Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications)

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications)

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications)

The discrete logarithm problem based on elliptic and hyperelliptic curves has gained a lot of popularity as a cryptographic primitive. The main reason is that no subexponential algorithm for computing discrete logarithms on small genus curves is currently available, except in very special cases. Therefore curve-based cryptosystems require much smaller key sizes than RSA to attain the same security level. This makes them particularly attractive for implementations on memory-restricted devices like smart cards and in high-security applications.

The **Handbook of Elliptic and Hyperelliptic Curve Cryptography** introduces the theory and algorithms involved in curve-based cryptography. After a very detailed exposition of the mathematical background, it provides ready-to-implement algorithms for the group operations and computation of pairings. It explores methods for point counting and constructing curves with the complex multiplication method and provides the algorithms in an explicit manner. It also surveys generic methods to compute discrete logarithms and details index calculus methods for hyperelliptic curves. For some special curves the discrete logarithm problem can be transferred to an easier one; the consequences are explained and suggestions for good choices are given. The authors present applications to protocols for discrete-logarithm-based systems (including bilinear structures) and explain the use of elliptic and hyperelliptic curves in factorization and primality proving. Two chapters explore their design and efficient implementations in smart cards. Practical and theoretical aspects of side-channel attacks and countermeasures and a chapter devoted to (pseudo-)random number generation round off the exposition.

The broad coverage of all- important areas makes this book a complete handbook of elliptic and hyperelliptic curve cryptography and an invaluable reference to anyone interested in this exciting field.

Download and Read Free Online Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications)

From reader reviews:

Sonja Johnson:

This Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) book is not really ordinary book, you have it then the world is in your hands. The benefit you have by reading this book is usually information inside this publication incredible fresh, you will get information which is getting deeper anyone read a lot of information you will get. This Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) without we understand teach the one who reading through it become critical in pondering and analyzing. Don't become worry Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) can bring whenever you are and not make your handbag space or bookshelves' turn into full because you can have it within your lovely laptop even cell phone. This Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) having great arrangement in word and layout, so you will not really feel uninterested in reading.

Joan Stauffer:

Information is provisions for folks to get better life, information presently can get by anyone in everywhere. The information can be a understanding or any news even a huge concern. What people must be consider while those information which is in the former life are hard to be find than now could be taking seriously which one is appropriate to believe or which one the actual resource are convinced. If you get the unstable resource then you understand it as your main information you will have huge disadvantage for you. All of those possibilities will not happen with you if you take Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) as your daily resource information.

Sheila Donovan:

This book untitled Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) to be one of several books that will best seller in this year, honestly, that is because when you read this reserve you can get a lot of benefit onto it. You will easily to buy this specific book in the book store or you can order it by way of online. The publisher in this book sells the e-book too. It makes you easier to read this book, as you can read this book in your Touch screen phone. So there is no reason for your requirements to past this guide from your list.

William Brown:

A lot of people always spent their particular free time to vacation or perhaps go to the outside with them friends and family or their friend. Did you know? Many a lot of people spent many people free time just watching TV, or perhaps playing video games all day long. If you would like try to find a new activity here is look different you can read a book. It is really fun to suit your needs. If you enjoy the book you read you can spent all day long to reading a publication. The book Handbook of Elliptic and Hyperelliptic Curve

Cryptography (Discrete Mathematics and Its Applications) it doesn't matter what good to read. There are a lot of individuals who recommended this book. We were holding enjoying reading this book. In case you did not have enough space bringing this book you can buy the e-book. You can m0ore very easily to read this book from a smart phone. The price is not to cover but this book offers high quality.

Download and Read Online Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) #16YZTXMENQI

Read Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) for online ebook

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) books to read online.

Online Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) ebook PDF download

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) Doc

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) Mobipocket

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) EPub