BCS Level 4 Certificate in Employment of Cryptography Syllabus
QAN 603/0892/8

Version 1.1
November 2016

This is a United Kingdom government regulated qualification which is administered and approved by one or more of the following: Ofqual, Qualification in Wales, CCEA or SQA.

BCS Level 4 Certificate in Employment of Cryptography Syllabus

Contents

Change History

Any changes made to the syllabus shall be clearly documented with a change history log. This shall include the latest version number, date of the amendment and changes made. The purpose is to identify quickly what changes have been made.

Version Number	Changes Made
Version 1.0 November 2016	Syllabus Created
Version 1.1 November 2016	Added mandatory Ofqual text

Introduction

This Certificate is the fifth of seven knowledge modules that are applicable to the Level 4 Cyber Security Technologist Apprenticeship. This is a general introduction to the deployment of cryptography. It covers the theory and application of methods available to secure information, computers and networks, as well as legal issues involved with cryptography.

Objectives

Apprentices should be able to demonstrate an understanding of the theory, deployment and legal issues related to cryptography. Key areas are:

1. The ability to demonstrate a thorough knowledge of the theory underpinning cryptographic techniques, common applications and limitations.

2. A comprehensive knowledge of the practical deployment of cryptography, how it is applied to secure a range of common public technologies, data and networked systems; in addition to issues faced in their deployment and updating.

3. A thorough understanding of the legal issues relevant to cryptography; particularly when crossing national borders and regulatory frameworks in place in various jurisdictions.

Evidence of lessons learnt in these key areas should be collected and reflected upon when the apprentice is compiling the Summative Portfolio. The apprentice should be able to identify how the task might be changed or improved upon with knowledge subsequently gained.

Target Audience

The certificate is relevant to anyone requiring an understanding of the core principles and foundations of a Cyber Security Technologist.

Course Format and Duration

Apprentices can study for this certificate by attending a training course provided by a BCS accredited Training Provider. The estimated total qualification time for this certificate is 125 hours.

Eligibility for the Examination

There are no specific pre-requisites for entry to the examination; however, apprentices should possess the appropriate level of knowledge to fulfil the objective shown above. Individual employers will set the selection criteria, but this is likely to include A' Levels, a relevant Level 3 apprenticeship, or other relevant qualifications, relevant experience and/or an aptitude test with a focus on functional maths.

Duration and Format of the Examination

The format for the examination is a one-hour multiple-choice examination consisting of 40 questions. The examination is closed book (no materials can be taken into the examination room). The pass mark is 26/40 (65%).

Additional Time for Apprentices Requiring Reasonable Adjustments Due to a Disability

Apprentices may request additional time if they require reasonable adjustments. Please refer to the reasonable adjustments policy for detailed information on how and when to apply.

Additional Time for Apprentices Whose Language Is Not the Language of the Exam

If the examination is taken in a language that is not the apprentice's native/official language then they are entitled to 25% extra time.

If the examination is taken in a language that is not the apprentice's native/official language then they are entitled to use their own **paper** language dictionary (whose purpose is translation between the examination language and another national language) during the examination. Electronic versions of dictionaries will **not** be allowed into the examination room.

Guidelines for Accredited Training Organisations

Each major subject heading in this syllabus is assigned an allocated time. The purpose of this is two-fold: firstly, to give both guidance on the relative proportion of time to be allocated to each section of an accredited course and an approximate minimum time for the teaching of each section; secondly, to guide the proportion of questions in the exam. Accredited Training Organisations may spend more time than is indicated and apprentices may spend more time again in reading and research. Courses do not have to follow the same order as the syllabus. Courses may be run as a single module or broken down into two or three smaller modules.

This syllabus is structured into sections relating to major subject headings and numbered with a single digit section number. Each section is allocated a minimum contact time for presentation.

Syllabus

For each top-level area of the syllabus, a percentage and K level is identified. The percentage is the exam coverage of that area and the K level identifies the maximum level of knowledge that may be examined for that area.

1. Theory of cryptographic techniques (40%, K3)

In this key topic, the apprentice will describe the technology of cryptography and name the available techniques, limitations and problems commonly encountered. Outcomes should include an ability to:

1.1 Describe cryptographic techniques and state their limitations. For example, but not limited to:
- Ciphertext vs. Plaintext
- Ciphers
- Cryptographic techniques
- Key length vs. Security
- Hashing
- Digital signatures
- Attacks

1.2 Describe the main features of symmetric cryptosystems, PK cryptosystems and key exchange.

1.3 Show where the various cryptographic techniques may be employed to secure data and systems. For example, but not limited to:
- Password verification
- Digital signatures
- VPNs
- Tunnelling
- Encapsulating & carrier protocols
- IPsec

1.4 Show how poorly applied cryptography can become a threat vector. Indicative areas of study include, but are not limited to:
- ECB mode
- Collision attacks
- Algorithm problems
- Key management problems
- Random number generation problems

1.5 Explain the significance and role of entropy in cryptography and discuss security problems associated with entropy.

2. Deployment of cryptography (40%, K2)

In this key topic, the apprentice will explain the deployment of cryptographic systems in a range of common public technologies; in the protection of data and networked systems and discuss issues faced in their deployment and updating. Outcomes should include an ability to:

2.1 Explain the significance of key management as it relates to controls, lifecycle and governance.

2.2 Describe the role of cryptography in a range of common public systems. For example, but not limited to:
- Mobile telecommunications
- Secure card payments
- Cyber applications
- Video broadcasting
- Private and home user considerations

2.3 Describe the role of cryptography as it applies to data on hard disks or in transit. For example, but not limited to:
- Secure Internet transaction technologies
- Data at rest
- Open vs closed source

2.4 List some of the practical issues encountered in implementing cryptography. Indicative areas may include, but not be limited to:
- Performance considerations
- Storage of keys
- Security clearance of custodians
- Historical consideration of broken cryptographic systems
- Theoretical vs practical security
- Kerckhoff's principle

2.5 Explain the practical issues faced when updating cryptographic techniques. For example, but not limited to:
- Vulnerability analysis
- Intelligence sources
- General understanding of validation processes
- Patching process and testing

3. Cryptography across jurisdictions (20%, K2)

In this key topic, the apprentice will discuss legal issues relevant to cryptography (particularly when crossing national borders) and describe UK, EU and US export control of cryptography and the Wassenaar Arrangement. Outcomes should include an ability to:

3.1 List the regulatory frameworks in place in different jurisdictions, covering such topics as:
- International Traffic in Arms Regulations
- DPA
- FoI
- The Combined Code
- Sarbanes-Oxley and their areas of governance
- RIPA 2000
- Key escrow
- International Data Encryption Algorithm (IDEA)

3.2 Describe some of the legal issues related to cryptography with respect to national borders.

3.3 List a range of resources available to obtain advice concerning cryptography and security. For example, but not limited to:
- CAVP
- CVE lists
- Open vs. closed reviews
- ISO
- OWASP
- SANS
- NIST
- NCSC

Levels of Knowledge / SFIA Levels

This course will provide apprentices with the levels of difficulty / knowledge skill highlighted within the following table, enabling them to develop the skills to operate at the levels of responsibility indicated. The levels of knowledge and SFIA levels are explained in on the website www.bcs.org/levels. The levels of knowledge above will enable apprentices to develop the following levels of skill to be able to operate at the following levels of responsibility (as defined within the SFIA framework) within their workplace:

Level	Levels of Knowledge	Levels of Skill and Responsibility (SFIA)
K7		Set strategy, inspire and mobilise
K6	Evaluate	Initiate and influence
K5	Synthesise	Ensure and advise
K4	Analyse	Enable
K3	Apply	Apply
K2	Understand	Assist
K1	Remember	Follow

Question Weighting

Syllabus Area	Target number of questions
1. Theory of cryptographic techniques. (40%, K3)	16
2. Deployment of cryptography. (40%, K2)	16
3. Cryptography across jurisdictions. (20%, K2)	8
Total	**40 Questions**

Format of Examination

Type	40 Question Multiple Choice.
Duration	1 Hour. An additional 15 minutes will be allowed for apprentices sitting the examination in a language that is not their native /mother tongue.
Pre-requisites	Accredited training is strongly recommended but is not a pre-requisite.
Supervised	Yes.
Open Book	No.
Pass Mark	26/40 (65%)
Calculators	Calculators cannot be used during this examination.
Total Qualification Time (TQT)	125 Hours.
Delivery	Online.

Trainer Criteria

Criteria	▪ Have 10 days' training experience or have a Train the Trainer qualification. ▪ Have a minimum of 3 years' practical experience in the subject area.

Classroom Size

Trainer to apprentice ratio	1:16