Preface

Algebraic Cryptanalysis is the process of breaking codes by solving polynomial systems of equations. In some ways this book began when the author began to explore cryptanalysis as a beginning graduate student, and realized with frustration that no book whatsoever existed on the topic. Since that time, some books have been written about Linear Cryptanalysis or Differential Cryptanalysis (e.g. [211] and [214] cover both), but none on Algebraic Cryptanalysis, which is a rich and growing field.

The author had some difficulty entering the field of Algebraic Cryptanalysis. Of course step one is a solid background in Abstract Algebra, and a solid background in cryptography[1]. But after these twin foundations, one is not quite ready to read research papers. This book is intended to be that stepping stone for graduate students wishing to do their dissertation in Algebraic Cryptanalysis, or any other part of cryptanalysis. Furthermore, researchers in other areas of Applied Abstract Algebra or cryptography might benefit from seeing what is going on in cryptanalysis.

The nucleus for the book was my dissertation, under the title "Algorithms for the Solution of Linear and Polynomial Systems of Equations over Finite Fields, with Applications to Cryptanalysis", submitted for the degree Doctor of Philosophy of Applied Mathematics and Scientific Computation, defended in the Summer of 2007, under the guidance of Professor Lawrence C. Washington. The author is *extremely* grateful for Prof. Washington's time, help and assistance at all stages.

In addition to being a text for graduate students, the author hopes the book will be also useful for those currently working in the field as well. The pressures of page counts often require that the internals or variants of algorithms cannot be published in exhaustive detail in the standard scientific literature. Here, we have explained and expanded upon several algorithms previously published by myself and by others. Often the details left out of a published paper are those required to make an algorithm work efficiently.

[1] If these subjects are not yet ones that the reader is comfortable with, the author recommends [216] for cryptography, and [119] for undergraduate Abstract Algebra.

The backbone of the theory of polynomial systems of equations, over any field, is algebraic geometry. This topic is exquisitely covered in *Ideals, Varieties, and Algorithms* by Cox, Little and O'Shea [86], also published by Springer-Verlag. The author therefore strongly encourages the reader to read [86] along with this text, but note that [86] is not, by any means, a prerequisite for this book. The topic of Gröbner Bases, in particular, is deferred to [86], because they do an exquisite job there.

Last but not least, a handy desk-reference for finite fields is the encyclopedia [165] by Lidl and Niederreiter. The previous edition of it, [164], was referred to as "the Bible" at several finite field conferences.

Why this Book was Written

Tradition in Applied Mathematics, particularly in the USA, dictates that the research of a doctoral dissertation be divided into journal articles, and published in the years immediately following the defense. However, there is an interesting category of work that is left in limbo. Original research can, of course, be published by normal means. But work that is "dug out of the dust", published but mostly forgotten, cannot be published again. For example, the proofs of the equi-complexity of matrix operations, have been known for a long time, but not published together in one place; the "degree dropper algorithm" (See Section 11.4 on Page 192) must have been known for decades, but the author could not find a proof of it anywhere; the Method of Four Russians for Multiplication was known anecdotally, but the original paper was in Russian [21] and the most recent textbook version found was from 1974 [13, Ch. 6]; much work has been published on SAT-solvers, and how they work, but there is no consolidated elementary introduction for those ignorant of the subject, as the author found himself at the start of this work; many of the algorithms of Nicolas Courtois, including ElimLin, are never fully and explicitly defined anywhere. The author only wishes to see these techniques and algorithms used. While the author is no master of exposition (as the reader is about to discover), he hopes that the space which a book affords has allowed him to render this topic more comprehensible, particularly to a graduate student audience, or even motivated undergraduates.

The author believes SAT-solvers, in particular, are a very underestimated tool. Other communities rely upon them as a computational engine of great power. It is hoped that the chapter on how SAT-solvers work will encourage scholars not to consider them as black-boxes. Furthermore, the author hopes that the two chapters on how to adapt polynomial systems of equations to be solved by SAT-solvers will stimulate research into new and unrelated applications for these techniques, such as solving combinatorial problems outside of cryptography such as graph-coloring. Toward this end we include an appendix introducing this connection.

Advice for Graduate Students

This book is primarily intended for those who are to embark on study in the field of algebraic cryptanalysis, particularly graduate students about to begin a dissertation or a masters thesis in that topic. The author therefore will present the following piece of advice: Read as many papers as possible.

Be sure to include some that are old, as old papers often have excellent ideas. Some of these are not electronically available. Reading a very long paper, in detail, verifying all the small steps with your pencil, is slow but important. There may be some papers which you cannot give this magnitude of time to. If so, it is better to read the first 4 pages of 10 papers than to only read the abstracts of 20 or 30.

With hope for the future,

Gregory V. Bard,
Visiting Assistant Professor,
Department of Mathematics,
Fordham University,
Bronx, New York, USA.

May 4th, 2009

http://www.springer.com/978-0-387-88756-2

Algebraic Cryptanalysis
Bard, G.
2009, XXXIII, 356 p., Hardcover
ISBN: 978-0-387-88756-2