

Cambridge University Press  
0521653746 - Elliptic Curves in Cryptography  
I. F. Blake, G. Seroussi and N. P. Smart  
Copyright Information  
[More information](#)

---

London Mathematical Society Lecture Note Series. 265

# Elliptic Curves in Cryptography

I. F. Blake  
*Hewlett-Packard Laboratories, Palo Alto*

G. Seroussi  
*Hewlett-Packard Laboratories, Palo Alto*

N. P. Smart  
*Hewlett-Packard Laboratories, Bristol*



Cambridge University Press  
0521653746 - Elliptic Curves in Cryptography  
I. F. Blake, G. Seroussi and N. P. Smart  
Copyright Information  
[More information](#)

CAMBRIDGE UNIVERSITY PRESS  
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press  
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

[www.cambridge.org](http://www.cambridge.org)  
Information on this title: [www.cambridge.org/9780521653749](http://www.cambridge.org/9780521653749)

© I.F. Blake, G. Seroussi, N.P. Smart 1999

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 1999  
Reprinted 2000 (three times), 2001, 2002, 2004

*A catalogue record for this publication is available from the British Library*

*Library of Congress Cataloguing in Publication data*

Blake Ian F.

Elliptic Curves in Cryptography / I.F. Blake, G. Seroussi, N.P. Smart  
p. cm. – (London Mathematical Society Lecture Note Series; 265)

Includes bibliographical references and index.

ISBN 0 521 65374 6 (pbk.)

1. Computer security. 2. Cryptography. 3. Curves, Elliptic—Data processing.

I. Seroussi, G. (Gadiel), 1955 - II. Smart, Nigel P. (Nigel Paul), 1967 -.

III. Title. IV. Series.

QA76.9.A25.B27 1999

005.8'.2—dc21 99—19696 CIP

ISBN-13 978-0-521-65374-9 paperback

ISBN-10 0-521-65374-6 paperback

Transferred to digital printing 2006