

A nighttime photograph of a city skyline, likely Dubai, with numerous skyscrapers illuminated. A large, semi-transparent white letter 'D' is overlaid in the center of the image. The lights from the buildings are reflected in the water in the foreground.

ID3 Services Limited

Cryptography and Blockchain

About the Course Presenter

The ID-3 training partner Dr Blundell is crypto specialist with a PhD in cryptography and mathematics from Royal Holloway, University of London. A cryptographer in both the telecommunications and defence sectors, and an example of an academic paper authored and published while working in industry can be found here.

One day Cryptography and Blockchain Course

Course Overview

Blockchain is a distributed list of events or transactions that is secured cryptographically. It was first implemented and widely adopted as a cryptocurrency, starting with Bitcoin. But its use has broadened to other applications such as smart contracts.

Cryptography is a set of fundamental security techniques with application ranging from protecting personal and commercial information using encryption, e-commerce, secure communication and network security.

This crypto and Blockchain course looks at Blockchain from a cryptographic perspective. It first looks at the set of core techniques that make up cryptography, including their functions and properties, and how they are used together to achieve different cyber security objectives.

All of the core techniques are covered, but with an emphasis on those parts more relevant to Blockchain. Also included are zero-knowledge protocols and homomorphic encryption, both relevant to Blockchain in the form of zkSNARKs. Finally, building on the topics covered already, the course looks at Blockchain itself and how it works.

Course Objectives

- Cryptography: Develop a broad knowledge that can be applied across many different security applications; establish a solid foundation on which to make judgements or assessment of secure systems; appreciate the cryptographic components on which Blockchain and its applications rely
- Blockchain: recognise what it does, how it works and its implications

Course Description

The course assumes no prior knowledge and includes the following:

- Cryptographic services
- Design principles
- Cipher types and characteristics
 - Symmetric ciphers & encryption: provably secure encryption; stream ciphers; block ciphers (including DES and AES); modes of operation; Message Authentication Codes (MACs)
 - Public key systems, including Diffie-Hellman and RSA
- Hash functions, zero-knowledge protocols, homomorphic encryption
- Digital Signatures
- Key management, including generation, distribution, storage, PKI and certificates
- Blockchain
 - What it does and how it works
 - Its implications
 - Cryptographic strengths
 - ZKSNARKs

Who Should Attend

Anyone with an interest in cyber security, cryptography and Blockchain, such as:

- Those with responsibility or oversight for managing, assessing or defining policy for cyber security and new applications
- Blockchain developers
- Those responsible for implementing security operations or secure applications such as Blockchain

Course Style

Location friendly and Face-to-face.