Security I – Mathematical prerequisites

Daniel R. Thomas

December 18, 2013

Abstract

The Security I course relies on some mathematical background which students may not be familiar with. This document seeks to provide exercises which ensure that the material is well understood so that students can be confident that they will understand Security I. I will provide some pointers to material which explains the concepts and a collection of exercises with solutions which should solidify understanding of the concepts.

The mathematics which you need to be comfortable with for Security I is discrete mathematics and probability. Some of this is dull – you need to learn some notation – while other parts are more interesting. The exercises will fall into three categories, bookwork questions (e.g. on definitions), usage questions where you will apply understanding to example problems and deeper understanding questions where proofs etc. will be required. All students should be able to do usage questions, first class students should find the understanding questions beneficial. No student is expected to attempt all questions. Answers will be provided (or cited) for all questions. Clearly it is to your benefit to do the questions before looking at the answers.

Aim: Students should be comfortable with working with these concepts in general and applying them in practise, both for use in cryptography and in other parts of Computer Science.

Material

The material to be covered is: notation, groups, rings, fields, GF(2^n), functions, modular arithmetic, XOR, probability, the birthday problem, permutations and random mappings.

Other people (including the course lecturer) have written texts which explain this material better than I can. The Security I slides [7] cover the material on slides 14–20, 25–26 and 66. If you want a longer exposition, Katz and Lindell's 'Introduction to Modern Cryptography' [3] is highly recommended by the lecturer and the material is covered in Appendices A and B. Denning's 'Cryptography and data security' [2] has a longer exposition and more exercises in Section 1.6. Knuth's 'The Art of Computer Programming' covers some of the material in 'Volume 1 – Fundamental Algorithms' [5] in Sections 1.2.4 and 1.2.5; and in 'Volume 2 – Seminumerical Algorithms' [6] in Sections 4.6.{0,1,2} again with exercises. Dan Boneh's Cryptography I course [1] is excellent and covers much of this material along with a large part of the rest of the Security I course (and other things covered in later courses or not at all). Frank King produced excellent notes on Probability [4] for his Lent 2007 course, the notes are available online.

Exercises

Almost all these questions use small numbers and can be solved using mental arithmetic and a piece of paper I don't think there are any intermediate results longer than 2 digits if using the correct method, except from some probability questions but a piece of paper is still sufficient.

Bookwork

n is an integer, p is prime.

Q1: If $A_i (1 \leq i \leq n)$ are finite what is $|A_1 \times A_2 \times \cdots \times A_n|$

Q2: A is finite, what is $|A^n|$ in terms of $|A|$?

Q3: What is A^*?

Q4: $|\text{Perm}(A)| =$?

Q5: How many functions are there of the form $f : A \rightarrow B$

Q6: What is a group?

Q7: What is an abelian group?

Q8: What kind of group is $(G, \bullet)$ if it has no inverse element?

Q9: What kind of group is $(\{0,1\}^n, \oplus)$?

Q10: Give two abelian and two monoid groups not previously mentioned.

Q11: What are the requirements for a ring?

Q12: What are the requirements for a field?

Q13: Give an example of a ring and of a field.

Q14: What does $n|(a-b)$ mean?

Q15: Under what condition does $a^{p-1} \equiv 1 \pmod{p}$?

Q16: $a \in \mathbb{Z}_n$, under what condition does a^{-1} exist?

Q17: What is $\mathbb{Z}_n^*$?

Q18: How do you generate $\mathbb{Z}_p^*$ with g?

Q19: What does it mean for a polynomial to be irreducible?

Q20: What is GF(p^n)?

Q21: How is GF(2^n) implemented?

Q22: Are operations on GF(2^n) efficient to compute?

Q23: What is the definition of perfect secrecy?

Q24: State Bayes theorem

Q25: What makes a cipher unconditionally secure?

Q26: What is the birthday problem?

Usage

Q27: Show that $(\mathbb{Z}, +)$ is an abelian group

Q28: Show that $(\mathbb{Z}, \cdot)$ is monoid

Q29: Why is exponentiation $a^b \pmod{n}$ faster to compute than a^b when $a^b > n$?

Q30: $53 \times 62 \mod 11 = ?$

Q31: $48 \times 73 \mod 7 = ?$

Q32: $33 \times 19 \mod 13 = ?$

Q33: $3^5 \mod 7 = ?$

Q34: $4^4 \mod 7 = ?$

Q35: $2^6 \mod 11 = ?$

Q36: $3^{-1} \mod 10 = ?$

Q37: $5^{-1} \mod 13 = ?$

Q38: $7^{-1} \mod 19 = ?$

Q39: What are all the elements in $\mathbb{Z}_{19}^*$ of multiplicative order 18 (i.e. when used as a generator they generate 18 elements)? [1, Ex 2.26]

Q40: As above but for $\mathbb{Z}_{13}^*$ of multiplicative order 12

Q41: As above but for $\mathbb{Z}_{11}^*$ of multiplicative order 10

Q42: In the Galois field GF(2^8) modulo $x^8 + x^4 + x + 1$ calculate:

1. the difference 1100 1010 minus 1001 0011;
2. the product 0100 1011 times 0000 1001.

[2013 P4 Q8 a]

Q43: Let $a = 100(x^2)$ in GF(2^3) with modulus $p(x) = 1011(x^3 + x + 1)$. Divide 1 0000 0000 0000 by 1011 to show that $a^{-1} = 100^6 \mod 1011 = 111$. [2, Ex 1.19, p56]

Q44: Let $a = 101$. If a is squared in GF(2^3) with irreducible polynomial $p(x) = x^3+x+1$ (1011 in binary), the product $d = a \times a =$? [2, p51]

Q45: Let $a = 111$ and $b = 100$. What is the product $d = a \times b$ computed in GF(2^3) with irreducible polynomial $p(x) = 1011$ ($x^3 + x + 1$)? [2, p51]

Q46: A bag contains one ball which, equiprobably, may be black or white. A white ball is added to the bag which is then shaken. One ball is retrieved at random and found to be white. What is the probability that the other ball is white? [4, Ex II.1, p2.12]

Q47: One person in 1000 is know to suffer from Nerd's Syndrome (a pathological inability to resist playing computer games). A standard test is such that 99% of those who suffer from Nerd's Syndrome show a positive result. The same test also (falsely) shows positive with 2% of *non*-suffers.

A person selected at random is tested and found positive. What is the probability that this person actually suffers from Nerd's Syndrome? [4, Ex II.3, p2.13]

Q48: Four people go to an oyster card swapping party (they want to be difficult to track). The oyster cards are thrown into a hat, shuffled, and then distributed randomly one to each participant. What is the probability that *no* participant goes home with his original card? [4, Ex II.8, p2.14]

Q49: Birthday problem: with 1024 bins how many balls are needed for the probability of collision to exceed 0.5? (You might want a calculator/computer for this one)

Understanding

Q50: Birthday problem: prove that as $n \to \infty$ the expected number of balls needed for a collision is $\sqrt{n\pi/2}$

Q51: Develop an algorithm to compute $a^b \pmod N$). [3, p515, B.3]

Q52: Show how to determine that an n-bit string is in $\mathbb{Z}_N^*$[3, p515, B.4]

Q53: Prove Bayes' Therom.

Solutions

Bookwork

n is an integer, p is prime.

A1: $|A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$

A2: $|A|^n$

A3: $\bigcup_{i=0}^{\infty} A^i$

A4: $|A|!$

A5: $|B^A| = |B|^{|A|}$?

A6: [7, p. 15]

A7: [7, p. 15]

A8: monoid

A9: abelian

A10: [7, p. 15]

A11: [7, p. 16]

A12: [7, p. 16]

A13: [7, p. 16]

A14: n divides $(a - b)$

A15: $\gcd(a, p) = 1$

A16: $\gcd(a, n) = 1$

A17: The set of all elements of $\mathbb{Z}_n$ that have an inverse.

A18: $\mathbb{Z}_p^* = \{g^i \bmod p | 0 \leq i \leq p - 2\}$

A19: [7, p. 18]

A20: [7, p. 18]

A21: [7, p. 19]

A22: Yes on hardware which supports it. [7, p. 19]

A23: [7, p. 25]

A24: [7, p. 25]

A25: [7, p. 26]

A26: [7, p. 66]

Usage

A27: Closure and associativity by definition, 0 is neutral, $-x$ is inverse.

A28: Closure and associativity by definition, 1 is neutral but there is no way of making an element smaller as all elements are 1 or greater (or perhaps 0 which only maps us to 0).

A29: You can reduce mod n as you go along. [2, p39, Figure 1.20]

A30: 8

A31: 4

A32: 3

A33: 5

A34: 4

A35: 9

A36: 7

A37: 8

A38: 11

A39: 2, 3, 10, 13, 14, 15

A40: 2, 6, 7, 11

A41: 2, 6, 7, 8

A42:

1. in GF(2^n) subtraction is the same as bitwise XOR: 0101 1001.
2. Binary multiplication without carry, then subtract (XOR) multiples (shifted versions) of $x^8 + x^4 + x + 1$ to elimiate any leading bits that make the result larger than 1111 1111: 0011 0101

[from the solution notes]

A43: Show that question.

A44: 111

A45: 1. So a and b are inverses mod 1011.

A46: $\frac{2}{3}$

A47: $\frac{11}{233}$

A48: $\frac{3}{8}$

A49: 38

Understanding

A50: [3, §A.4, p496]

A51: [3, p507, Algorithm B.13]

A52: Solutions welcome.

A53: [3, Thrm A.8, p495]

References

[1] Dan Boneh. *Cryptogrphy I.* 2013. URL: `https://www.coursera.org/course/crypto` (cit. on pp. 1, 2).

[2] Dorothy Elizabeth Robling Denning. *Cryptography and Data Security.* Addison-Wesley, 1982, pp. i–xiii,1–400. ISBN: 0-201-10150-5. URL: `http://dl.acm.org/citation.cfm?id=539308` (cit. on pp. 1–4).

[3] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography.* Chapman & Hall/CRC, 2008, pp. i–xvii, 1–534. ISBN: 1-58488-551-3 (cit. on pp. 1, 3, 4).

[4] Frank H. King. *Probability.* 01/2008. URL: `http://www.cl.cam.ac.uk/teaching/0708/Probabilty/` (cit. on pp. 1, 3).

[5] Donald E. Knuth. *The Art of Computer Programming – Volume 1 – Fundamental Algorithms.* Third Edit. Addison-Wesley, 1998, pp. i–xx, 1–650. ISBN: 0-201-89683-4 (cit. on p. 1).

[6] Donald E. Knuth. *The Art of Computer Programming – Volume 2 – Seminumerical Algorithms.* Third Edit. Addison-Wesley, 1998, pp. i–xiv, 1–762. ISBN: 0-201-89684-2 (cit. on p. 1).

[7] Markus Kuhn. *Security I slides.* 2013. URL: `http://www.cl.cam.ac.uk/teaching/1213/SecurityI/slides.pdf` (cit. on pp. 1, 3).