

## Possible projects for M470

### Number-Theoretic

1. Look at primitive roots: does every prime  $p$  have a primitive root and how many are there for a given prime; What if the number is now composite? How does one compute them - what algorithms are available? We have seen their utility on several occasions, what other cryptographic uses do they have?
2. Finite fields allows one to extend many of the ideas we have used for integer arithmetic to more complex structures and this has provided several instances when we have obtained more powerful algorithms as a consequence. Examples are to shift registers and to factoring. The book has a section on this and one can easily go beyond what is found here from other sources. Just beware not to reproduce the textbook.

### Statistical/Probability-based

3. For the Vigenere cipher we know that the various inner products are likely to have a definite maximum when we have obtained the correct shift and also the key length can be guessed from looking at maxima of displacement values. This is "easier" - that is more distinct maxima are obtained the more text we have available. What is the likelihood (using standard statistical ideas) that say these maxima will be above a given threshold  $t$  As a function of the value for  $m$  - the length of the message text we have available?
4. Look at *timing attacks* on various ciphers such as RSA. There is a lot written on this topic but to go beyond the purely documentary one has to take a theoretical analysis and this will require some knowledge of probability. There is a brief section in chapter 6 of the text that can get you started.

### Historical

5. The most likely one here is *Enigma*. If you attempt this beware of several pitfalls: there has to be some mathematical content and some discussion of cryptographic security from this perspective - mere description isn't of any value - there are lots already out there with that slant; from the historical perspective be aware that the record here is partly missing and much of what has been filled in has both individual and nationalistic bias (as most historical descriptions are); and finally this project will require excellent writing skills.

### Algorithmic

6. LFSR sequences has much more to offer than we had time to discuss. This will bring in issues of how to generate random numbers and one could extend the linear part to look at some nonlinear sequences. One could also look at the various cryptographic applications. Web source will also get you started.
7. Primality tests. We looked a several but there are others including the number theoretic *Lucas* test and the probabilistic *Frobenius* test. This project could take either a number theoretic or algorithmic flavour and it could also have a coding aspect - comparing the efficiency of some of these schemes.
8. Differential Cryptanalysis. The book gives a brief discussion in chapter 4. This had an effect on both DES and Rijndael. You should tie this topic to some of the ciphers such as these.

### Coding

There are lots of possibilities here, I suggest two that haven't been taken by anyone.

9. Write code to implement the quadratic sieve. Documentation of both the code and the user instructions is *essential*. Language is open, but a good interface with intermediate printouts of the results of the main steps is important. There are several such codes already available - but this would be a "from scratch" effort. I wouldn't worry about extended arithmetic - up to 20 digit numbers would suffice for this project.
10. Write code to implement the index calculus for the discrete log problem. All of the issues from the previous suggestion are germane here.