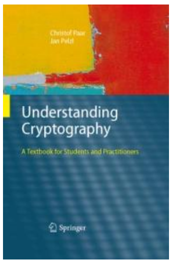

Student Projects

Understanding Cryptography,

A Textbook for Students and Practitioners

by Christof Paar and Jan Pelzl

www.crypto-textbook.com

ver. January 3, 2011

In the following, ideas for projects are provided that dovetail nicely with our book. We distinguish between three types of projects:

1. "Written report" – the focus is on learning about a certain topic which is not too theoretical, and to provide a well written report on the subject. In many cases 10-20 pages are appropriate
2. "Research" – the focus is on understanding new theoretical concepts and to describe them.
3. "Programming" projects require writing of software. Since the descriptions are rather generic, we do not mandate a certain programming language.

For all projects researching previous work, which are often scientific publications, is necessary so that students get experience with working with original literature. Good starting points for many projects are the "Discussion and Further Reading" sections at the end of each chapter.

Our project descriptions are often rather broad and allow the student to set her/his own focus. Instructors who prefer more finely defined projects are encouraged to use this compilation as a starting point and to add specific references which the students should use.

Christof Paar and Jan Pelzl

Chapter 1 – Introduction to Cryptography and Data Security

1.1 **Enigma Break** [Research + written report] The break of the Enigma encryption machine in WW II is probably the most famous cryptanalytic event in recent history. Your task is (i) to describe how the Enigma machine worked and (ii) to describe how the machine was broken by the Polish/British/American intelligence services. Part (ii) is the more challenging one.

1.2 **Attacks in Network** [Written report] In Figure 1.6 of *Understanding Cryptography* attacks against cryptographic schemes are summarized. Security solutions, e.g. secure web browsing or hard disk encryption, are usually complex and cryptographic algorithms are only one part of the overall system. Consequently, there are many more attacks possible against security systems which do not necessarily target the crypto algorithms per se, e.g., phishing attacks or botnets. Provide a comprehensive written report about attacks that are currently possible against IT security systems. You may want to focus on attacks against computer networks and the Internet.

Chapter 2 – Stream Ciphers

2.1 **eSTREAM** [Written report, possibly with programming, possible with research] Describe the 4-year eSTREAM effort. First there should be a description of the eSTREAM *process*, including motivation for eSTREAM, description of the different stages of eSTREAM, description of the ciphers submitted etc. You may want to highlight the differences between eSTREAM and the AES selection process. Second, focus on one or two of the eSTREAM candidates and describe them in detail. An option is to program the selected cipher(s) in your favorite programming language. Another option is to focus on one of the broken eSTREAM submissions and describe the attack.

2.2 **GSM Encryption** [Written report, possible with research] Describe the various security mechanisms in the GSM mobile communication standard. As a major part of the report should be a description of the voice encryption algorithms A5/1, A5/2 and Kasumi. Do also address the weaknesses/attacks against these ciphers.

2.3 **GSM Encryption** [Research, possible with programming] Research the various attacks against A5/1 and describe one of the attacks. You can do a partial implementation of the attack.

Chapter 3 – The Data Encryption Standard (DES) and Alternatives

3.1 **Cryptanalytical Hardware and DES** [Written report with some research] Describe the various brute-force attacks proposed against DES over the decades. (You do not have to address the analytical attacks, differential and linear cryptanalysis.) Pay special attention to the details used for Deep Crack and COPACOBANA.

3.2 **Differential Cryptanalysis** [Research] Learn about differential cryptanalysis and show how it applies to DES or another block cipher of your choice.

3.3 **Lightweight Cryptography** [Written report] Describe what is understood as lightweight cryptography (a recent trend in block cipher design). As a major part of the project, describe the pros and cons of promising lightweight ciphers, including (but not limited to) Clefia, HIGHT, mCrypton and PRESENT.

Chapter – The Data Encryption Standard (DES) and Alternatives

4.1 **Fast Software Implementations: Bit Slicing** [Programming] Describe how bit slicing works and how it can be applied to AES. Provide a bit-slices implementation of AES in your favorite programming language.

4.2 **Hardware Implementation** [Written report with some research] Describe the various proposals to implement AES in hardware from the literature since the late 1990s. The general options you may want to describe are: High-speed architectures based on pipelining and loop-unrolling, very small architectures on FPGAs, lightweight implementations for RFID. A theoretically interesting part are ways of realizing the AES S-box with few gates using tower field (aka composite field) representations for GF(2^8).

4.3 **AES Attacks** [Mainly mathematical research] Describe the analytical attacks proposed against AES.

Chapter 5 – More about Block Ciphers

5.1 **Modes of Operation** [Written report] Describe the modes of operation for block ciphers recommended by NIST and highlight the pros and cons for the various modes. In particular, address the theoretical limitations of modes provided by the field of provable security.

5.2 **Advanced Brute Force Attacks** [Research] Describe how time-memory trade-off attack works, including the important concept of distinguish points. More advances students should also describe rainbow tables.

Chapter 6 – Introduction to Public-Key Cryptography

6.1 **Alternative Public-Key Schemes** [Research] There are four families of alternative public-key schemes that are potentially interesting for use in practice: (1) hash-based, (2) code-based, (3) lattice-based and (4) multivariate quadratic (MQ) public-key algorithms. Choose one of the algorithm families and describe how they work and what they pros and cons are relatively to RSA.

Chapter 7 – The RSA Cryptosystem

7.1 **Factoring Algorithms** [Research, quite mathematical] Learn about factoring algorithm and describe the various algorithms. (There are several good books on factoring available.) For more advanced and mathematical-leaning students: describe the principle about number field sieves, the most powerful family of factoring algorithms which was used in the most recent factoring attacks.

7.2 **RSA Software Implementation** [Research, optional implementation] Research and describe the most popular algorithms to accelerate RSA implementations in software: Sliding window exponentiation, long number modular multiplication using the Montgomery algorithm, and the Karatsuba method for fast multiplication. Note that all 3 algorithms are unrelated and accelerate different parts of the RSA computation.

7.3 **Timing Attacks** [Research] Research and describe how timing attacks work against RSA.

Chapter 8– Public-Key Cryptosystems Based on the Discrete Logarithm Problem

8.1 **DL Attacks: Pollard-Rho** [Research] Describe how the Pollard-Rho attack works against generic DL schemes.

8.2 **DL Attacks**: Index-Calculus [Research] Describe how the index-calculus attack works against DL problems in prime fields.

Chapter 9 – Public Elliptic Curve Cryptosystems

9.1 **ECC History** [Written report] Write a summary and discuss the article:
Ann Hibner Koblitz, Neal Koblitz, and Alfred Menezes. Elliptic curve cryptography: The serpentine course of a paradigm shift. Cryptology ePrint Archive, Report 2008/390, 2008.

9.2 **ECC Implementation** [Programming] Implement a basic elliptic curve crypto system with one of the curves over prime fields standardized by NIST. Use the GNU MP long number library for this.

9.3 **Special primes** [Research and written report] Part (i) Describes how generalized Mersenne primes (aka Solina's primes) can be used for fast modular reduction for ECC systems. Part (ii) Describe how optimal extension fields (OEFs) can be use for fast ECC implementations. Literature for the latter: *D. Bailey, C. Paar, "Efficient Arithmetic in Finite Field Extensions with Application in Elliptic Curve Cryptography", Journal of Cryptology, 2001.*

Chapter 10 – Digital Signatures

10.1 **TESLA Signature Scheme** [Research and written report] A digital signature scheme entirely different from the conventional number theoretical algorithms (i.e., RSA, DL, ECC) is the TESLA authentication scheme. Research TESLA, describe its functioning and its pros and cons relatively to the.

10.2 **Hash-based signatures** [Research and written report] Another digital signature scheme entirely different from the conventional number theoretical algorithms (i.e., RSA, DL, ECC) are schemes based on hash chains. Research them and describe their functioning and its pros and cons relatively to the.

Chapter 11 – Hash Functions

11.1 **SHA-3** [Written report, possibly with programming, possible with research] Describe the ongoing SHA-3 competition administered by NIST. An option is to select one (or more) hash functions and to program them in your favorite programming language. Another option is to focus on one of the broken hash function and describe the attack.

11.2 **MD5 Attack** [Research and written report] Research the attacks against the MD5 hash function. In addition to describing the attack, judge how serious they are in practice. This is a quite mathematical project.

Chapter 13 – Key Establishment

13.1 **SSL/TLS Protocol** [Written report] Describe how SSL/TLS works. Address issues such as the different key establishment mechanisms and the role that certificates play.

13.2 **Chain of Trust vs. Certificates** [Written Report] Describe how a chain of trust work. What are the pros and cons of it relatively to certificates