

Implementation of Format-Preserving Encryption

Advisor: **Oliver Popa**

Motivation

Format-Preserving Encryption (FPE) enables encryption for applications where input validation is critical, but were originally designed to expect a plaintext of a specific format (e.g. credit card numbers, verification codes). FPE schemes are designed to preserve the original format for the encrypted message and provide confidentiality without redesigning existing applications.

Recently, a new family of length- and format-preserving ciphers, called ALF, was introduced. Its main construction ALF-n-t, supports block sizes from 16 to 127 bits and targets 128-bit security against key-recovery attacks. The family also includes ALF-0 and ALF-1-t for smaller plaintext domains, ALF-16-t for larger domains, and ALF-L for longer plaintexts of arbitrary binary width. The designers additionally introduce a new transformation that turns the ALF-n-t variants into format-preserving ones.

In this project, you will extend an existing Python implementation of ALF with support for format-preserving encryption.

Goals and Tasks

- Get familiar with FPE and the idea behind the ALF cipher suite
- Implement the format-preserving variants of ALF
- Evaluate and analyze your implementation

Literature

- M. Bellare et al.
  Format-Preserving Encryption
  SAC 2009
  doi:10.1007/978-3-642-05445-7_19
- D. Wang, A. Maximov, and T. Johansson
  Introducing the ALF Family: AES-NI-Based Length- and Format-Preserving Encryption
  IACR Transactions on Symmetric Cryptology 2026
  doi:10.46586/tosc.a0iv7t4tdypv

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in cryptography
- Programming (mainly Python)

Advisor Contact

oliver.popa@tugraz.at