Higher National Unit Specification

General information

Unit title: Cryptography: Practical Applications (SCQF level 7)

Unit code: J4BF 34

Superclass: CB

Publication date: October 2020

Source: Scottish Qualifications Authority

Version: 02

Unit purpose

The purpose of this unit is to introduce learners to the essential concepts of cryptography and explore how data encryption techniques are applied in order to maintain data security.

Cryptography is the formal study of encryption in the security of information systems. It covers the main modern cryptography methods used to secure information and focuses on the application of modern crypto systems. Learners will gain an understanding of the basic concepts of cryptography and how they are applied to ensure identity, securely transfer data as well as securing data at rest. The focus of the unit is on the concepts and applications of cryptography as opposed to the applied mathematics and the programming techniques associated with such solutions.

The unit is suitable for learners with no previous experience or those who already have some basic knowledge of cyber security and want to further develop their knowledge and skills. They will gain an understanding of how the various fundamental cryptographic primitives and protocols operate, including symmetric and public key exchange protocols and digital signature algorithms.

This unit is a **specialist** unit intended for learners with a vocational interest in cyber security cryptography. On completion of this unit, learners will be able to identify the main types of modern crypto-systems and the typical applications an organisation will apply them for. They will be able to describe the role of cryptography as a process and the main techniques in order to maintain awareness.

Higher National Unit Specification: General information (cont)

Unit title: Cryptography: Practical Applications (SCQF level 7)

Outcomes

On successful completion of the unit the learner will be able to:

1 Describe the basic concepts of cryptography.
2 Explain cryptographic methods.
3 Apply modern crypto methods for data security.

Credit points and level

1 Higher National Unit credit at Scottish Credit and Qualifications Framework (SCQF) level 7: (8 SCQF credit points at SCQF level 7)

Recommended entry to the unit

The unit is suitable for learners with no previous experience or those who already have some basic knowledge of cyber security and want to further develop their skills and knowledge. However, it would be beneficial if learners have an appreciation of information systems. This unit is particularly suitable for those working in vocational and professional areas who wish to enhance their knowledge and skills in cyber security.

It would be desirable if learners could demonstrate a basic understanding of data transfer and a basic understanding of mathematical functions and related concepts such as random number generation.

Core Skills

Achievement of this Unit gives automatic certification of the following Core Skills component:

Core Skill component Critical Thinking at SCQF level 6

There are also opportunities to develop aspects of Core Skills which are highlighted in the support notes of this unit specification.

Context for delivery

If this unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

This unit is one of several units that make up the Professional Development Award (PDA) in Cyber Resilience at SCQF level 8. This unit, ideally, should be delivered as part of the award. The unit can be delivered on a stand-alone basis.

Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

Higher National Unit Specification: Statement of standards

Unit title: Cryptography: Practical Applications (SCQF level 7)

Acceptable performance in this unit will be the satisfactory achievement of the standards set out in this part of the unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Where evidence for outcomes is assessed on a sample basis, the whole of the content listed in the knowledge and/or skills section must be taught and available for assessment. Learners should not know in advance the items on which they will be assessed, and different items should be sampled on each assessment occasion.

Outcome 1

Describe the basic concepts of cryptography.

Knowledge and/or skills

- Cryptography terms and meanings
- Confidentiality, integrity, non-repudiation, data origin authentication and entity authentication
- Historical uses of ciphers (eg enigma and Turing) in secret communications
- The role of cryptographic techniques and protocols to protect the transmission and storage of information
- Symmetrical and asymmetrical encryption systems
- Encryption and decryption

Outcome 2

Explain cryptographic methods.

Knowledge and/or skills

- The purpose and operation of symmetric encryption
- Block and stream ciphers
- Using a one-time pad (OTP) as an encryption technique
- Public-key encryption schemes
- Advantages and disadvantages of digital signatures
- Data encryption standards

Higher National Unit Specification: Statement of standards (cont)

Unit title: Cryptography: Practical Applications (SCQF level 7)

Outcome 3

Apply modern crypto methods for data security.

Knowledge and/or skills

- Encrypting data at rest with disk encryption
- Password-based authentication, password hashing
- Secure credit-card transactions over the internet
- Digital signatures
- Digital certificates
- Certification authorities

Evidence requirements for this unit

Evidence is required to demonstrate that learners have achieved the knowledge and/or skills across all outcomes. The evidence requirements for this unit are:

- Knowledge evidence — outcomes 1 and 2
- Product evidence — outcome 3

The knowledge evidence must include all the knowledge and/or skill statements of outcomes 1 and 2 and may be written or oral, or a combination of these. Evidence may be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital).

It is anticipated assessment of these outcomes would take the form of a knowledge-based written exam, assignment, presentation/interview, or a combination of these. All evidence must be produced by the learner. Authentication must be used where this is uncertain.

This evidence should be produced over the life of the unit under loosely controlled conditions (including access to resources and reference materials). The knowledge evidence may be sampled when testing is used. When testing is used, it must be controlled in terms of location, timing and access to reference materials. Learners are expected to demonstrate a breadth of understanding across all the knowledge statements: as a result, sampling need not be of a detailed nature.

The product evidence for outcome 3 should demonstrate practical competence in applying crypto-methods to a range of data scenarios (eg at rest, the learner's password-based encryption for transferring different types of data).

If a project-based approach is taken, the choice of project may be directed by the assessor by providing the learner with a topic or brief as a basis. In some circumstances, the learner could base the project around a 'real-life' scenario, possibly relating to the learner's own workplace, or an organisation with which they are already familiar. Learner-led projects should be cleared with the assessor first to ensure their suitability in terms of meeting the assessment criteria, and with the host employer (if applicable) to ensure that relevant information can be accessed and used for the purposes of assessment.

Higher National Unit Specification: Statement of standards (cont)

Unit title: Cryptography: Practical Applications (SCQF level 7)

When assessing project-based work, a checklist must be developed defining the knowledge and skills to be covered and the standards to be achieved. This will help to ensure that the assessment is valid, reliable and that the requirements of the brief are met. This should not consist of a set of tick boxes but must allow space for the assessor to reference evidence against the outcome and/or standard for each aspect of the project.

This evidence should be produced over the life of the unit under managed conditions without close supervision, although guidance and support may be provided by the assessor.

The level of this unit (SCQF level 7) provides additional context on the nature of the required evidence and the associated standards. The following level descriptors are particularly relevant to the evidence.

- An overall appreciation of the body of knowledge that is embedded in the main theories, concepts and principles
- Apply knowledge and skills in practical contexts
- Use some of the basic and routine professional skills, techniques, practices and materials
- Use a range of approaches to address defined and/or routine problems
- Exercise initiative and independence in carrying out defined activities at a professional level
- Take account of own and others' roles and responsibilities when carrying out tasks

These level descriptors should be used (explicitly or implicitly) when making judgements about the evidence.

When evidence is produced in uncontrolled or loosely controlled conditions it must be authenticated. The 'guide to assessment' provides further advice on methods of authentication.

The 'guidelines on approaches to assessment' (see the support notes section of this specification) provides specific examples of instruments of assessment.

Higher National Unit Support Notes

Unit title: Cryptography: Practical Applications (SCQF level 7)

Unit support notes are offered as guidance and are not mandatory.

While the exact time allocated to this unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this unit

The context for this unit is the recognition at national level of the importance of embedding cyber security knowledge and skills across the workforce in every sector. In order to improve the cyber resilience of organisations then raising the awareness of cryptography and the application of modern crypto systems is important in increasing organisational capability to better protect against cyber security threats and to defend information systems and assets. Cryptography is a large part of most enterprise-wide cyber security strategies.

The main purpose of this unit is to provide learners with the knowledge and skills to understand the core concepts of cryptography. Learners undertaking this unit need not cover topics in a detailed nature. It is important however that good coverage is given to each of the knowledge statements in order to provide the learner with a broad view of the outcomes and the steps taken throughout each of the processes. The assessor must ensure that learners are understanding the key characteristics of cryptography, and the encryption processes used to implement them. Learners should develop an overall appreciation of modern crypto systems.

This unit encourages the learner to become knowledgeable in the main applications of cryptography such as for secure messaging, password-based authentication, secure credit-card transactions over the internet, digital signatures and disk encryption.

The unit is useful for those wanting to better understand cyber security in relation to the practical application of modern cryptography and those who may intend to work in either a technical or non-technical business role, educational role or service role.

Please note that the following guidance, relating to specific outcomes, does not seek to explain each knowledge/skills statement, which is left to the professionalism of the assessor. It seeks to clarify the statement of standards where it is potentially ambiguous. It also focuses on non-apparent teaching and learning issues that may be over-looked, or not emphasised, during unit delivery. As such, it is not representative of the relative importance of each knowledge/skill.

Higher National Unit Support Notes (cont)

Unit title: Cryptography: Practical Applications (SCQF level 7)

Outcome 1: The primary objective relating to this outcome is to build an underpinning knowledge of the basic concepts of the practical applications of cryptography and acts as a foundation for the later outcomes. Learners will understand the process of encryption and decryption and key cryptography terms and meanings. Learners will explore historical uses of ciphers (which are algorithms for performing encryption or decryption) such as enigma and Turing in secret communications.

Learners will understand the application of cryptographic techniques and protocols to protect the transmission and storage of information, provide confidentiality, integrity, protected message exchanges, data origin authentication, entity authentication and non-repudiation.

Learners will appreciate the role of cryptographic techniques and protocols to protect the transmission and storage of information and be introduced to symmetrical and asymmetrical encryption systems.

Useful resources may include:

International Standards Organisation (ISO) guidance, including:

ISO27001 How to use the cryptography according to ISO 27001
ISO/IEC 19790:2012 Information technology — Security techniques — Security requirements for cryptographic modules

The Secret History of Cryptography:
https://www.theneweconomy.com/technology/the-secret-history-of-cryptography

Cryptography — A quick guide:
https://www.tutorialspoint.com/cryptography/cryptography_quick_guide.htm

Outcome 2: The primary objective relating to this outcome is to develop an understanding of the role and purpose of encryption methods including: symmetric encryption; block and stream ciphers; one-time pad; public key encryption and digital signatures. Learners will learn that stream ciphers and block ciphers are two encryption/decryption algorithms that belong to the family of symmetric key ciphers. They will explore using a one-time pad (OTP), an encryption technique that cannot be cracked but requires the use of a one-time pre-shared key. As a result, one-time pad ciphers have been used by nations for critical diplomatic and military communication, but the problems of secure key distribution have made them impractical for most other applications. Learners will learn the important properties of the public key encryption scheme, including that different keys are used for encryption and decryption and that there are three types of public key encryption schemes: RSA Cryptosystem; ElGamal Cryptosystem and Elliptic Curve Cryptography (ECC).

They will learn that a digital signature is a digital identity that can be associated with a user. Digital signatures generally use asymmetric cryptography. Learners will appreciate the role of data encryption standards.

Higher National Unit Support Notes (cont)

Unit title: Cryptography: Practical Applications (SCQF level 7)

Useful resources may include:

What Is Symmetric Key Cryptography?:
https://www.binance.vision/security/what-is-symmetric-key-cryptography

An Introduction to Stream Ciphers vs Block Ciphers:
https://www.jscape.com/blog/stream-cipher-vs-block-cipher

Difference-between-block-cipher-and-stream-cipher:
https://www.geeksforgeeks.org/difference-between-block-cipher-and-stream-cipher/

One-Time Pad (OTP) — The unbreakable code:
https://www.cryptomuseum.com/crypto/otp/index.htm

IEEE P1363 covers most aspects of public-key cryptography

Advantages and Disadvantages of Digital Signature:
https://lerablog.org/technology/data-security/advantages-and-disadvantages-of-digital-signatures/

Comparing ECDSA vs. RSA:
https://www.ssl.com/article/comparing-ecdsa-vs-rsa/

Outcome 3: The primary objective relating to this outcome is to develop an understanding of the applications of cryptography in common scenarios. Learners will appreciate that cryptography is used in two different ways: keeping a secret (where you want to either send some information to someone else, or you want to store information in a way that prevents others from accessing it) and proving identity.

Learners will explore applications of cryptography including electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Useful resources may include:

Basics of Cryptography: the practical application and use of cryptography:
https://resources.infosecinstitute.com/basics-of-cryptography-the-practical-application-and-use-of-cryptography/

Guidance on approaches to delivery of this unit

A practical, hands-on approach to learning should be adopted in order to engage learners and exemplify key concepts.

At this level, learning should be mainly led by the learner, with some assessor intervention. It is anticipated that some initial introduction and explanation will be required for each outcome. However, there is significant scope for learners to research and explore the topics once this initial seeding has taken place. Assessors should expect a significant amount of independent learning to take place and support learners with this where appropriate.

The outcomes should be undertaken in order with outcome 1 attempted first, then outcome 2 and outcome 3 last.

Higher National Unit Support Notes (cont)

Unit title: Cryptography: Practical Applications (SCQF level 7)

A suggested distribution of time across the outcomes is:

Outcome 1: 12 hours
Outcome 2: 12 hours
Outcome 3: 16 hours

Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable for learners.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

Assessment of knowledge evidence could be achieved by a combination of the evidence-based assessment utilising the differentiated instruction methods described above and traditional multiple-choice questions. In some circumstances, it may be more practical to carry out the entirety of the knowledge assessment with a traditional multiple-choice based approach.

The knowledge evidence for outcomes 1 and 2 could be assessed by*:*

1 Individual or small group presentations including exercises around the analysis of use cases. The rubric should account for elements such as: overall demonstration of understanding of the topic covered or the use case provided; thoroughness of content; accuracy of content; sequencing of content; appropriate levels of sophistication; originality; sourcing of references; and overall quality of the delivery of the presentation.

2 Online or paper-based selected-response test comprising 30-40 questions with one correct response and three distractors for each question. The test should cover all the knowledge and/or skills statements across all the outcomes with at least one question for each statement.

A more contemporary approach to assessment would involve the use of a web log (blog) to record learning (and the associated activities) throughout the life of the unit. The blog would provide knowledge evidence (in the descriptions and explanations). The blog should be assessed using defined criteria to permit a correct judgement about the quality of the digital evidence. In this scenario, every knowledge and skill must be evidenced: sampling would not be appropriate.

Learners should be encouraged to complete formative assessments in a closed-book manner then use any books or reference materials for the course to check their responses. Learners should be able to complete formative assessments at any time and repeat them as often as needed. In some instances, assessors may want to collect learner responses to formative assessments for the purposes of gauging the overall master level of the cohort group as mentioned above. In addition to this traditional approach to formative assessment, learners may also achieve the same outcomes and provide the same level of gauging for assessors via the blog-based approach.

Higher National Unit Support Notes (cont)

Unit title: Cryptography: Practical Applications (SCQF level 7)

Traditional multiple-choice based summative assessments should be delivered under supervision by appropriate personnel in a closed-book environment.

Where possible and practical, learners should be provided with the opportunity to present their knowledge directly to the rest of their peers, either through in-classroom discussions and presentations, if applicable, or their blog posts.

The assessment for outcome 3 could be assessed through an open-book practical assignment.

The practical assignment could involve research or an investigative approach, eg learners using their knowledge and skills to apply crypto-methods to a range of data scenarios (eg at rest, password-based encryption for transferring different types of data). They could deliver a set of encryption guidelines and test these against real or simulated scenarios, possibly relating to the learner's own workplace, or an organisation with which they are already familiar. However, due to the likely sensitive nature of the information required from a real-life case, it is recommended that assignments relating to any real context are cleared with the employer and assessor first to ensure both their suitability in terms of meeting the assessment criteria and the practicalities of accessing information.

An assessor checklist could be used to verify completion of the practical assessment. Assessors should take reasonable steps to ensure that the work an individual learner submits for assessment is their own, for example, by asking them to sign a declaration.

There are opportunities to carry out formative assessment at various stages of the unit. For example, formative assessment could be carried out on the completion of each outcome to ensure that learners have grasped the knowledge contained within it. This would provide assessors with an opportunity to diagnose misconceptions and intervene to remedy them before progressing to the next outcome.

Summative assessment may be carried out at any time. However, when testing is used it is recommended that this is carried out towards the end of the unit (but with enough time for remediation and re-assessment). When continuous assessment is used, this could commence early in the life of the unit and be carried out throughout the duration of the unit.

Opportunities for e-assessment

E-assessment may be appropriate for some assessments in this unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all learner evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

Higher National Unit Support Notes (cont)

Unit title: Cryptography: Practical Applications (SCQF level 7)

Opportunities for developing Core and other essential skills

Although this unit does not embed any Core Skills, there are opportunities to develop Core Skills in *Communication, Problem Solving* and *Information and Communication Technology (ICT)*.

All outcomes involve research led problem solving and use of ICT systems to conduct research to identify the types of cryptography techniques.

In addition, all outcomes should provide opportunities to practise writing clearly and simply, which will contribute to the Core Skill component of Written Communication.

The unit will also provide opportunities to develop broader skills, such as analytical thinking, which will be required when learners functionally decompose learning objectives.

The Critical Thinking component of Problem Solving at SCQF level 6 is embedded in this unit. When a learner achieves the unit, their Core Skills profile will also be updated to include this component.

History of changes to unit

Version	Description of change	Date
02	Core Skills Component Critical Thinking at SCQF level 6 embedded.	06/10/20

General information for learners

Unit title: Cryptography: Practical Applications (SCQF level 7)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This unit is suitable for you whether you have no previous experience or already have some basic knowledge of cyber security and want to further develop your knowledge and practical skills in this increasingly important field. No previous knowledge of cyber security is required before you begin this unit. However, it would be advantageous for you to have a basic understanding of computer systems, computer networks and cyber security. The unit is particularly suitable for those already working in vocational and professional roles who wish to enhance their knowledge and skills in cyber security.

The purpose of this unit is to introduce you to the essential concepts of cryptography and explore how it is implemented in data encryption techniques. This is a specialist unit intended for learners with a vocational interest in computing or Science, Technology, Engineering and Mathematics (STEM), however, any learner may benefit from developing an understanding of cryptographic principles and how they are applied in practice.

You will gain an understanding of the basic concepts of cryptography and how they are applied to securely transfer data as well as ensure identity. The focus of the unit is on the concepts and applications of cryptography as opposed to the applied mathematics and the programming techniques associated with such solutions.

The unit covers the theoretical and practical aspects of the overall process that encompass cryptography. The unit broadly covers the following topics:

- Understand the essential components, principles and historical aspects of cryptography
- Understand the fundamental principles and applications of symmetric encryption to provide an improved cyber security posture
- Understand the fundamental principles and application of public-key encryption to provide an improved cyber security posture
- Understand the application of cryptographic techniques and protocols to protect the transmission and storage of information, provide confidentiality, integrity, protected message exchanges, data origin authentication, entity authentication and non-repudiation
- Identify and explain digital signatures, their operation and application
- Identify and understand the requirements to implement cryptographic applications

Teaching methodologies for this unit incorporate a variety of techniques, in active, project-based and collaborative learning, and can be assessed in a variety of ways; for example, completing a case study project or by more contemporary means, such as a blog or e-portfolio, to showcase your work.

There will be opportunities for you to develop Core Skills in *Communication, Information Communication Technology (ICT)* and *Problem Solving*.

This unit is delivered as an optional unit in the Professional Development Award (PDA) in Cyber Resilience at SCQF level 8. By the end of the unit you will have learned the importance of using cryptography to secure transmission and storage of information. On completion you may be able to progress to further study at SCQF level 9, broader HNC/HND qualifications in cyber security and a range of industry certifications.

General information for learners

Unit title: Cryptography: Practical Applications (SCQF level 7)

The Critical Thinking component of Problem Solving at SCQF level 6 is embedded in this unit. When a learner achieves the unit, their Core Skills profile will also be updated to include this component.