
Elliptic Curve Cryptography Matlab Code

Selected Areas in Cryptography

FULL SOURCE CODE: POSTGRESQL FOR DATA ANALYTICS AND VISUALIZATION WITH PYTHON GUI

Elliptic Curves in Cryptography

FULL SOURCE CODE: SQLITE FOR STUDENTS AND PROGRAMMERS WITH PYTHON GUI

Guide to Elliptic Curve Cryptography

Towards a Quarter-Century of Public Key Cryptography

Applications of Abstract Algebra with Maple and MATLAB, Second Edition

Algebraic Curves in Cryptography

MATLAB Implementation of the Steganographic Algorithm F5

Elliptic Curves

Understanding Cryptography

FULL SOURCE CODE: POSTGRESQL FOR DATA SCIENTISTS AND DATA ANALYSTS WITH PYTHON GUI

Elliptic Curve Arithmetic for Cryptography

Introduction to Cryptography with Mathematical Foundations and Computer Implementations

Patently Mathematical

FULL SOURCE CODE: THE COMPLETE GUIDE TO LEARNING POSTGRESQL AND DATA SCIENCE WITH PYTHON GUI

Public Key Cryptography

FULL SOURCE CODE: SQL SERVER FOR STUDENTS AND DATA SCIENTISTS WITH PYTHON GUI

Introduction to Cryptography with Mathematical Foundations and Computer Implementations

FULL SOURCE CODE: POSTGRESQL AND DATA SCIENCE FOR PROGRAMMERS WITH PYTHON GUI

Elliptic Curves and Their Applications to Cryptography

Advances in Elliptic Curve Cryptography

Elliptic Curve Public Key Cryptosystems

Cryptography In The Information Society

Handbook of Elliptic and Hyperelliptic Curve Cryptography

Handbook of Elliptic and Hyperelliptic Curve Cryptography

Introduction to Cryptography

FULL SOURCE CODE: PRACTICAL DATA SCIENCE WITH SQLITE AND PYTHON GUI

Elliptic Curve Cryptography for Developers
Applied Abstract Algebra with Maple™ and MATLAB
Cryptography and Cryptanalysis in MATLAB
EC Cryptography Tutorials - Herong's Tutorial Examples
Secret History
Guide to Pairing-Based Cryptography
Introduction to Cryptography
Elliptic Curves in Cryptography
Efficient Algorithms for Elliptic Curve Cryptosystems using Endomorphisms
Elliptic Curves
Implementing Elliptic Curve Cryptography
Cryptography for Developers

*Elliptic Curve
Cryptography
Matlab Code*

*Downloaded
from
<ftp.bonide.com>
by guest*

ALVARO LARSON

*Selected Areas in
Cryptography* CRC Press

This book explains the basic methods of modern cryptography. It is written for readers with only basic mathematical knowledge who are interested in modern cryptographic

algorithms and their mathematical foundation. Several exercises are included following each chapter. From the reviews: "Gives a clear and systematic

introduction into the subject whose popularity is ever increasing, and can be recommended to all who would like to learn about cryptography." --
 ZENTRALBLATT MATH
FULL SOURCE CODE:
POSTGRESQL FOR DATA ANALYTICS AND VISUALIZATION WITH PYTHON GUI Elsevier
 From the exciting history of its development in ancient times to the present day, Introduction to Cryptography with Mathematical Foundations and Computer Implementations provides

a focused tour of the central concepts of cryptography. Rather than present an encyclopedic treatment of topics in cryptography, it delineates cryptographic concepts in chronological order, developing the mathematics as needed. Written in an engaging yet rigorous style, each chapter introduces important concepts with clear definitions and theorems. Numerous examples explain key points while figures and tables help illustrate more difficult or

subtle concepts. Each chapter is punctuated with "Exercises for the Reader;" complete solutions for these are included in an appendix. Carefully crafted exercise sets are also provided at the end of each chapter, and detailed solutions to most odd-numbered exercises can be found in a designated appendix. The computer implementation section at the end of every chapter guides students through the process of writing their own programs. A supporting website

provides an extensive set of sample programs as well as downloadable platform-independent applet pages for some core programs and algorithms. As the reliance on cryptography by business, government, and industry continues and new technologies for transferring data become available, cryptography plays a permanent, important role in day-to-day operations. This self-contained sophomore-level text traces the evolution of the field, from its origins through

present-day cryptosystems, including public key cryptography and elliptic curve cryptography. ~~~~~
 ~~~~~  
 ~~~BRIEF TABLE OF CONTENTS: Preface Chapter 1: An Overview of the Subject Chapter 2: Divisibility and Modular Arithmetic Chapter 3: The Evolution of Codemaking Until the Computer Era Chapter 4: Matrices and the Hill Cryptosystem Chapter 5: The Evolution of Codebreaking Until the Computer Era Chapter 6:

Representation and Arithmetic of Integers in Different Bases Chapter 7: Block Cryptosystems and the Data Encryption Standard (DES) Chapter 8: Some Number Theory and Algorithms Chapter 9: Public Key Cryptography Chapter 10: Finite Fields in General, and GF(256) in Particular Chapter 11: The Advanced Encryption Standard Protocol (AES) Chapter 12: Elliptic Curve Cryptography Appendix A: Sets and Basic Counting Principles Appendix B:

Randomness and
Probability
Appendix C:
Solutions to all Exercises
for the Reader
Appendix
D: Answers to Selected
Exercises
References
Index
~~~~~  
~~~~~EDITORIAL  
REVIEWS:
This book is a
very comprehensible
introduction to
cryptography. It will be
very suitable for
undergraduate students.
There is adequate
material in the book for
teaching one or two
courses on cryptography.
The author has provided
many mathematically

oriented as well as
computer-based
exercises. I strongly
recommend this book as
an introductory book on
cryptography for
undergraduates.—IACR
Book Reviews, April
2011... a particularly good
entry in a crowded field.
... As someone who has
taught cryptography
courses in the past, I was
particularly impressed
with the scaled-down
versions of DES and AES
that the author describes
... . Stanoyevitch's writing
style is clear and
engaging, and the book

has many examples
illustrating the
mathematical concepts
throughout. ... One of the
many smart decisions that
the author made was to
also include many
computer
implementations and
exercises at the end of
each chapter. ... It is also
worth noting that he has
many MATLAB
implementations on his
website. ... It is clear that
Stanoyevitch designed
this book to be used by
students and that he has
taught this type of
student many times

before. The book feels carefully structured in a way that builds nicely ... it is definitely a solid choice and will be on the short list of books that I would recommend to a student wanting to learn about the field.—MAA Reviews, May 2011

Elliptic Curves in
Cryptography BALIGE
PUBLISHING

In this project, we provide you with a PostgreSQL version of an Oracle sample database named OT which is based on a global fictitious company that sells computer

hardware including storage, motherboard, RAM, video card, and CPU. The company maintains the product information such as name, description standard cost, list price, and product line. It also tracks the inventory information for all products including warehouses where products are available. Because the company operates globally, it has warehouses in various locations around the world. The company records all customer information including

name, address, and website. Each customer has at least one contact person with detailed information including name, email, and phone. The company also places a credit limit on each customer to limit the amount that customer can owe. Whenever a customer issues a purchase order, a sales order is created in the database with the pending status. When the company ships the order, the order status becomes shipped. In case the customer cancels an

order, the order status becomes canceled. In addition to the sales information, the employee data is recorded with some basic information such as name, email, phone, job title, manager, and hire date. In this project, you will write Python script to create every table and insert rows of data into each of them. You will develop GUI with PyQt5 to each table in the database. You will also create GUI to plot: case distribution of order date by year, quarter, month, week,

and day; the distribution of amount by year, quarter, month, week, day, and hour; the distribution of bottom 10 sales by product, top 10 sales by product, bottom 10 sales by customer, top 10 sales by customer, bottom 10 sales by category, top 10 sales by category, bottom 10 sales by status, top 10 sales by status, bottom 10 sales by customer city, top 10 sales by customer city, bottom 10 sales by customer state, top 10 sales by customer state, average amount by

month with mean and EWM, average amount by every month, amount feature over June 2016, amount feature over 2017, and amount payment in all years.

*FULL SOURCE CODE:
SQLITE FOR STUDENTS
AND PROGRAMMERS
WITH PYTHON GUI CRC
Press*

In this project, we will use the PostgreSQL version of SQL Server based BikeStores as a sample database to help you work with PostgreSQL quickly and effectively. The detailed structure of

database can be found at: <https://www.sqlservertutorial.net/sql-server-sample-database/>. The stores table includes the store's information. Each store has a store name, contact information such as phone and email, and an address including street, city, state, and zip code. The staffs table stores the essential information of staffs including first name, last name. It also contains the communication information such as email and phone. A staff works at a store specified by the value in the store_id

column. A store can have one or more staffs. A staff reports to a store manager specified by the value in the manager_id column. If the value in the manager_id is null, then the staff is the top manager. If a staff no longer works for any stores, the value in the active column is set to zero. The categories table stores the bike's categories such as children bicycles, comfort bicycles, and electric bikes. The products table stores the product's information such as name,

brand, category, model year, and list price. Each product belongs to a brand specified by the brand_id column. Hence, a brand may have zero or many products. Each product also belongs to a category specified by the category_id column. Also, each category may have zero or many products. The customers table stores customer's information including first name, last name, phone, email, street, city, state, zip code, and photo path. The orders table stores the sales order's header

information including customer, order status, order date, required date, shipped date. It also stores the information on where the sales transaction was created (store) and who created it (staff). Each sales order has a row in the sales_orders table. A sales order has one or many line items stored in the order_items table. The order_items table stores the line items of a sales order. Each line item belongs to a sales order specified by the order_id column. A sales order line

item includes product, order quantity, list price, and discount. The stocks table stores the inventory information i.e. the quantity of a particular product in a specific store. In this project, you will write Python script to create every table and insert rows of data into each of them. You will develop GUI with PyQt5 to each table in the database. You will also create GUI to plot: case distribution of order date by year, quarter, month, week, day, and hour; the distribution of amount by

year, quarter, month, week, day, and hour; the distribution of bottom 10 sales by product, top 10 sales by product, bottom 10 sales by customer, top 10 sales by customer, bottom 10 sales by category, top 10 sales by category, bottom 10 sales by brand, top 10 sales by brand, bottom 10 sales by customer city, top 10 sales by customer city, bottom 10 sales by customer state, top 10 sales by customer state, average amount by month with mean and EWM, average amount by

every month, amount feature over June 2017, amount feature over 2018, and all amount feature.

Guide to Elliptic Curve Cryptography

HerongYang.com

From the exciting history of its development in ancient times to the present day, *Introduction to Cryptography with Mathematical Foundations and Computer Implementations* provides a focused tour of the central concepts of cryptography. Rather than present an encyclopedic

treatment of topics in cryptography, it delineates cryptographic concepts in chronological order, developing the mathematics as needed. Written in an engaging yet rigorous style, each chapter introduces important concepts with clear definitions and theorems. Numerous examples explain key points while figures and tables help illustrate more difficult or subtle concepts. Each chapter is punctuated with "Exercises for the Reader;" complete

solutions for these are included in an appendix. Carefully crafted exercise sets are also provided at the end of each chapter, and detailed solutions to most odd-numbered exercises can be found in a designated appendix. The computer implementation section at the end of every chapter guides students through the process of writing their own programs. A supporting website provides an extensive set of sample programs as well as downloadable platform-independent

applet pages for some core programs and algorithms. As the reliance on cryptography by business, government, and industry continues and new technologies for transferring data become available, cryptography plays a permanent, important role in day-to-day operations. This self-contained sophomore-level text traces the evolution of the field, from its origins through present-day cryptosystems, including public key cryptography and elliptic curve

cryptography.
Towards a Quarter-Century of Public Key Cryptography CRC Press
 Eliminating the need for heavy number-crunching, sophisticated mathematical software packages open the door to areas like cryptography, coding theory, and combinatorics that are dependent on abstract algebra. Applications of Abstract Algebra with Maple and MATLAB®, Second Edition explores these topics and shows how to apply the software programs to

abstract algebra and its related fields. Carefully integrating Maple™ and MATLAB®, this book provides an in-depth introduction to real-world abstract algebraic problems. The first chapter offers a concise and comprehensive review of prerequisite advanced mathematics. The next several chapters examine block designs, coding theory, and cryptography while the final chapters cover counting techniques, including Pólya's and Burnside's theorems.

Other topics discussed include the Rivest, Shamir, and Adleman (RSA) cryptosystem, digital signatures, primes for security, and elliptic curve cryptosystems. New to the Second Edition Three new chapters on Vigenère ciphers, the Advanced Encryption Standard (AES), and graph theory as well as new MATLAB and Maple sections Expanded exercises and additional research exercises Maple and MATLAB files and functions available for download online and from

a CD-ROM With the incorporation of MATLAB, this second edition further illuminates the topics discussed by eliminating extensive computations of abstract algebraic techniques. The clear organization of the book as well as the inclusion of two of the most respected mathematical software packages available make the book a useful tool for students, mathematicians, and computer scientists.

**Applications of
Abstract Algebra with
Maple and MATLAB,**

Second Edition Springer Science & Business Media In this project, we provide you with the SQL SERVER version of SQLite sample database named chinook. The chinook sample database is a good database for practicing with SQL, especially PostgreSQL. The detailed description of the database can be found on: <https://www.sqlitetutorial.net/sqlite-sample-database/>. The sample database consists of 11 tables: The employee table stores employees

data such as employee id, last name, first name, etc. It also has a field named ReportsTo to specify who reports to whom; customers table stores customers data; invoices & invoice_items tables: these two tables store invoice data. The invoice table stores invoice header data and the invoice_items table stores the invoice line items data; The artist table stores artists data. It is a simple table that contains only the artist id and name; The album table stores data about a list of

tracks. Each album belongs to one artist. However, one artist may have multiple albums; The media_type table stores media types such as MPEG audio and AAC audio files; genre table stores music types such as rock, jazz, metal, etc; The track table stores the data of songs. Each track belongs to one album; playlist & playlist_track tables: The playlist table store data about playlists. Each playlist contains a list of tracks. Each track may belong to multiple playlists. The relationship

between the playlist table and track table is many-to-many. The playlist_track table is used to reflect this relationship. In this project, you will write Python script to create every table and insert rows of data into each of them. You will develop GUI with PyQt5 to each table in the database. You will also create GUI to plot: case distribution of order date by year, quarter, month, week, and day; the distribution of amount by year, quarter, month, week, day, and hour; the

bottom/top 10 sales by employee, the bottom/top 10 sales by customer, the bottom/top 10 sales by customer, the bottom/top 10 sales by artist, the bottom/top 10 sales by genre, the bottom/top 10 sales by play list, the bottom/top 10 sales by customer city, the bottom/top 10 sales by customer city, the bottom/top 10 sales by customer city, the bottom/top 10 sales by customer city, the payment amount by month with mean and EWM, the average payment amount by every month, and amount

payment in all years.

Algebraic Curves in Cryptography John Wiley & Sons

This textbook describes the main techniques and features of contemporary cryptography, but does so using secondary school mathematics so that the concepts discussed can be understood by non-mathematicians. The topics addressed include block ciphers, stream ciphers, public key encryption, digital signatures, cryptographic protocols, elliptic curve cryptography, theoretical

security, blockchain and cryptocurrencies, issues concerning random numbers, and steganography. The key results discussed in each chapter are mathematically proven, and the methods are described in sufficient detail to enable their computational implementation. Exercises are provided.

MATLAB Implementation of the Steganographic Algorithm F5 BALIGE PUBLISHING

The reach of algebraic curves in cryptography

goes far beyond elliptic curve or public key cryptography yet these other application areas have not been systematically covered in the literature. Addressing this gap, *Algebraic Curves in Cryptography* explores the rich uses of algebraic curves in a range of cryptographic applications, such as secret sh

[Elliptic Curves](#) CRC Press
 This book focuses on fast algorithms for computing scalar multiplication (or point multiplication) on certain types of elliptic

curves, as scalar multiplication is the most time-consuming operation in elliptic curve cryptography (ECC). More precisely, the text provides readers with both a theoretical perspective on the use of low Hamming weight Frobenius expansion for scalar multiplication and a practical perspective on the implementation of scalar multiplication using the above technique. ECC has a wide range of applications, including public-key encryption and digital signatures.

However, along with the use of ECC in low-end devices, the goal is to improve the efficiency of the operation. The results of this book can be used for the efficient implementation of various ECC-based applications. The book will be of interest to all readers who have at least a basic grasp of the theory of elliptic curves, or are familiar with the use of cryptography. After reading this book, readers will understand both the theory and implementation of fast

scalar multiplication algorithms.

Understanding

Cryptography Springer
Science & Business Media

This text is for a course in cryptography for advanced undergraduate and graduate students. Material is accessible to mathematically mature students having little background in number theory and computer programming. Core material is treated in the first eight chapters on areas such as classical cryptosystems, basic number theory, the RSA

algorithm, and digital signatures. The remaining nine chapters cover optional topics including secret sharing schemes, games, and information theory. Appendices contain computer examples in Mathematica, Maple, and MATLAB. The text can be taught without computers.

*FULL SOURCE CODE:
POSTGRESQL FOR DATA
SCIENTISTS AND DATA
ANALYSTS WITH PYTHON
GUI* Manning

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.
Elliptic Curve Arithmetic for Cryptography Pearson
Winner of an Outstanding Academic Title Award from CHOICE Magazine
Most available cryptology books primarily focus on either mathematics or history. Breaking this mold, Secret History: The Story of Cryptology gives a thorough yet accessible treatment of both the mathematics and history of cryptology. Requiring minimal mathematical prerequisites, the

Introduction to Cryptography with Mathematical Foundations and Computer Implementations CRC Press
Complete coverage of the current major public key cryptosystems their underlying mathematics and the most common techniques used in attacking them
Public Key Cryptography: Applications and Attacks introduces and explains the fundamentals of public key cryptography and explores its application in all major

public key cryptosystems in current use, including ElGamal, RSA, Elliptic Curve, and digital signature schemes. It provides the underlying mathematics needed to build and study these schemes as needed, and examines attacks on said schemes via the mathematical problems on which they are based – such as the discrete logarithm problem and the difficulty of factoring integers. The book contains approximately ten examples with detailed solutions, while

each chapter includes forty to fifty problems with full solutions for odd-numbered problems provided in the Appendix. Public Key Cryptography:

- Explains fundamentals of public key cryptography
- Offers numerous examples and exercises
- Provides excellent study tools for those preparing to take the Certified Information Systems Security Professional (CISSP) exam
- Provides solutions to the end-of-chapter problems

Public Key Cryptography provides a solid

background for anyone who is employed by or seeking employment with a government organization, cloud service provider, or any large enterprise that uses public key systems to secure data.

Patently Mathematical BALIGE PUBLISHING

Since their invention in the late seventies, public key cryptosystems have become an indispensable asset in establishing private and secure electronic communication, and this need, given the tremendous growth of the

Internet, is likely to continue growing. Elliptic curve cryptosystems represent the state of the art for such systems. Elliptic Curves and Their Applications to Cryptography: An Introduction provides a comprehensive and self-contained introduction to elliptic curves and how they are employed to secure public key cryptosystems. Even though the elegant mathematical theory underlying cryptosystems is considerably more involved than for other

systems, this text requires the reader to have only an elementary knowledge of basic algebra. The text nevertheless leads to problems at the forefront of current research, featuring chapters on point counting algorithms and security issues. The Adopted unifying approach treats with equal care elliptic curves over fields of even characteristic, which are especially suited for hardware implementations, and curves over fields of odd characteristic, which have

traditionally received more attention. Elliptic Curves and Their Applications: An Introduction has been used successfully for teaching advanced undergraduate courses. It will be of greatest interest to mathematicians, computer scientists, and engineers who are curious about elliptic curve cryptography in practice, without losing the beauty of the underlying mathematics.

FULL SOURCE CODE: THE COMPLETE GUIDE TO LEARNING POSTGRESQL

AND DATA SCIENCE WITH PYTHON GUI BALIGE PUBLISHING

Applied Abstract Algebra with Maple™ and MATLAB provides an in-depth introduction to real-world abstract algebraic problems. This popular textbook covers a variety of topics including block designs, coding theory, cryptography, and counting techniques, including Polya's and Burnside's theorems. The book also includes a concise review of all prereq

Public Key

Cryptography CRC Press

This EC (Elliptic Curve) cryptography tutorial book is a collection of notes and sample codes written by the author while he was learning cryptography technologies himself. Topics include rule of chord and point addition on elliptic curves; Abelian groups with additive/multiplicative notations; EC as Abelian groups; DLP (Discrete Logarithm Problem) and trapdoor function; Galois fields or finite fields with Additive/Multiplicative

Abelian Group; Prime fields, binary fields, and polynomial fields; EC fields reduced with modular arithmetic; EC subgroup and base points; EC private key and public key pairs; ECDH (Elliptic Curve Diffie-Hellman) protocol; ECDSA (Elliptic Curve Digital Signature Algorithm); ECES (Elliptic Curve Encryption Scheme) protocol; Java tool/program to generate EC keys. Updated in 2024 (Version v1.03) with minor changes. For latest updates and free sample chapters, visit

<https://www.herongyang.com/EC-Cryptography>.
FULL SOURCE CODE: SQL SERVER FOR STUDENTS AND DATA SCIENTISTS WITH PYTHON GUI
 Springer Science & Business Media
 Master the essentials of cryptography and cryptanalysis and learn how to put them to practical use. Each chapter of this book starts with an introduction to the concepts on which cryptographic algorithms are based and how they are used in practice, providing fully working

examples for each of the algorithms presented. Implementation sections will guide you through the entire process of writing your own applications and programs using MATLAB. Cryptography and Cryptanalysis in MATLAB will serve as your definitive go-to cryptography reference, whether you are a student, professional developer, or researcher, showing how a multitude of cryptographic challenges can be overcome using the powerful tools of MATLAB.

You will: Discover MATLAB's cryptography functions Work with conversion mechanisms in MATLAB Implement cryptographic algorithms using arithmetic operations Understand the classical, simple cryptosystems that form the basis of modern cryptography Develop fully working solutions (encryption/decryption operations) Study pseudo-random generators and their real-life implementations Utilize hash functions by way of practical examples

Implement solutions to defend against practical cryptanalysis methods and attacks Understand asymmetric and symmetric encryption systems and how to use them Leverage visual cryptography, steganography, and chaos-based cryptography.

Introduction to Cryptography with Mathematical Foundations and Computer Implementations
Cambridge University Press

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.

FULL SOURCE CODE:
POSTGRESQL AND DATA
SCIENCE FOR
PROGRAMMERS WITH
PYTHON GUI BALIGE
PUBLISHING

This project uses the PostgreSQL version of MySQL-based Sakila sample database which is a fictitious database designed to represent a DVD rental store. The tables of the database include film,

film_category, actor, film_actor, customer, rental, payment and inventory among others. You can download the database from <https://dev.mysql.com/doc/sakila/en/>. In this project, you will write Python script to create every table and insert rows of data into each of them. You will develop GUI with PyQt5 to each table in the database. You will also create GUI to plot case distribution of film release year, film rating, rental duration, and categorize film length; plot rating

variable against rental_duration variable in stacked bar plots; plot length variable against rental_duration variable in stacked bar plots; read payment table; plot case distribution of Year, Day, Month, Week, and Quarter of payment; plot which year, month, week, days

of week, and quarter have most payment amount; read film list by joining five tables: category, film_category, film_actor, film, and actor; plot case distribution of top 10 and bottom 10 actors; plot which film title have least and most sales; plot which actor have least and most sales; plot which film

category have least and most sales; plot case distribution of top 10 and bottom 10 overdue costumers; plot which store have most sales; plot average payment amount by month with mean and EWM; and plot payment amount over June 2005.