A Hands On Introduction to Symmetric Key Cryptanalysis

Eran Lambooij

March 11, 2020

1 Introduction

In this course we discuss basic symmetric-key cryptanalysis concepts and techniques. We use this knowledge to break toy and real-world ciphers. This includes Meet-in-the-Middle attacks, differential cryptanalysis, and linear cryptanalysis. Apart from the cryptanalysis we also discuss how to implement the attacks. Since this course focuses on both practical and theoretical attacks, a solid understanding of programming and data structures is needed as well as (some) affinity with cryptography. The course has 2 hours of lectures and 3 hours of homework exercises a week. In the end there will be a 20-hour final project focussing on implementing a state of the art attack. The course is given in **English**.

2 Learning objective

The goal of this course is to provide the student with sufficient knowledge to conduct basic cryptanalysis on real-world ciphers. The course studies Meet-in-the-Middle attacks, differential and linear cryptanalysis in depth and touches lightly on some more advanced concepts. Apart from a theoretical understanding of the attacks, the student also learns how to implement these attacks. After the course is finished the student should be able to break (simplified) symmetric encryption schemes.

3 Prerequisites

- Algebra 1
- Data Structures
- Intro to Cryptography or Computer & Network Security

4 Grading

The course has both weekly exercises and a final project. The average of the weekly exercises counts for 50% of the final grade and the grade of the final project counts for 50% of the final grade. The weekly exercises may be done in pairs, the final project is **individual**.

5 Schedule

Week 1 In this lesson we first make sure that everyone is aware of the basic concepts used throughout the course. We discuss the attacker model, and what is expected in terms of course obligations. We also look briefly at the design and implementation of AES. A first exercise is given to asses the knowledge of programming and to get the student acquainted with some common constructions.

Week 2 In this lesson we cover basic MitM attacks and how to efficiently implement them. We will attack a toy cipher using the MitM technique and discuss what can be done to mitigate the attack from a design perspective. The exercise for this week focuses on developing and implementing an attack for a toy cipher using the MitM technique.

Week 3 In this lesson we cover some more advanced techniques for MitM attacks, how to (automatically) search for MitM attacks, and how to implement both the search and more sophisticated attacks. The exercise for this week focuses on the implementation of searching for good MitM attacks for a toy cipher.

Week 4 In this lesson we cover basic differential distinguishers and key recovery attacks using differential distinguishers based on single characteristics. This week's exercise focuses on implementing a differential attack on a toy cipher.

Week 5 In this lesson we introduce the concept of differentials and cover how to find good differential characteristics using SAT solvers. This week's exercise is to find good differentials for a toy cipher.

Week 6 In this lesson we look at the differential cryptanalysis of real-world ciphers and touch on further techniques to improve the basic attacks. We also discuss the final project. This week does not have an exercise.

Week 7 In this lesson we introduce the concept of linear cryptanalysis. We look at how linear cryptanalysis attacks can be implemented. This week's exercise focuses on implementing a simple linear attack on a toy cipher.

Week 8 In this lesson we look at how to find good linear attacks using SAT solvers and introduce the concept of linear hulls. In this week's exercise we find good linear hulls using a SAT solver.

Week 9 In this lesson we look at some advanced concepts in linear cryptanalysis and how they can be used to attack existing ciphers. This week does not have an exercise.

Week 10 In this lesson we look at how we can implement attacks which use high amounts of data, time, and memory. We look at common data structures and how they impact our attacks. We also look at how we can optimize the cipher for use in cryptanalytic attacks. The exercise for this week is to do some high load computations (like finding two orthogonal vectors in a big set of vectors) as fast as possible.

Week 11 In this lesson we look at how we can speed up the cryptanalytic attacks discussed earlier by using vectorization and parallelism. We look at how certain constructions can vectorized and implemented efficiently. This week's exercise is to make a vectorized implementation of an attack.

Week 12 Question session, no exercise.

6 Reading Material

- The Block cipher Companion. L.R. Knudsen, M. Robshaw
- Understanding Cryptography by C. Paar, J. Petzl
- Differential Cryptanalysis of DES-like Cryptosystems. E. Biham, A. Shamir, Journal of Cryptology 4(1), 1991
- Linear Cryptanalysis Method for DES Cipher. M. Matsui, Eurocrypt 1993
- All Subkeys Recovery Attack on Block Ciphers: Extending Meet-in-the-Middle Approach. T. Isobe, K. Shibutani, Selected Areas in Cryptography 2012
- Handbook of Applied Cryptography, A.J. Menezes, P.C. van Oorschot, S.A. Vanstone