Post Quantum Cryptography Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Post-quantum cryptography is no longer just a futuristic concept, but a necessity in the present day. Anyone who works in the field and ignores its principles and techniques could be left at a severe disadvantage. This course offers a comprehensive overview of post-quantum cryptography.

Day 1 explores quantum-based attacks, lattices, and their applications in schemes and key exchange. Day 2 delves into error-correcting codes, isogenies, and their security implications. Day 3 covers the MQ problem, various schemes, including oil and vinegar, rainbow, and their cryptanalysis.

Other candidates, such as hash-based signatures and MPC-in-the-head signatures, and side-channel attacks, are also discussed. Participants will gain a thorough understanding of post-quantum cryptography and its potential impact on modern cryptography.

High Level Overview of the class topics;

- Introduction to post-quantum cryptography
- Attacks on DLOG and factoring
- Lattices and related algorithms
- LWE and Regev's encryption scheme
- NTRU and NTRUPrime
- Codes and cryptosystems
- Isogenies and elliptic curves
- MQ problem and its variants
- Other candidates for PQC
- Side-channel attacks and countermeasures

Prerequisites

General knowledge of cryptography.

What You Will Learn

You will;

- Be able to evaluate the security of different cryptographic primitives
- Be able to select suitable cryptographic algorithms for their specific use case and deployment scenario
- Have practical experience implementing and using post-quantum cryptographic schemes
- Understand the mathematical foundations of post-quantum cryptography
- Be familiar with the state-of-the-art in post-quantum cryptography
- Possess knowledge and skills to defend against side-channel and physical attacks on cryptographic implementations