Cryptography, Freedom, Democracy
How Basic Science Affects Everyone

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112−0090
USA
Email: beebe@math.utah.edu, beebe@acm.org,
beebe@computer.org (Internet)
WWW URL: **http://www.math.utah.edu/~beebe**
Telephone: +1 801 581 5254
FAX: +1 801 581 4148

To most people, research in basic science seems irrelevant, and consequently, citizens, legislators, government funding agencies, and corporations are disinclined to support it.

Nevertheless, basic science can have deep impacts on our lives. This talk examines two developments in basic science in the Twentieth Century. The first of them, Albert Einstein’s work in 1905, changed the field of physics, and the course of history. The second, the invention of public−key cryptography in 1975, has important consequences for privacy, freedom, and democracy.

Many of mankind’s discoveries have potential for both good and bad. The talk concludes with a discussion of some recent uses of technology that pose the very serious risk of our complete loss of privacy, freedom, and democracy.

Books: History, Social Effects, Technology

B. Jack Copeland
Colossus: The First Electronic Computer
ISBN 0−19−284055−X

Niels Ferguson and Bruce Schneier
Practical Cryptography (2003)
ISBN 0−471−22894−X (hardcover), 0−471−22357−3 (paperback)

Sarah Flannery and David Flannery
In Code: A [Young Women’s] Mathematical Journey
ISBN 1−56512−377−8

David Kahn
The codebreakers: the story of secret writing (1181)
ISBN 0−684−83130−9

Bruce Schneier
Secrets and Lies: Digital Security in a Networked World (2000)
ISBN 0−471−25311−1

Bruce Schneier
Beyond Fear: Thinking Sensibly About Security in an Uncertain World (2003)
ISBN 0−387−02620−7

Bruce Schneier
Applied Cryptography: Protocols, Algorithms, and Source Code in C (1994)
ISBN 0−471−59756−2

Simon Singh
**The Code Book: The Evolution of Secrecy from Mary, Queen of Scots,
to Quantum Cryptography** (1999)
ISBN 0−385−49531−5

Michael Smith
Station X: The Codebreakers of Bletchley Park (1998)
ISBN 0−7522−7148−2

Michael Smith and Ralph Erskine
**Action This Day: Bletchley Park from the breaking of
the Enigma Code to the birth of the modern computer** (2001)
ISBN 0−593−04910−1

Electronic Resources

CRYPTO−GRAM newsletter:	**http://www.schneier.com/crypto−gram.html**
Free Software Foundation:	**http://www.fsf.org/**
GNU Project:	**http://www.gnu.org/**
Center for Democracy and Technology:	**http://www.cdt.org/**
Verified Voting:	**http://verifiedvoting.org/**
ACM Computing & Public Policy:	**http://www.acm.org/serving/**
IEEE Security & Privacy:	**https://www.ieeecommunities.org/securityandprivacy**
Slides for this talk:	**http://www.math.utah.edu/~beebe/talks/2005/cryptofreedom**
Online bibliographies:	**http://www.math.utah.edu/pub/tex/bib/index−table.html**