Einführung in die Kryptologie

Ziel und Zielgruppe:
Ziel der Schulung ist die Vermittlung von grundlegenden Kenntnissen der Kryptologie. Im ersten Teil der Schulung werden historische Verschlüsselungsverfahren (wie bspw. die Cäsar-Chiffre) vorgestellt, deren Schwächen aufgezeigt und konkrete Angriffe durchgeführt.
Im zweiten Teil werden aktuelle kryptografische Verfahren und deren Designprinzipien vorgestellt. Dazu gehören u.a. AES (Advanced Encryption Standard), RSA (Rivest, Shamir und Adleman) und ECC (Elliptic Curve Cryptography). Abschließend werden als typische Anwendungsszenarien Digitale Zertifikate (X.509), Digitale Signaturen und PKI (Public-Key-Infrastruktur) vorgestellt.

Für die Teilnahme an der Schulung existieren keine formalen Voraussetzungen. Die Schulung ist sowohl für Anfänger, als auch für fortgeschrittene Anwender geeignet und als Vorbereitung auf HSM-Schulungen sinnvoll.

Rahmen:
Schulungsumfang: 1 Tag
Teilnehmer: 4-6 Personen
Uhrzeit: 09:30 - 18:00 Uhr
Ort: Düsseldorf
Schulungsgebühr: 950 Euro / Person

Schulungsinhalte:

- Historische Kryptographie
  - Cäsar-, Substitutions-, Permutations-, Polyalphabetische- und Vigenère-Chiffren
  - Funktionsweise Enigma
- Moderne Kryptographie
  - Hash Algorithmen (MD5, SHA-1 und SHA-2)
  - One-Time-Pad
  - Symmetrische Kryptographie (DES, 3DES und AES)
  - Asymmetrische Kryptographie (RSA, ECC, Digitale Signaturen)
  - Hybride Kryptographie
  - Key Agreement (Diffie-Hellman)
  - PKI (CA und X.509-Zertifikate)