Certificate

Cryptography

User **Rene@Karkkainen.net** has completed **100%** of section **Cryptography**.

100 %

Description:

From the history of cryptography to current use, the basics of encryption, technologies, applications and their impact on security.

Completed modules:

- What is cryptography? Basic concepts and uses
- Caesar Cipher: The Ancient Code That Changed Communication
- The Enigma Machine: How WWII Codebreakers Unlocked the Greatest Mystery of the War
- Checksums

- What are hash functions and what are they used for?
- Cracking Hashes: How Does It Work?
- MD5 hash - a broken classic
- PBKDF2, BCrypt, SCrypt and Argon2
- SHA2 vs SHA3 vs PBKDF2 vs bcrypt vs SCrypt vs Argon2: Which to choose for password storage?
- What is MAC and why is it needed?
- Different MAC algorithms
- Random numbers in cryptography
- What is symmetric cryptography?
- Block Ciphers
- DES, 3DES and AES
- Stream Ciphers
- Initialization vector (IV) and its vulnerabilities in cryptography
- What is asymmetric cryptography?
- Digital signatures
- Key exchange algorithms
- Encoding methods
- TLS (Transport Layer Security): The foundation of Internet security
- Certificates: Building blocks of digital trust
- Public Key Infrastructure (PKI): The Foundation of Digital Trust
- TLS Building Blocks: Cipher Suites
- SSL/TLS threats
- What is key management and why is it important?
- Key management in cloud services: AWS, GCP and Azure

- On-Premise Key Management with HashiCorp Vault
- CertBot and automatic renewal of certificates
- HSM modules
- TPM modules
- Auditing SSL/TLS settings with Qualys' SSL Labs scanner
- Auditing SSH settings with Nmap
- CyberChef - A browser-based cryptographic Swiss army knife