Level 4 Certificate in Employment of Cryptography (3660-05)

September 2019 Version 1.0

Qualification Handbook

Qualification at a glance

Subject area	IT Professional
City & Guilds number	3660
Age group approved	16+
Entry requirements	Centres must ensure that any pre-requisites stated in this Handbook are met.
Assessment	Online multiple choice test
Qualification grade scale	Pass
Approvals	Approval application required. Please see **www.cityandguilds.com** for details.
Registration and certification	Registration and certification of this qualification is through the Walled Garden, and is subject to end dates.

Title and level	GLH	TQT	City & Guilds qualification number	Ofqual accreditation number
Level 4 Certificate in Employment of Cryptography	55	132	3660-05	TBC

Version and date	Change detail	Section
1.0 September 2019	Document created	

Contents

1 Introduction

This document tells you what you need to do to deliver the qualifications:

Area	Description
Who is the qualification for?	This qualification is designed to support learners who are on the **Technologist** pathway of the **Level 4 Cyber Security Technologist** apprenticeship, forming a mandatory qualification in that pathway.
What does the qualification cover?	Learners will explore the concepts, theory and terminology of cryptography in the context of modern information security practices, legislation and cross-border agreements on trade, and use of cryptographic technology. Learners will cover: • The key developments in the history of cryptography including early written examples such as the Caesar and Scytale cipher • The key concepts of confidentiality, integrity and availability • The main ways to break a code • The differences between public and private keys The qualification emphasises the employment of cryptography in every-day use by organisations and individuals who have a need to ensure the confidentiality, integrity and availability of information.
What opportunities for progression are there?	On achieving this qualification the learner will have completed a section of the knowledge element as part of their apprenticeship journey on the **Technologist** pathway: **Technologist pathway** • Level 4 Certificate in Cyber Security Introduction (3660-01) • Level 4 Certificate in Network and Digital Communications Theory (3660-02) • Level 4 Award in Security Case Development and Design Good Practice (3660-03) • Level 4 Award in Security Technology Building Blocks (3660-04)

	• Level 4 Certificate in Employment of Cryptography (3660-05)
Who did we develop the qualification with?	It was developed in collaboration with employers, sector experts and training providers using the Apprenticeship Standard and Occupational Brief as the baseline. These were created by The Tech Partnership and their Employer Groups for the specific areas. The qualification embodies the required learning for an apprentice to have the opportunity to successfully gain the relevant knowledge for their chosen career path in cyber security.
Is it part of an apprenticeship framework or initiative?	Yes – Level 4 Cyber Security Technologist (9660-12/13)

Structure

Learners must complete the single unit 405 to gain this qualification.

Total Qualification Time

Total Qualification Time (TQT) is the number of notional hours which represents an estimate of the total amount of time that could reasonably be expected for a learner to achieve and demonstrate the achievement of the level of attainment necessary for the award of a qualification.

TQT is comprised of the following two elements:

- The number of hours which an awarding organisation has assigned to a qualification for Guided Learning, and
- An estimate of the number of hours a learner will reasonably be likely to spend in preparation, study or any other form of participation in education or training, including assessment, which takes place as directed by - but, unlike Guided Learning, not under the immediate guidance or supervision of - a lecturer, supervisor, tutor or other, appropriate provider of education or training

Title and level	GLH	TQT
Level 4 Certificate in Employment of Cryptography	55	132

2 Centre requirements

Approval

To offer this qualification, new centres will need to gain both centre and qualification approval. Please refer to the *City & Guilds Centre Manual* for further information.

Centre staff should familiarise themselves with the structure, content and assessment requirements of the qualification before designing a course programme.

Resource requirements

Resources

Please see the individual unit information for any resources required.

Centre staffing

Staff delivering this qualification must be able to demonstrate that they meet the following occupational expertise requirements. They should:

- be occupationally competent or technically knowledgeable in the area[s] for which they are delivering training and/or have experience of providing training. This knowledge must be to the same level as the training being delivered
- have recent relevant experience in the specific area they will be assessing
- have credible experience of providing training

Centre staff may undertake more than one role, e.g. tutor and assessor or internal verifier, but cannot internally verify their own assessments.

Learner entry requirements

City & Guilds does not set entry requirements for this qualification. However, centres must ensure that candidates have the potential and opportunity to gain the qualification successfully and that they have the full engagement of the employer for the full programme.

Age restrictions

City & Guilds cannot accept any registrations for candidates under 16 as these qualifications are not approved for under 16s.

3 Delivering the qualification

Initial assessment and induction

An initial assessment of each candidate should be made before the start of their programme to identify:

- if the learner has any specific training needs
- support and guidance they may need when working towards their qualifications
- any units they have already completed, or credit they have accumulated which is relevant to the qualifications
- the appropriate type and level of qualification

We recommend that centres provide an induction programme so the candidate fully understands the requirements of the qualification, their responsibilities as a candidate, and the responsibilities of the centre. This information can be recorded on a learning contract.

Support materials

The following resources are available for this qualification:

- Practice exam available both paper-based and on-screen

4 Assessment

Summary of assessment methods

Candidates must:
- successfully complete one evolve test for the mandatory unit

Available assessments/assignments:

City & Guilds has written the following assessments to use with this qualification:

- Evolve tests

Assessment Types			
Unit	**Title**	**Assessment method**	**Where to obtain assessment materials**
405	Employment of Cryptography	Multiple choice questions – online Evolve Test	Please see www.cityandguilds.com

Assessment strategy

Test specifications
The way the knowledge is covered by each test is laid out in the table below:

Assessment type: Multiple choice online test
Assessment conditions: Invigilated examination conditions
Number of questions: 20
Duration: 30 minutes
Pass mark: 13/20 (65%)
Grading: Pass/Fail

Test: 405 Employment of Cryptography

Learning Outcome	Topic	Number of questions	Weighting
1 Describe the principles of cryptography	1.1 Confidentiality, Integrity and Availability	3	45%
	1.2 Benefits and limitations of cryptography	2	
	1.3 Legislative considerations for cryptography	4	

2 Explain the main cryptographic techniques	2.1 Development of cryptography	3	35%
	2.2 Concepts and Use of Public Key and Private Key cryptography	4	
3 Describe methods of code breaking	3.1 Code breaking concepts	2	20%
	3.2 Cryptographic vulnerabilities	2	
Total		**20**	

Recognition of prior learning (RPL)

Recognition of prior learning means using a person's previous experience or qualifications which have already been achieved to contribute to a new qualification.

RPL is not allowed for this qualification.

5 Administration

Quality assurance

Internal quality assurance

Registered centres must have effective quality assurance systems to ensure optimum delivery and assessment of qualifications. Quality assurance includes initial centre registration by City & Guilds and the centre's own internal procedures for monitoring quality. Centres are responsible for internal quality assurance and City & Guilds is responsible for external quality assurance.

Standards and rigorous quality assurance are maintained by the use of:

- internal quality assurance
- City & Guilds external moderation

In order to carry out the quality assurance role, Internal Quality Assurers must have appropriate teaching and vocational knowledge and expertise.

Access arrangements and special consideration

We have taken note of the provisions of equalities legislation in developing and administering this specification.

We follow the guidelines in the Joint Council for Qualifications (JCQ) document: Regulations and Guidance Relating to Candidates who are Eligible for Adjustments in Examination GCSE, GCE, GNVQ, AEA, Entry Level, Basic Skills & Key Skills Access Arrangements and Special Consideration. This is published on the JCQ website: http://www.jcq.org.uk/access_arrangements/

Access arrangements

We can make arrangements so that learners with disabilities, special educational needs and temporary injuries can access the assessment. These arrangements must be made before the examination. For example, we can produce a Braille paper for a learner with visual impairment.

Special consideration

We can give special consideration to learners who have had a temporary illness, injury or indisposition at the time of the examination. Where we do this, it is given after the examination.

Applications for either access arrangements or special consideration should be submitted to City & Guilds by the Examinations Officer at the centre.

Language of examinations

We will provide this specification in English only.

Other issues

European Dimension

City & Guilds has taken account of the 1988 Resolution of the Council of the European Community in preparing this specification and associated specimen units.

Environmental Education

City & Guilds has taken account of the 1988 Resolution of the Council of the European Community and the Report Environmental Responsibility: An Agenda for Further and Higher Education 1993 in preparing this specification and associated specimen units.

Avoidance of bias

City & Guilds has taken great care in the preparation of this specification and specimen units to avoid bias of any kind.

6 Units

Availability of units

The unit information can be found in this document.

Structure of the units

These units each have the following:

- City & Guilds reference number
- Title
- Level
- Guided learning hours (GLH)
- Learning outcomes

Centres must deliver the full breadth of the range. Specialist equipment or commodities may not be available to all centres, so centres should ensure that their delivery covers their use.

Unit 405 Employment of Cryptography

Level:	4 Certificate
GLH:	55
TQT:	132

What is this unit about?

Learners will explore the concepts, theory and terminology of cryptography in the context of modern information security practices, legislation and cross-border agreements on trade, and use of cryptographic technology.

Learners will cover:

- The key developments in the history of cryptography including early written examples such as the Caesar and Scytale cipher
- The key concepts of confidentiality, integrity and availability
- The main ways to break a code
- The differences between public and private keys

The unit emphasises the employment of cryptography in every-day use by organisations and individuals who have a need to ensure the confidentiality, integrity and availability of information.

This unit is a mandatory unit for apprentices completing the 'Technologist' pathway of the Level 4 Cyber Security Technologist apprenticeship.

This unit is assessed through a multiple-choice test, taken online.

Learning outcomes

In this unit, learners will be able to

1. Describe the principles of cryptography
2. Explain the main cryptographic techniques
3. Describe methods of code breaking

Learning outcome

1. Explain the principles of cryptography

Topics

1.1 Confidentiality, Integrity and Availability
1.2 Benefits and limitations of cryptography
1.3 Legislative considerations for cryptography

Depth

The learner will be able to explain the principles of cryptography, the benefits and drawbacks of employing cryptography and the legislative framework within which cryptographic technology is used across national borders. Particular emphasis should

be given to the use of cryptography in an organisational context such as government or business usage.

Topic 1.1

The learner will be able to explain the concepts of confidentiality, integrity and availability as they apply to cryptography:

- Confidentiality of information (concept of least privilege):
    - Control of access to information in storage (at rest), usage and transmission:
        - Encryption:
            - Asymmetrical
            - Symmetrical
- Integrity of information (non-repudiation, digital watermarking):
    - Storage, usage and transmission of information in an unchanged state, such as Hashing
- Availability of information, such as:
    - Failover
    - Available to authorized individuals
    - Access denied to unauthorized individuals:
        - Usernames and passwords
        - Multi factor authentication
        - One-time passwords

Topic 1.2

The learner will be able to explain the key benefits, limitations and disadvantages of implementing cryptography:

- Benefits:
    - Security of information through control of access
    - Increased trust in reliability
    - Verifiability of authenticity:
        - Digital signatures
    - Verifiability or origin:
        - Digital Certificates
- Limitations:
    - Trade-off between ease of implementation and the burden on the computer resources
    - Risk to information loss (unable to decrypt)
    - Security of keys
    - Key length, key generation, entropy
    - Rigor of algorithms
- Disadvantages:
    - Challenges for law enforcement
    - Challenges for open societies
    - Use by criminal organisations
    - Vulnerabilities of weak or compromised cryptographic design and implementation

Topic 1.3

The learner will be able to explain the legislation that applies to cryptographic technology:

- Import and Export controls (EU):
    - Variations by country
- The Electronic Communications Act (2000) & the Electronic Signatures Regulations (2002)
- Wassenaar Arrangement (1996):
    - Purpose
    - Category 5 – Part 2 (Information Security)
    - Participating entities (NATO, EU, Non-EU)
    - 2003 amendments on intrusion detection software
- Regulation of Investigatory Powers Act (UK law enforcement)
- International Traffic in Arms Regulations (ITAR)
- Disclosure Laws:
    - UK, such as: Public Interest Disclosure Act, Freedom of Information Act
    - EU nations
    - USA
- Data Protection Act combined with the General Data Protection Regulation:
    - Data controllers
    - Data processors
    - Data Protection Officers
    - Information Commissioners Office (ICO)
    - Storage and Retention of Information
    - Usage of Information

Learning outcome

2. Explain the main cryptographic techniques

Topics

2.1 Development of cryptography
2.2 Concepts and Use of Public Key and Private Key cryptography

Depth

The learner will be able to list and compare the main cryptographic techniques and identify their utility for different needs, summarizing the benefits and limitations of the listed techniques.

Topic 2.1

The key developments in cryptography:

- Substitution and Transposition ciphers:
    - Early written examples (Caesar cipher, Scytale cipher)
    - Obfuscation

    - Electro-mechanical (TypeX, Enigma, Lorenz, Poem Codes, Hagelin)
- Development of digital cryptography:
    - Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES) / Rijndael, RC4, RC5, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, WPA3, Elliptical Curve Cryptography (ECC), ElGamal
    - Public key (RSA) (Diffie-Hellman)
    - Transport Layer Security (version 1.3)
    - Future developments (Quantum cryptography)
- Contemporary usage of cryptography:
    - Data encryption in storage, in usage and in transit (disks, network)
    - Data hashing (verification of origin, passwords, look-up tables, software verification, MD5)

Topic 2.2

The concepts of public key (asymmetric) and private key (symmetric) cryptography:

- The principles of public key and private key cryptography:
    - Key distribution
    - Public key and private key typical uses
    - Kerckhoff's principle
- Concepts of public key cryptography:
    - Pairing of public and private keys
    - Encryption (Integer, logarithmic, elliptic curve)
    - Digital signing (Digital Signature Algorithm, RSA)
    - Key Escrow services
- Public Key Infrastructure (PKI):
    - Certificate Authorities
    - Domain Validation
    - Extended Validation
    - Root validation
    - Client validation
    - Revoking keys
- Concepts of private key cryptography:
    - Stream and Block ciphers
    - One-time keys
    - Problems of key distribution and key length
    - Derivation

Learning outcome

3. Describe methods of code breaking and bypassing

Topics

3.1 Code breaking concepts
3.2 Cryptographic vulnerabilities

Depth

Topic 3.1

The learner will be able to describe the concepts of code breaking and by passing, and the techniques to break or bypass cryptographic systems, such as:

- Dictionary attacks
- Frequency analysis
- Social Engineering:
    - Phishing
    - Spear phishing
    - Vishing
    - Shoulder surfing
    - Whaling
- Side channels:
    - Man in the middle
    - Power analysis
- Malware:
    - Key loggers
    - Screen monitors
- Rainbow table
- Brute force

Topic 3.2

The learner will be able to describe some of the inherent vulnerabilities in cryptographic systems, and methods that mitigate those vulnerabilities, such as:

- Human factors:
    - Negligence
    - Inadvertent behaviour
    - Malicious behaviour
- Policies and procedures:
    - Poor or unclear security policies
    - Out-dated security policies and procedures
    - Poor key management
    - Lack of communication
    - Lack of compliance monitoring and enforcement)
- Communications (poor, infrequent or unclear communications on security policies and procedures)
- Detection and verification (absence of intrusion or security breach detection)
- Out dated cryptographic techniques (failure to move on from techniques with proven vulnerabilities that are exploited)
- Key management issues:
    - Key salting
    - Key stretching
    - Key aging
    - Weak keys
    - Keys not encrypted during transmission or storage
    - Failure to clear keys after end of life

Supporting Information

Guidance for delivery

While this unit is focused on concepts, theory, terminology and knowledge of cryptography, access to videos, simulations and other demonstration aids to illustrate the concepts and application of cryptographic techniques will aid delivery.

Full advantage should be taken of video content, journal articles, and desktop pen and paper exercises (e.g., design of a cryptographic system), group discussion (e.g, description of techniques for breaking codes) and memory reinforcement techniques (e.g, word searches, quizzes) to aid learning.

Tutors may also wish to draw upon some of the main recent code-breaking attacks, such as:

- HEIST (SSL/TLS browser based attack)
- BREACH (HTTP compression exploit)
- CRIME (Authentication cookie exploit)
- BEAST (SSL/TLS exploit)
- DROWN (SSL 2.0 exploit)
- POODLE (SSL 3.0 exploit)
- FREAK (SSL/TLS protocol exploit)
- Sweet32 (3DES and Blowfish exploit)

Suggested learning resources

Books

Understanding Cryptography: A Textbook for Students and Practitioners
By Christof Paar and Jan Petzl
Published by: Springer, 2011, ISBN: 978-3642041006

Pretty Good Privacy (PGP),
1st Edition by Simson Garfinkel
Published by: O'Reilly Media, 1994, ISBN: 978-1565920989

The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography
1st Edition by Simon Singh
Published by: Fourth Estate, 1999, ISBN: 978-1857028799

Websites

BCS The Chartered Institute for IT: www.bcs.org
National Institute of Standards and Technology: https://www.nist.gov
The Institute of Engineering and Technology: www.theiet.org
Institute of Information Security Professionals: https://www.iisp.org/
BCS Information Security Specialist Group: www.bcs.org/category/19042

Journals

ITNOW: The Magazine of BCS The Chartered Institute for IT, ISSN: 1746-5702
Journal of Cyber Security: Oxford University Press, ISSN: 2057-2085

7 Sources of general information

The following documents contain essential information for centres delivering City & Guilds qualifications. They should be referred to in conjunction with this handbook. To download the documents and to find other useful documents, go to the Centres and Training Providers homepage on www.cityandguilds.com.

Centre Manual - Supporting Customer Excellence contains detailed information about the processes which must be followed and requirements which must be met for a centre to achieve 'approved centre' status, or to offer a particular qualification, as well as updates and good practice exemplars for City & Guilds assessment and policy issues.

Specifically, the document includes sections on:

- The centre and qualification approval process
- Assessment, internal quality assurance and examination roles at the centre
- Registration and certification of candidates
- Non-compliance
- Complaints and appeals
- Equal opportunities
- Data protection
- Management systems
- Maintaining records
- Assessment
- Internal quality assurance
- External quality assurance.

Our Quality Assurance Requirements encompasses all of the relevant requirements of key regulatory documents such as:

- SQA Awarding Body Criteria (2007)
- NVQ Code of Practice (2006)

and sets out the criteria that centres should adhere to pre and post centre and qualification approval.

Access to Assessment & Qualifications provides full details of the arrangements that may be made to facilitate access to assessments and qualifications for candidates who are eligible for adjustments in assessment.

The **centre homepage** section of the City & Guilds website also contains useful information on such things as:

- **Walled Garden**: how to register and certificate candidates on line
- **Events:** dates and information on the latest Centre events
- **Online assessment**: how to register for e-assessments.

Centre Guide – Delivering International Qualifications contains detailed information about the processes which must be followed and requirements which must be met for a centre to achieve 'approved centre' status, or to offer a particular qualification.

Specifically, the document includes sections on:

- The centre and qualification approval process and forms
- Assessment, verification and examination roles at the centre
- Registration and certification of candidates
- Non-compliance
- Complaints and appeals
- Equal opportunities
- Data protection
- Frequently asked questions.

Linking to this document from web pages

We regularly update the name of documents on our website, therefore in order to prevent broken links we recommend that you link to our web page that the document resides upon, rather than linking to the document itself.

8 Useful contacts

UK learners General qualification information	**E: learnersupport@cityandguilds.com**
International learners General qualification information	**E: intcg@cityandguilds.com**
Centres Exam entries, Certificates, Registrations/enrolment, Invoices, Missing or late exam materials, Nominal roll reports, Results	**E: centresupport@cityandguilds.com**
Single subject qualifications Exam entries, Results, Certification, Missing or late exam materials, Incorrect exam papers, Forms request (BB, results entry), Exam date and time change	**E: singlesubjects@cityandguilds.com**
International awards Results, Entries, Enrolments, Invoices, Missing or late exam materials, Nominal roll reports	**E: intops@cityandguilds.com**
Walled Garden Re-issue of password or username, Technical problems, Entries, Results, e-assessment, Navigation, User/menu option, Problems	**E: walledgarden@cityandguilds.com**
Employer Employer solutions including, Employer Recognition: Endorsement, Accreditation and Quality Mark, Consultancy, Mapping and Specialist Training Delivery	**E: business@cityandguilds.com**

If you have a complaint, or any suggestions for improvement about any of the services that we provide, email: **feedbackandcomplaints@cityandguilds.com**

About City & Guilds

As the UK's leading vocational education organisation, City & Guilds is leading the talent revolution by inspiring people to unlock their potential and develop their skills. We offer over 500 qualifications across 28 industries through 8500 centres worldwide and award around two million certificates every year. City & Guilds is recognised and respected by employers across the world as a sign of quality and exceptional training.

City & Guilds Group

The City & Guilds Group is a leader in global skills development. Our purpose is to help people and organisations to develop their skills for personal and economic growth. Made up of City & Guilds, City & Guilds Kineo, The Oxford Group and ILM, we work with education providers, businesses and governments in over 100 countries.

Copyright

Published by City & Guilds, a registered charity established to promote education and training

City & Guilds
5-6 Giltspur House
London EC1A 9DE
www.cityandguilds.com