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

Version 3.0
March 2020

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
Version 2.0 October 2019	Update to branding. Exam question balance also amended.
Version 3.0 March 2020	Full syllabus review.

Introduction

This certificate is the fifth of the five knowledge modules that are applicable to the Technologist pathway for 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. Describe the main cryptographic techniques (e.g. symmetric, public key, secure hash, digital signing, block cipher etc), how they are applied and to what end and their limitations (including study of some examples of badly applied or implemented cryptographic techniques).
2. Explain the significance of key management and the main features, benefits and limitations of symmetric and public key cryptosystems and the significance of entropy.
3. Describe the role of cryptographic techniques in a range of different systems (e.g. GSM, Chip&PIN, common hard disk encryption, TLS, SSL, privacy enforcing technology) and the practical issues introducing such into service and updating them.
4. Appreciate that there are legal issues relevant to cryptography in particular when crossing national borders. Awareness of UK, EU and US export control of cryptography and the Wassenaar Arrangement and where to go to get advice.

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 cryptography.

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 and Practice of Cryptographic Techniques and Key Management (80%, K2)

In this key topic, the apprentice will describe the main cryptographic techniques and explain the significance of key management and the main features of cryptosystems. Outcomes should include an ability to:

1.1 Describe the main cryptographic techniques in use.

- Symmetric;
  - stream ciphers (e.g. RC4, ChaCha);
  - block ciphers (e.g. RC5, AES, 3DES, Blowfish);
- asymmetric or public key;
  - RSA;
  - Diffie-Hellman;
  - PGP;
  - elliptic curve ciphers;
- Hashing;
  - MD5;
  - SHA.

1.2 Describe how the main cryptographic techniques are used and the limitations of each in those situations.

- file and disk encryption;
  - removable media;
  - WDE for storage in desktops and servers;
  - mobile phones;
  - individual document encryption;
- database encryption;
  - individual fields or records;
  - transparent whole database encryption;
- digital rights management;
  - product keys;
  - copy protection for electronic media;
  - DVD encryption;
  - online authentication or activation;
- Ransomware;
  - removing access to files;
  - key recovery;
- ecommerce;
  - TLS/SSL protected transactions;
  - cryptocurrency;
- wireless communications;
  - WLANs;
  - wireless WAN backhaul;
- email;
  - message encryption;
  - message signing;
- data destruction;
  - destroying keys to remove access to data;
- blockchain;
- protecting passwords and other authentication mechanisms;
  - hashing passwords;
  - password managers;
  - protecting biometrics;
  - smart cards;
- VPNs;
  - user authentication;
  - network to network authentication;
  - traffic encryption.

1.3 Explain how crypto systems are attacked.

- replay attacks;
- side channel;
- traffic analysis;
- brute force;
- MITM;
- key theft.

1.4 Explain how crypto systems and algorithms become obsolete and can be poorly implemented.
- DES;
- WEP;
- MD5;
- SHA1.

1.5 Describe the features of key management including the key lifecycle and the challenges associated with each stage.
- generate;
- distribute;
- deploy;
- archive;
- revoke;
- destroy.

1.6 Explain how key management works in symmetric and asymmetric cryptosystems describing the benefits and limitations of each.
- open and closed source key management systems;
- cloud based key management services;
- PKI and digital certificates.

1.7 Explain the significance of entropy in cryptography.

2 Practical and Legal Issues Affecting Cryptographic Implementations (20%, K2)

In this key topic, the apprentice will describe the role of cryptographic techniques in a range of different systems and recognise the legal issues relevant to cryptography. Outcomes should include an ability to:

2.1 Describe how cryptographic techniques are used in different systems and the practical difficulties of each in those situations including how to introduce and maintain them in an existing ecosystem.
- cellular radio e.g. GSM and professional radio e.g. TETRA;
- chip and PIN enabled payment cards;
- authentication tokens;
- file and disk encryption in desktop operating systems;
- online transactions using TLS/SSL;
- 'chat' communications e.g. WhatsApp, iMessage;
- password managers.

2.2 Recognise that there are legal issues surrounding cryptography when crossing national borders or exporting / importing cryptographic technology.

2.3 Describe the purpose of the Wassenaar Arrangement and how it impacts on cryptography.

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 and Practice of Cryptographic Techniques and Key Management	32
2 Practical and Legal Issues Affecting Cryptographic Implementations	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