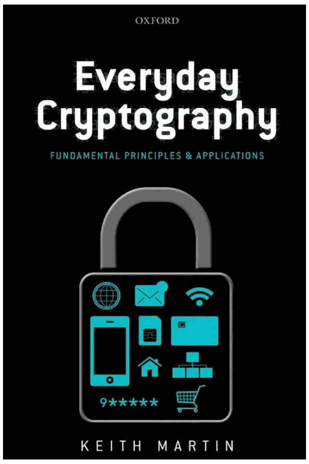
Book Reviews

Everyday Cryptography

Keith M. Martin
Oxford University Press, 2012, ISBN: 978-0-19-969559-1

To a mathematician, cryptography means public-key encryption using a one-way trapdoor function. We often teach it as an elegant application of results in number theory, such as the Euler–Fermat Theorem, the basis of the RSA cryptosystem, or the discrete logarithm problem using either a primitive root of a large prime or an element of an elliptic curve over a prime field, the basis of the ElGamal and Diffie–Hellman cryptosystems.



But to an engineer, public-key encryption is only a minor part of cryptography. He or she is concerned with the efficient encryption, transmission and decryption in real time of vast amounts of data in the form of strings of binary digits. The favoured procedure, symmetric-key encryption, is for the sender, popularly known as Alice, to encrypt the plaintext by bitwise addition of a secret pseudorandom key of the same length as the plaintext, and for the receiver, Bob, to add the same key to the ciphertext to recover the plaintext. But how can Alice and Bob both have access to a secret key? The answer is that they don't: they generate it dynamically during the process of encryption or decryption. The idea is that Alice encrypts a short seed, say 128 bits for normal security or 256 for top secret security, by public-key encryption and transmits it to Bob who recovers the seed. The first 128-bit block of plaintext is encrypted by Alice and decrypted by Bob using the seed. Then Alice uses a public algorithm such as AES (Advanced Encryption Standard) to permute each ciphertext block as it is produced and then encrypts the next plaintext block using this permutation. Bob of course does the same to decrypt the ciphertext. The point is that symmetric-key cryptography is fast and reliable, while public-key cryptography is far too slow to use on mobile phone communications, financial transactions or pay TV signals.

But there is much more to cryptography than encryption and decryption. Bob needs to know that the message he received really did come from Alice, requiring a digital signature; that it was really the message she sent, requiring a message authentication code; and that it is the message she most recently sent, requiring a timestamp. Alice, in turn, may need to know that the recipient of her message really is Bob. Cryptography is also needed for secure storage of passphrases, as well as identification codes and corresponding PINs for smart cards. This is where hash functions are part of the arsenal of the cryptographer. In fact, a major part of practical cryptography is concerned with ensuring data integrity and secure key management. It seems that most of the hacking of email storage and mobile phones that have made the news recently is the result of the failure not of cryptographic security, but of humans to observe the appropriate protocols.

I come now to the book *Everyday Cryptography*. The author, Keith M. Martin, is truly on the engineering side of cryptography. He is Professor of Information Security at Royal Holloway, University of London, and this book is an introduction to the subject aimed at beginning Communications Engineers. As such, it is light on theory and heavy on implementation. Mathematics gets short shrift; for example, modular arithmetic, the Fermat–Euler Theorem and the discrete logarithm problem are relegated to a few pages in the appendix and students are several times comforted that they don't really have to master this material. Many pages are devoted to explanations of engineering standards for symmetric-key encryption as well as message authentication codes, timestamps and digital signature protocols. There are detailed explanations of applications to information security on the Internet, wireless local area networks, mobile phone communications, pay TV broadcasts and financial transactions.

This is not a text suitable for mathematics students; but if you want to know how secure your credit card and PIN are, you will find it all here.

Phill Schultz
School of Mathematics and Statistics, The University of Western Australia.
Email: phill.schultz@uwa.edu.au

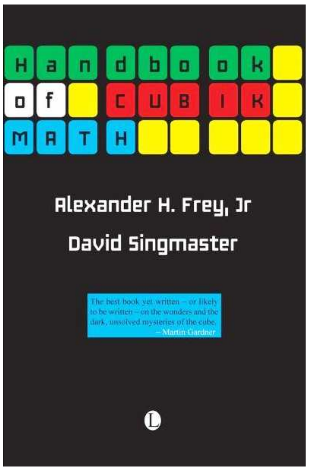
◇ ◇ ◇ ◇ ◇ ◇

Handbook of Cubik Math

Alexander H. Frey, Jr and David Singmaster
Lutterworth Press (an imprint of James Clarke & Co Ltd), 2010,
ISBN: 978-0-71-889209-8

Rubik's Cube arrived in Australia in about 1980 and started a craze remembered by many. Books presenting easy-to-follow algorithms for solving the cube (for example, Taylor [4]) soon appeared and were very popular. Some persistence was required to follow their algorithms but no mathematical knowledge was needed. However, the cube grabbed the attention of mathematicians because it provides a concrete example of groups and some group-theoretic concepts.

The cube looks like a $3 \times 3 \times 3$ stack of little cubes sitting together to make one larger cube. Initially, each face of the large cube has its own colour. The centre pieces (little cubes) on each face are attached to each other internally and can only spin in place. The other 20 visible pieces are permuted by turning the six faces. There are 12 pieces that always occupy an edge position and eight pieces that are always in a corner; each piece is unique because of the way it is coloured. There are two possible orientations for each edge piece and three for each corner piece. Thus the number of possible arrangements of these 20 pieces, taking into account orientation, is at most $12!\,8!\,2^{12}3^{8}$. The actual number of arrangements achievable by turning the faces of the cube is less than this, and some group theory explains why. Group theory also suggests good moves, making it easy to find an algorithm which can be used to obtain any possible configuration of the pieces. Frey and Singmaster's book explains all this clearly, logically and in detail. It is more than a 'how to' manual; there is a first course in group theory woven through the book.


H a n d b o o k
o f C U B I K
M A T H
Alexander H. Frey, Jr
David Singmaster
The best book yet written – or likely to be written – on the wonders and the dark, unsolved mysteries of the cube.
– Martin Gardner
L

The *Handbook of Cubik Math* is not new; it was originally published in 1982 [3]. This 2010 imprint looks much slimmer than my copy of the 1982 book, and indeed has 10 fewer pages. However, it is almost identical to the 1982 publication (including the preface and the acknowledgements).

The cube is still around and a new generation is discovering it, providing a new audience for a book on the cube and the mathematics behind it.

After a short introduction (Chapter 1), Chapter 2 describes the parts of the cube and notation. Chapter 2 includes exercises, as do most chapters. Solutions to all exercises are in the back of the book.

An algorithm for restoring the cube to its pristine state, 'a solution to the cube', is presented in Chapter 3. Though most who are interested in solving the cube should be able to solve a single face with a little effort and no help, Frey and Singmaster do this in great detail for those who want it. The book takes the reader slowly through the steps, with many helpful illustrations. Explanations of what the moves do begin to give the reader an understanding of some concepts such as the use of conjugates.

Chapter 4 begins with a challenge: to minimise the number of moves required to restore the cube to its initial state. Cycle notation is introduced. Readers are then introduced to inverses, permutations, commutators, conjugates, order and many other notions that appear in a first course on group theory. These concepts are introduced in the context of the cube.

Chapter 5 uses some of what has been learnt to improve on the algorithm presented in Chapter 3.

Chapter 6 moves on to subgroups, supergroups and to some of the variants of the standard cube that were available in 1982. One very simple variation on the standard cube is to mark the faces so that the orientation of the centre pieces is visible. This increases the number of possible patterns by a factor of 2^{11} (calculated in Chapter 7). The $4 \times 4 \times 4$ cube appeared around the time that the book was written or soon after, the $6 \times 6 \times 6$ and $7 \times 7 \times 7$ cubes are much more recent. However, the group theory principles explained by Frey and Singmaster apply to these puzzles as well, and anyone who can understand how one finds a solution to Rubik's Cube should be able to solve these larger puzzles. The main problem with the larger puzzles becomes the number of pieces; compare the 20 moving pieces of Rubik's Cube to the 212 moving pieces of the 7 × 7 × 7 cube. (To see a puzzle with many, many more pieces search the web for 'petaminx'.)

Chapter 7 begins with odd and even permutations and uses these to conclude that a single transposition of two pieces is not possible. One also learns why a single edge flip and some corner twists are not possible. This enables the number of patterns obtainable by turning faces of the cube to be calculated.

Chapter 8 takes the group theory further and uses it to show how to obtain an upper bound on the number of moves needed to solve the cube. Normal subgroups and isomorphisms are among the concepts introduced.

Chapter 9, the final chapter, presents what was known about 'God's Algorithm' when the book was first published in 1982. 'God's Algorithm' uses the fewest possible moves[1] to solve the cube. If one knows 'God's Algorithm' then one knows 'God's Number', the smallest number of moves which is sufficient to solve the cube regardless of starting position. This smallest number was only recently proved to be 20 [1]. 'God's Algorithm' has kept mathematicians and computer scientists busy over the years. Rokicki [1], [2] contains results and methods used recently.

The book includes an appendix of useful moves, mostly short sequences of twists which permute a small number of pieces. There is also an index.

Though it is 30 years since it first appeared, *Handbook of Cubik Math* is still an excellent book on the cube and its mathematics. I consider it to be the best such book ever written, one which I would recommend to anyone with an interest in the cube or related puzzles. One can go as far as a partial solution or learn enough to find good algorithms to solve the huge variety of 'cube'-like puzzles now on the market as well as covering a first course on group theory.

References

[1] Rokicki, T. (2010). God's number is 20. http://www.cube20.org/.

[2] Rokicki, T. (2010). Twenty-two moves suffice for Rubik's cube. *The Mathematical Intelligencer* **32** 33–40.

[3] Singmaster, D. and Frey, A.H. (1982). *Handbook of Cubik Math*. Enslow Publishers, Inc., Berkeley Heights, NJ.

[4] Taylor, D. (1981). *Mastering Rubik's Cube: The Solution to the 20th Century's Most Amazing Puzzle*. Greenhouse Publications, Melbourne, Australia.

Leanne Rylands
School of Computing, Engineering and Mathematics, University of Western Sydney, NSW.
Email: l.rylands@uws.edu.au

[1] Here, one move is a quarter turn or a half turn; this is the 'face-turn' or 'half-turn' metric.