cryptosolutions

An der Ziegelei 17
45133 Essen

contact@cryptosolutions.de
cryptosolutions.de

Advanced Cryptography Training
Symmetric Cryptanalysis

Are you curious, why the Advanced Encryption Standard (AES) is todays most-trusted encryption scheme? Have you ever wondered, what can go wrong when designing your own cipher and do you want to learn how to do it correctly? Or would you like to learn how to break a weak cipher?

In this advanced cryptography training on symmetric cryptanalysis techniques, you will find out.

Goals After completing this training, you will

- thoroughly understand the security of AES and know the purpose of typical components used in symmetric ciphers,
- have applied standard cryptanalysis techniques, such as differential and linear cryptanalysis, and understood their mechanics,
- be able to assess basic security guarantees of block ciphers.

Structure The training builds upon not only theoretical parts, but also emphasizes practical parts and thus consists of

- *lectures*, which presents technical topics,
- *practical exercises*, to support the individual understanding,
- (optionally) an *extended project*, to deepen the gained knowledge and practice the covered techniques beyond the initial training session.

Prerequisites For a successful participation, we recommend a basic math understanding, a laptop, and (optionally) a working SageMath installation for the exercises.

Join us in following this fascinating path and find out how deep the rabbit hole goes.

For more information, please get in

contact@cryptosolutions.de