [examples]:*

- *The EU Cyber Diplomacy Toolbox (June 2017)*
- *The EU Cybersecurity Act ( June 2019)*
- *The EU's Cybersecurity Strategy for the Digital Decade*
- *Regulation (EU) eIDAS Regulation N°910/2014*

Additional information

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.

In order to facilitate discussion between course participants and trainers/experts/guest speakers, the **Chatham House Rule** is used during the residential Module: "*participants to the CSDP HLC 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*"**.**