Cryptography, Freedom, and Democracy

How Basic Science Affects Everyone

Nelson H. F. Beebe

Research Professor
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

25 September 2011

The value of basic science

Near the end of his life, one of the Twentiet
mathematicians wrote in his memoir:

> There is one comforting conclusion
> mathematician. Real mathematics ha
> one has yet discovered any warlike p
> the theory of numbers or relativity, ar
> that anyone will do so for many year

G. H. Hardy, *A Mathemat*

The value of basic science . . .

He was wrong!

Relativity and quantum mechanics

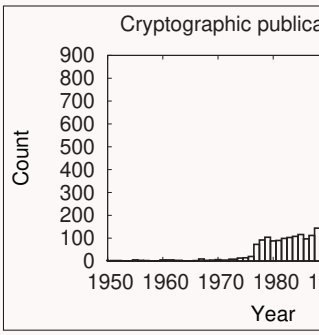
- Albert Einstein's Special Theory of Rela
  equation, $E = mc^2$, relates energy, mas
  ($c = 299\,792\,458$ m/s *(exact!)* $\approx 186\,28$
- Just two years after getting his doctora
  Denmark developed an early quantum t
- Erwin Schrödinger in Germany discover
  wave equation in 1926.
- Otto Hahn and Fritz Strassman in Gerr
  atom by neutron bombardment in 1938
  Meitner and Otto Frisch (Meitner's nep
  24, 1938.

Relativity and quantum mechanics . . .

- Nazi Germany invaded Poland on September 1, 1939, beginning World War II.
- Japan attacked Pearl Harbor, HI on December 7, 1941, bringing the until-then-neutral USA into the war.
- Manhattan Project began in 1942 at Columbia University Physics Department in New York City (December 6, 1941 by FDR!)
- Manhattan Project later involved University of Chicago, and secret new towns of Hanford, WA, Los Alamos, NM, and Oak Ridge, TN.
- First atomic bomb exploded at the Trinity Site in Alamogordo, NM at 5:29:45 am on July 16, 1945.
- Flight crews trained at Wendover, UT flew from Tinian Island in the Pacific to Japan to drop the Little Boy bomb on August 6, 1945 on Hiroshima, and the Fat Man bomb on Nagasaki on August 9, 1945.
- Japan surrendered August 14, 1945 (formally on September 2), ending World War II.
- Nuclear arms race and the Cold War began shortly thereafter.

Number theory

Whitfield Diffie and Martin Hellman at Stan
Ralph Merkle at the University of California,
unpublished until 1978), independently disco
public-key cryptography. Their work was b
problems of number theory, and unleashed a



This lecture will discuss why this work matt

Unexpected and curious connections

- In September 2005, a paper appeared in the *Journal of Cryptology* on **relativistic cryptography**, and a Web search with `http://www.google.com/` found 17 documents (39 in September 2011) with that phrase, the oldest being from 1998.
  One has the title *Remarks on Mistrustful Quantum and Relativistic Cryptography*, connecting the three basic fields in the introduction to this talk.
- Corrections from both Special Relativity (1905) and General Relativity (1916) are essential for the Global Positioning System on which modern air traffic now depends.

Preliminaries: Some dictionary defi

code A system of symbols, letter
arbitrary meanings, used fo
requiring secrecy or brevity.

cipher A message written in a sec

cryptogram A piece of writing in code

cryptography The science of analyzing ar
ciphers and cryptograms.

cryptanalysis The analysis and decipherin
systems.

encryption To put into code or cipher.

decryption To decode or decipher.

plaintext The unencrypted form of a

ciphertext A text in encrypted form, a

Preliminaries: Some dictionary definitions . . .

prime number A positive whole number not divisible without a remainder by any positive whole number other than itself and one.
For example, the primes up to 100 are:

2 3 5 7 11 13 17 19 23 29 31 37 41
43 47 53 59 61 67 71 73 79 83 89 97

steganography Hiding a secret message within a larger object in such a way that others can not discern the presence or contents of the hidden message.
For example, a message might be hidden within an image by changing the least significant bits to be the message bits.

A cartoonist's view of prime numb

Simple cryptography: substitution ciphers

Change each letter into another unique letter.

A	B	C	D	E	F	G	H	I	J	K	L	M
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Q	U	Z	M	X	L	K	T	G	P	R	H	O

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
V	Y	D	E	W	J	S	A	N	C	F	I	B

For example, to encrypt a message, use the rules in that table like this:

plaintext	**ATTACK**	**AT**	**DAWN**
substitute	↓	↓	↓
ciphertext	**QSSQZR**	**QS**	**MQCV**

To decrypt, just reverse the substitution direction:

ciphertext	**QSSQZR**	**QS**	**MQCV**
substitute	↓	↓	↓
plaintext	**ATTACK**	**AT**	**DAWN**

Simple cryptography: substitution

One of the earliest substitution ciphers is th
The substitutions are not to randomly-order
same alphabet shifted circularly by three pla

A	B	C	D	E	F	G	H
↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K

N	O	P	Q	R	S	T	U
↓	↓	↓	↓	↓	↓	↓	↓
Q	R	S	T	U	V	W	X

Encryption proceeds as before:

plaintext	**ATTACK**
substitute	↓
ciphertext	**DWWDFN**

Decryption is just the reverse: change ↓ to

Cryptographic keys

There are two important features of substitution ciphers:

- A **secret key** controls the encryption, either the substitution table (for example, QUZMXLKTGPRHOVYDEWJSANCFIB), or for the simpler Caesar cipher, just the number 3 that determines the table shift distance.
- Encryption and decryption are **symmetric**: the same key is used for both. Most cryptographic methods share this property (but *public-key cryptography* does not).

Kerchhoffs' principles of cryptograp

1. The system must be practically, if not
2. It must not be required to be secret, ar the hands of the enemy without inconv
3. Its key must be communicable and reta written notes and changeable or modifi correspondents.
4. It must be compatible with the means security mechanisms result in message into nontextual data).
5. It must be portable, and its usage and concourse of several people (consider w banking site from computer B when yo computer A).
6. Given the circumstances that command must be easy to use, requiring neither knowledge of a long series of rules to o

Cryptographic security

We have to assume that an attacker has captured our ciphertext. Encryption security then depends primarily on:

- the secrecy of the plaintext,
- the secrecy of the key,
- the complexity of the key (simple keys can be guessed by automated dictionary attacks),
- the quality and strength of the encryption method, and
- the difficulty of cracking captured ciphertext by cryptanalysis.

Cryptographic security . . .

Security can *sometimes* be improved by:

- hiding word boundaries (concealing **yes**
- padding messages to a fixed length wit
- adding random prefixes and suffixes to
- using multiple levels and/or methods o
- changing the key at suitable intervals (message).

Frequency analysis

Expected letter frequencies of natural-language text is important for cryptanalysis. Large bodies of English text suggest the order **e t a o i n s h r d l u**:

Alice in Wonderland		Hamlet		Roget's Thesaurus		Treasure Island	
19.75%	space	15.70%	space	16.00%	space	18.61%	space
9.40%	e	9.04%	e	8.41%	e	9.28%	e
7.43%	t	7.11%	t	5.81%	a	6.96%	t
6.00%	a	6.53%	o	5.63%	t	6.54%	a
5.69%	o	5.87%	a	5.49%	i	6.03%	o
5.22%	i	5.09%	i	5.34%	n	5.31%	n
4.92%	h	4.95%	s	5.27%	o	4.95%	h
4.84%	n	4.92%	h	4.87%	r	4.95%	i
4.46%	s	4.90%	n	4.36%	s	4.67%	s
3.86%	r	4.63%	r	3.84%	,	4.26%	r
3.36%	d	3.71%	l	3.41%	c	3.77%	d
3.24%	l	3.06%	d	3.33%	l	3.19%	l
2.40%	u	2.70%	u	2.65%	u	2.28%	u

Comments on cryptanalysis

- The more ciphertext that is available, t ciphers to be cracked by letter-frequenc
- Serious cryptanalysts have automated t common and historical encryption sche very quickly.
- Certain government agencies devote ve cryptanalysis. The US National Securit world's largest employer of mathematic largest computer systems, and its budg
- Successful cracks are not announced by research published.
- US and Britain monitor and analyze all network traffic.

Weaknesses of simple cryptographic methods

- With enough ciphertext, all of the standard ones are easily crackable.
- Unless the key is changed, a given plaintext letter is always converted to the same ciphertext letter, facilitating frequency-analysis attacks.
- Key reuse makes cryptanalysis easier.
- Chosen plaintext makes cryptanalysis easier (e.g., encryption of disinformation).
- Keys may be captured at either end of the communications channel, without the other end detecting the capture, compromising all future traffic.
- Keys must be shared by sender and receiver: this is the **most serious drawback** (e.g., key changes for army headquarters and troops in the battlefield, or naval command and a submarine).
- Eavesdropping is rarely detectable (photons and electrons cannot be tagged).
- Traffic analysis can still reveal important information, even if the traffic itself cannot be understood by the attacker.

Stream and block ciphers

- Simple encryption methods work on a c they are **stream ciphers**.
- In stream ciphers, a particular characte matter where it appears in the data str
- A transmission error in a single charact
- Better methods work on groups of char are **block ciphers**.
- In a block cipher, the encryption of a p all others in the same block.
- Thus, in a block method, a particular c encrypted differently, depending on its
- A transmission error in a single charact
- Block methods therefore require reliabl
- The best modern encryption methods a

Uncrackable encryption method: the one-time pad

Cryptanalysis is possible whenever there are patterns in the encryption of plaintext to ciphertext. The only way to prevent cryptanalysis is to use a **different** encryption for each plaintext letter, because that destroys all patterns.

A **one-time pad** satisfies this requirement. For example, use successive letters of text from a mutually-agreed-on book (the **key**) to determine the shift count of a Caesar-like substitution cipher:

> Call me Ishmael. Some years ago—never mind how long precisely—having little or no money in my purse, and nothing particular to interest me on shore, I thought I would sail about a little and see the watery part of the world.

Herman Melville, *Moby Dick*, London (1851)

Weaknesses of our one-time pad

- Unfortunately, when a book of natural-
one-time pad, there are still patterns pr
cryptanalysis (e.g., **and**, **I**, **little**, **me**, a
words have repeated letters (**ee**, **ll**, and
- What does one do when the book is ex
safely be reused.
- What is needed is a **completely-rando**
unlimited length for the one-time pa
- A computer method for generating ran
starting number, called the **seed**, that

Example of the one-time pad

The encryption does not reveal message length, although it **does** reveal common plaintext prefixes:

```
encrypt(123,"A")
        2b 04aa0f ef15ce59 654a0dc6 ba409618 daef6924 5729580b
        af3af319 f579b0bc

encrypt(123,"AB")
        2b47 315b 22fdc9f1 b90d4fdb 1eb8302a 4944eddb e7dd1bff
        8d0d1f10 1e46b93c

encrypt(123,"ABC")
        2b4775 2c 286a4724 40bf188f c08caffa 1007d4cc 2c2495f9
        cd999566 abfe0c2d

encrypt(123,"ABCD")
        2b477571 f970b4a2 7346ca58 742e8379 e0ce97b3 1d69dc73
        c7d921dc 018bc480
```


Example of the one-time pad . . .

The encryption does not reveal letter repetit

```
encrypt(123,"AAAAAAAAAAAAAAAAAAAAAAAAA
        2b46736e 3b83cd28 777d88c8 ad1
        e1ed75bc 5737fd71 6e68fb7d 4ac
        6d299f
```

Now encrypt a famous message from Ameri

```
ciphertext = encrypt(123, \
"One if by land, two if by sea: Paul Re
println ciphertext
        3973974d 63a8ac49 af5cb3e8 da3
        19cca7e0 7730dc80 8e9c265c 5be
        9114c057 620da15b 0670bb1d 3c9
```

Example of the one-time pad . . .

Attempt to decrypt the ciphertext with a nearby key. Decryption **does** reveal the message length, although that flaw could easily be fixed:

```
decrypt(122, ciphertext)
?^?/?)?D?fN&???w??V???Gj5?????(????1???J???i?i)y?I?-G?????b?o??X?
```

Attempt to decrypt the ciphertext with the correct key:

```
decrypt(123, ciphertext)
One if by land, two if by sea: Paul Revere's Ride, 16 April 1775
```

Attempt to decrypt the ciphertext with another nearby key:

```
decrypt(124, ciphertext)
??$???W?????N????????!?Z?U???????Q??????3?B}‘<?O ?P5%??VdNv??kS??
```

Lesson: a nearby key is as useless as a faraway key: almost-right isn't good enough.

Limitations of the one-time pad

- Although very good methods are now k
  numbers on a computer, they are alway
  that introduces patterns that can aid c
  popular methods have been cracked.
- Truly-unpredictable sources of random
  decay, cannot be replicated for the send
- The problem of secure key distribution

Public-key cryptography

- Public-key cryptography solves the key-distribution problem. Instead of a **single shared secret key**, each participant has a pair of keys: a **public key**, and a companion **private key**.
- The keys are related, such as two very large prime numbers whose product is hard to factorize. However, that is mathematically a very hard problem: given one of the keys, it is **computationally infeasible** to determine the other.
- Such problems are sometimes called **one way trap doors**.
- Easy to put needle in haystack, but much harder to remove it.

Public-key cryptography and prime

- Prime factorization of small numbers is

$$
\begin{aligned}
99 &= 3 \times 3 \times 11 \\
6860 &= 2 \times 2 \times 5 \times 7 \\
62271 &= 3 \times 3 \times 11 \times \\
62273 &= 62273 \quad \text{pri} \\
97272 &= 2 \times 2 \times 2 \times 3
\end{aligned}
$$

- Prime factorization of big numbers is h

$$
\begin{aligned}
1447473570262981491527798 &= 2 \times 109 \times 3 \\
899298750044215762751119 &= 19 \times 318023 \\
899298750044215762751119 &= 8992987500 \\
170547276604013968050272 &= 2082815984
\end{aligned}
$$

- Brute-force factorization of an N-digit
  factors up to size $N/2$ digits: work is $\mathcal{O}$

Using public key cryptography

Alice and Bob communicate securely as follows:

- Alice encrypts her plaintext with Bob's public key and sends it to him.
- Bob decrypts Alice's ciphertext with his private key to recover her plaintext.
- Bob encrypts his response with Alice's public key and sends it to her.
- Alice decrypts Bob's ciphertext with her private key to recover his plaintext.

Security and uses of public-key cry

- An attacker cannot claim to be either A private keys are not known to him.
- The technique can easily be extended t **unforgeable digital signatures** (if pr
- The mathematics of prime factorizatior and is believed to be intractable for lar
- Other public-key methods based on elli logarithms provide a failover should a n uncover a fast way to crack factorizatic
- Public-key methods are not practical fo communication. They are therefore use randomly-chosen keys for faster symme to be secure, e.g., **NIST Advanced E**
- Examples include **secure shell** on Unix connections, and some recent network

Cryptography and the citizen

- Public-key cryptography solves the key-exchange problem, and allows use of hard-to-crack random keys for symmetric methods.
- It can allow individuals to communicate with considerable confidence that no one, not even **secret government agencies** with powerful computers, can crack their communications.
- Private keys are still subject to compromise, such as by carelessness, eavesdropping, threat of violence, or force of law.
- Verification of ownership of public keys remains a problem. Why should Alice believe Bob's public key is really his, unless she knows him personally, and got the key directly from him?
- Public-key certification services by large corporations, such as Verisign, are advocated by some, but this just transfers the trust problem to another large organization over which you have no control, and little confidence in. [DigiNotar in July 2011: later bankrupt]
- Registration of public keys in a number of different key servers scattered around the world makes it harder to forge a public key.

Can cryptography ensure privacy?

Alas, no.

- Bruce Schneier wrote two editions of a **Cryptography**, and with Niels Ferguso **Practical Cryptography** and **Cryptog** the mathematics and computer science
- He wrote two more books, **Secrets &** deal with the social aspects of security
- In modern computer systems, plaintext encryption-key compromise, by capturir keyboard sniffer, screen images, or keyb data after decryption, or by cracking ci methods (simple passwords, Bluetooth, Microsoft Windows passwords and prot

Can cryptography ensure privacy? . . .

- Faulty software implementations of cryptographic methods, communications, and protocols have reduced or eliminated security in far too many cases.
- Only well-studied publicly-available encryption techniques believed to be secure by the cryptographic research community are trustworthy.
- Beware of **"security by obscurity"** and **"proprietary encryption techniques"**.
- Absence of a published successful attack against an encryption method **does not mean that it is secure**. Only published reports of repeated failed attacks and mathematical analysis can give confidence in its security.
- Storage of encrypted data is perilous: if you forget the key, or an employee leaves with the key, your data is lost, compromised, or could be held hostage.
- If an attacker learns your encryption key, your traffic or data may be monitored without your knowledge.

Dangers of technology

- Radio-frequency identification (RFID) t
  clothing, embedded under skin, . . .) en
  make them targets for theft or violent a
- Triangulation of cell-phone signals can
  carrying such a phone (500M manufact
- Biometric identifiers end up in shared d
  (e.g., fingerprinting and photographing
  newborns).
- Health-care records and genetic history
  premium increases or even denial of cov
- Airport watch lists of personal names c
  innocent people.
- High-resolution beneath-clothing scann
- Computer-based facial recognition has

Dangers of technology . . .

- Video surveillance cameras in public and corporate areas, and even some homes. And now in cell phones.
- Records of **all** telephone and email traffic to be maintained by European Union for possible prosecution.
- Records of library borrowing demanded by law enforcement.
- Web browser caches and history files.
- Highway toll-booth scanners read vehicle ID and bill the owner.
- Photocop on every corner?
- Chips in World Cup soccer balls used to determine goal entry.
- VCR and DVD players that prevent skipping commercials.
- Region coding in DVDs.
- DRAM data recovery after shutdown.
- Swedish kindergartner location tracking.

Dangers of technology . . .

- British proposal to put cameras with au
  recognition **every 400 yards on motor**
  supermarkets, petrol stations and in
- British number plates encode vehicle ye
  include county, dealer tag identifies city
  identifies neighborhood.
- Revision histories and user information
  document formats from office applicati
- Cleartext and otherwise unsecured or in
  including cell phones, Bluetooth, garag
- Unicode characters in Internet hostnam
  Names) can be deceptive.
- Color printer output encoding printer se
- Thieves use Bluetooth phones to find B
  parked cars, and then steal the laptops.

Reread George Orwell's book *1984*: **Big Bro**

Freedom and democracy

- Electronic communication over wired and wireless channels is now the norm in many countries.
- Free communication between individuals and groups enhances freedom and democracy, and makes it difficult for dictatorships to survive. [written in 2005: in 2011, Arab Spring]
- Modern cryptography allows individuals, organizations, and governments to keep private data secure against outside eavesdropping.
- Traffic analysis can still reveal critical information.
- Legislation in some countries makes use of cryptography a crime or treats cryptography (both research and software) as a weapon subject to prepublication review or export controls, or requires individuals to surrender encryption keys to law enforcement or to a government escrow agency (e.g., the US Clipper Chip proposals of the 1990s).

Freedom and democracy . . .

- Cryptography and computer systems ar
  are **poorly understood** by the genera
  legislative, and judicial branches of gov
- Because computers are new and glitzy,
  and adopt computer technology as if it
  frequently is not.
- Electronic voting systems are being wid
  yet they are **impossible to secure, tr**
- While elections with paper ballots can
  precincts, with electronic voting, the se
  elections are at risk.
- A Washington state gubernatorial elect
  election, and two US Presidential electi

Recent news on e-voting

```
Argonne researchers 'hack' Diebold e-voting system
Breaking into system using a $10 electronic component was
'ridiculously easy,' says official at national research lab

September 28, 2011 11:51 AM EST
Computerworld -

Researchers at the Argonne National Laboratory this week
showed how an electronic voting machine model that's
expected to be widely used to tally votes in the 2012
elections can be easily hacked using inexpensive,
widely-available electronic components.
```


Conclusions and lessons

- Learn the limitations of technology, and
  inappropriately.
- The social and technological impact of
  generally impossible to predict until yea
- **Reject electronic voting.**
- Guard against government attempts to
  controls and monitoring of citizens in t
  Patriot Act, and unlimited detention wi
- Oppose database aggregation, and exce
  data that violates your privacy and you

Where to learn more

- Read Bruce Schneier's books, especially **Secrets & Lies**.
- Subscribe to the monthly `crypto-gram` newsletter.
- Visit Web sites like:
  - `http://www.fsf.org/` (Free Software Foundation),
  - `http://www.gnu.org/` (GNU Project),
  - `http://www.cdt.org/` (Center for Democracy and Technology),
  - `http://verifiedvoting.org/`,
  - `http://www.acm.org/serving/` (ACM site on Computing & Public Policy, with link to Risks Forum),
  - `https://www.ieeecommunities.org/securityandprivacy` (IEEE Security & Privacy forum and journal),
  - `http://www.math.utah.edu/~beebe/` (notes on PGP, and slides and handouts for talks), and
  - `http://www.math.utah.edu/pub/tex/bib` (bibliographies on cryptography, including journals: **Cryptologia** covers history of field).