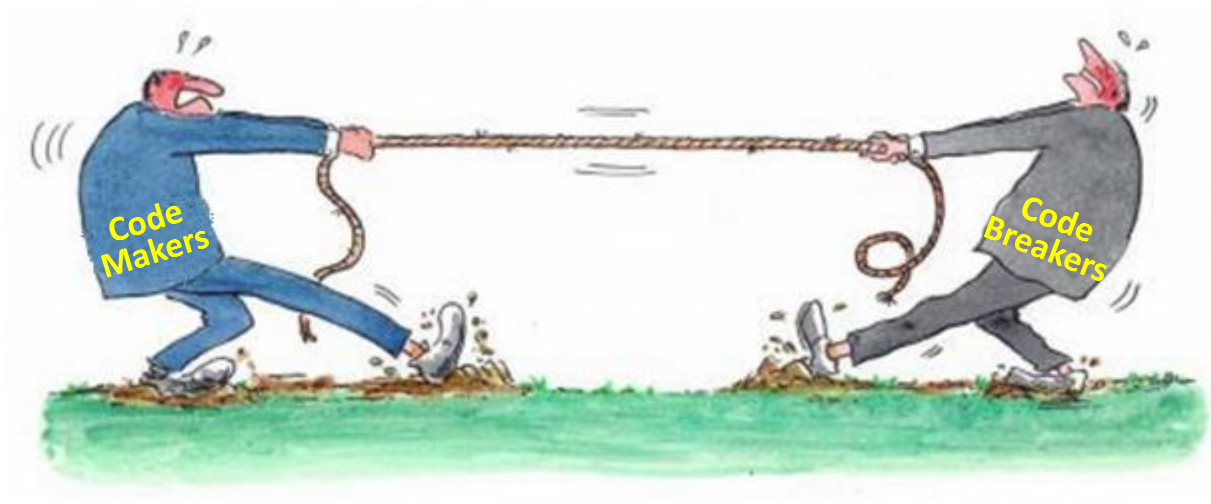
Cryptography for the Rest of Us

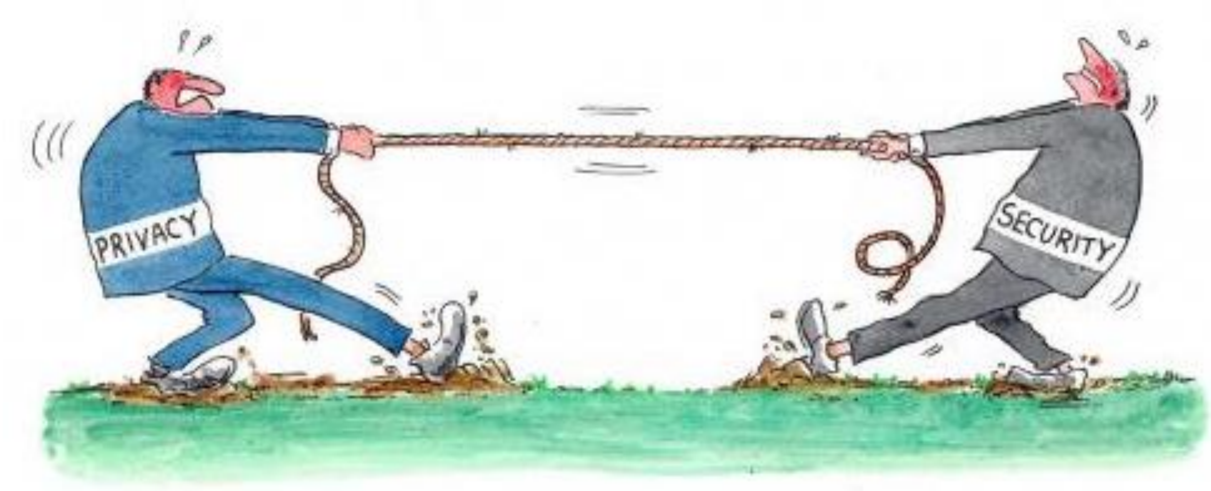
Lorrin R. Garson

OPCUG & PATACS

June 21, 2014

Constant Strife & Competition



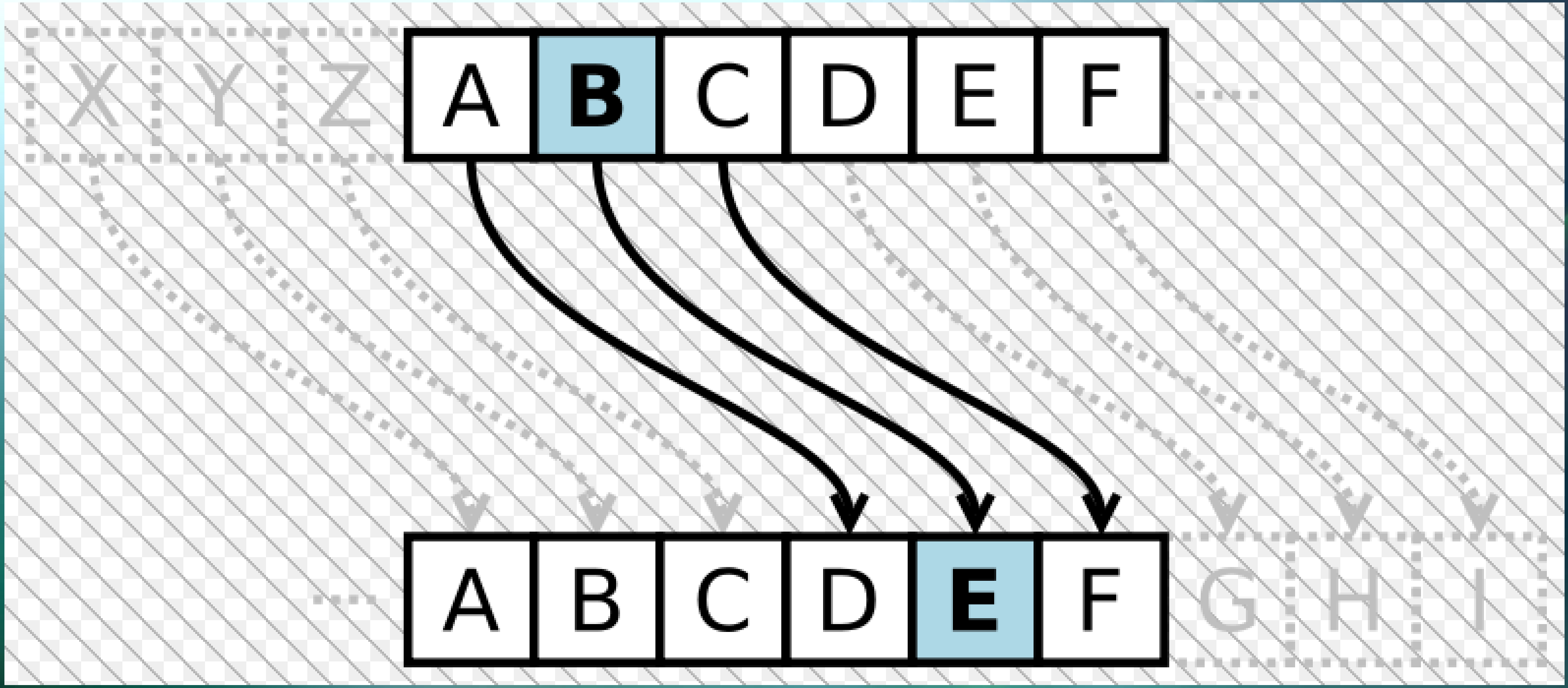


A Little History

- ~3000 BC—Egypt: transformed hieroglyphs
- 1500 BC—Mesopotamia: craftsman encrypted recipe for pottery glaze
- 600-500 BC—Hebrew scholars used a simple monoalphabetic substitution

Julius Caesar
or Mxolxv Fdhvdu

- ~50 BC—Caesar cipher aka shift cipher, or substitution cipher **Offset of 3**



Abū Bakr Aḥmad ben ‘Ali ben Waḥshiyya an-Nabati

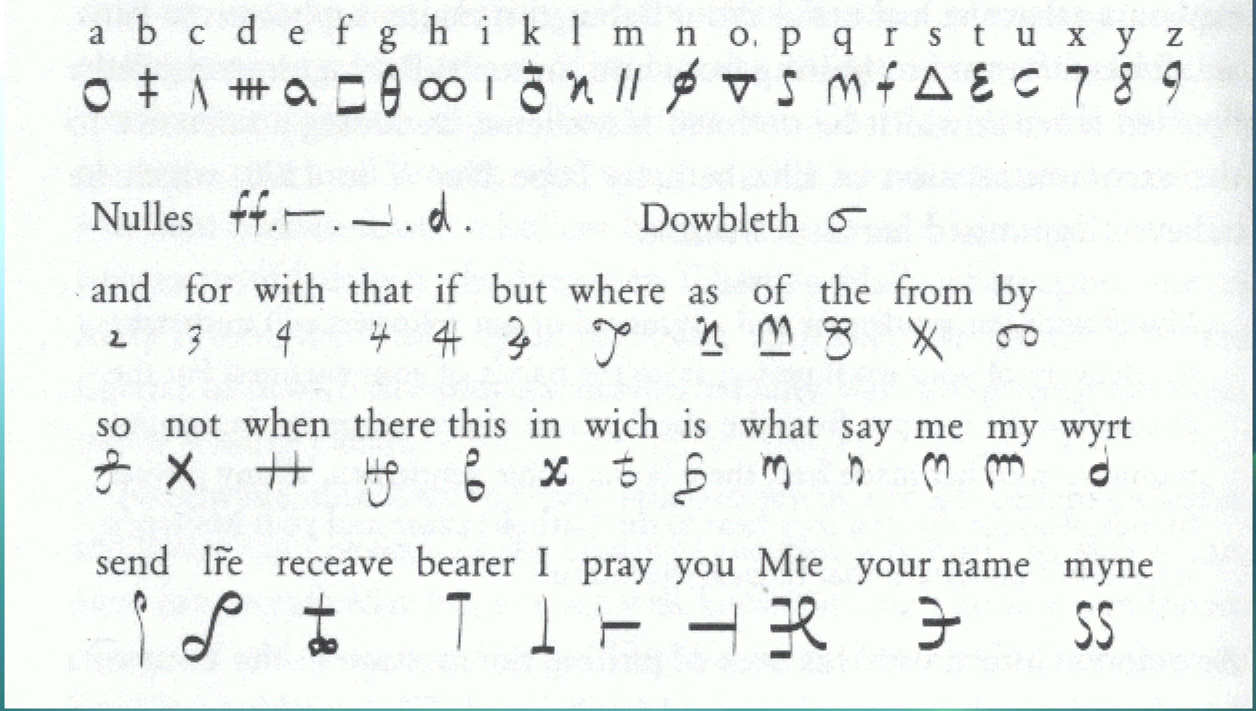
- 855—”Book of the Frenzied Devotee’s Desire to Learn About the Riddles of Ancient Scripts”
- Arabs first to employ systematic cryptanalysis

Mary, Queen of Scots vs. Elizabeth I

- 1586: Mary sent enciphered messages to Anthony Babington, a conspirator
- Communications intercepted by Sir Francis Walsingham (Secretary of State to Elizabeth) and colleagues
- Thomas Phelippes easily deciphered Mary’s messages

Mary’s Nomenclator

- A mixture of codes and ciphers



a b c d e f g h i k l m n o. p q r s t u x y z

Nulles ff. — . — . d .

Dowbleth

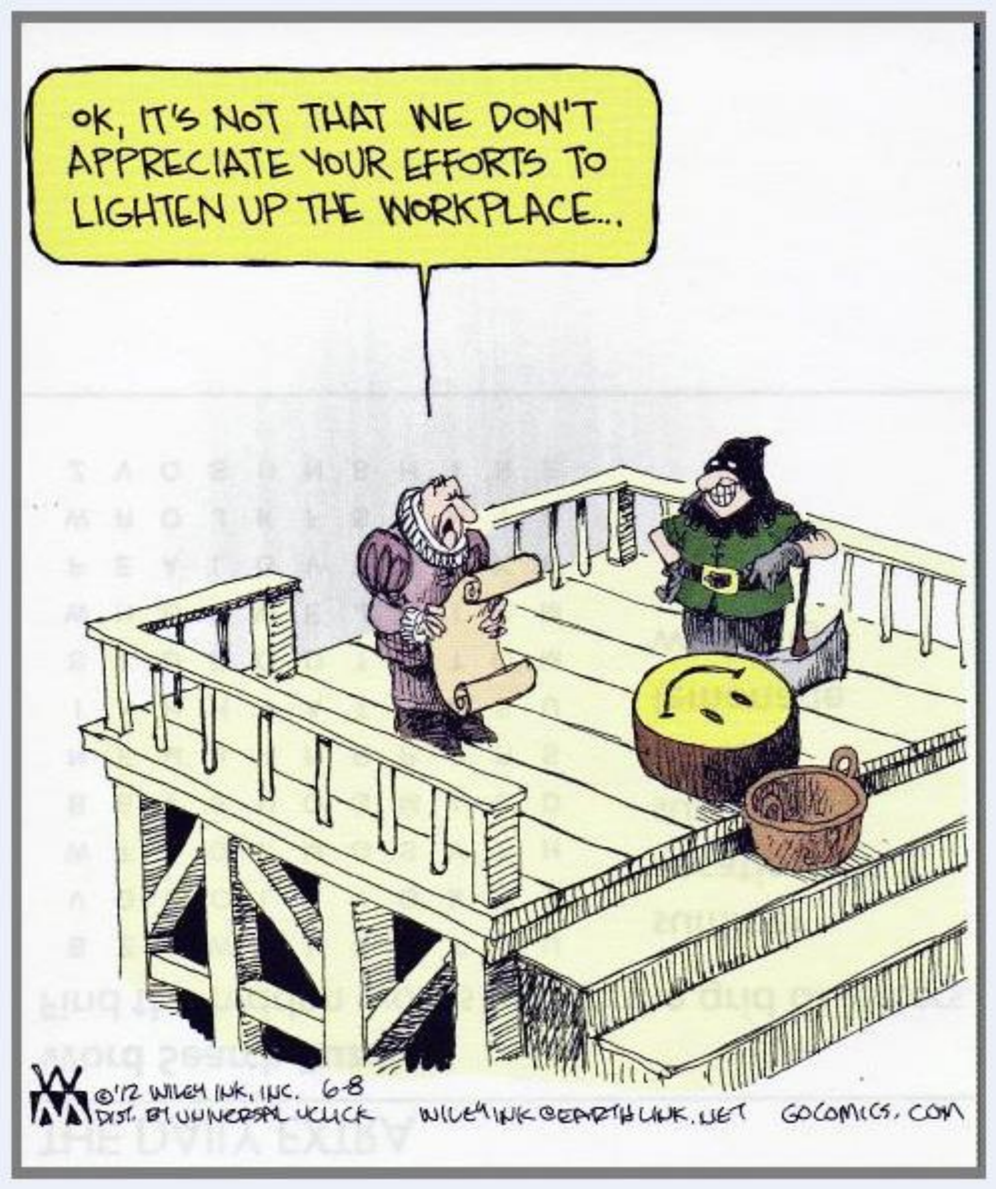
and for with that if but where as of the from by

so not when there this in wich is what say me my wyrt

send lr̃e receave bearer I pray you Mte your name myne

- And the consequence…

Mary, Queen of Scots—February 8, 1587


OK, IT'S NOT THAT WE DON'T APPRECIATE YOUR EFFORTS TO LIGHTEN UP THE WORKPLACE...
©'12 WILEY INK, INC. 6-8
DIST. BY UNIVERSAL UCLICK
WILEYINK@EARTHLINK.NET
GOCOMICS.COM

Blaise de Vigenère

- 1586: Encryption using a series of Caesar ciphers based on a keyword
- Polyalphabetic substitution
- Defies letter frequency analysis
- Resisted systematic decryption for 300 years
- See ⓘ ⓘ ← **Click for more information**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère Table

Keyword is “RELATIONS”

Message is “ATTACK AT DAWN’

Keyword: RELAT IONSR ELATI

Plaintext: ATTAC KATDA WN

Cyphertext: RXEAV SOGVR AY

↑↑↑

To decrypt the cyphertext, position the keyword above the cyphertext as shown:

Keyword: RELAT IONSR ELATI

Cyphertext: RXEAV SOGVR AY

Plaintext: ATTAC KATDA WN

1. Locate the keyword letter in the top row
2. Go down that column to the cypher letter
3. Read the plaintext letter in the far left column

Thomas Jefferson

- ~1795 developed “wheel cipher”*
- Used while Secretary of State
- Consists of 20-36 disks each with 26 letters on each disk. Each disk is numbered.
- Order of the disks represents the “key”
- Plaintext is spelled out by rotating disks
- Sender transmits one of other 25 strings
- Recipient sets up wheels identically and dials the cyphertext to read the plaintext

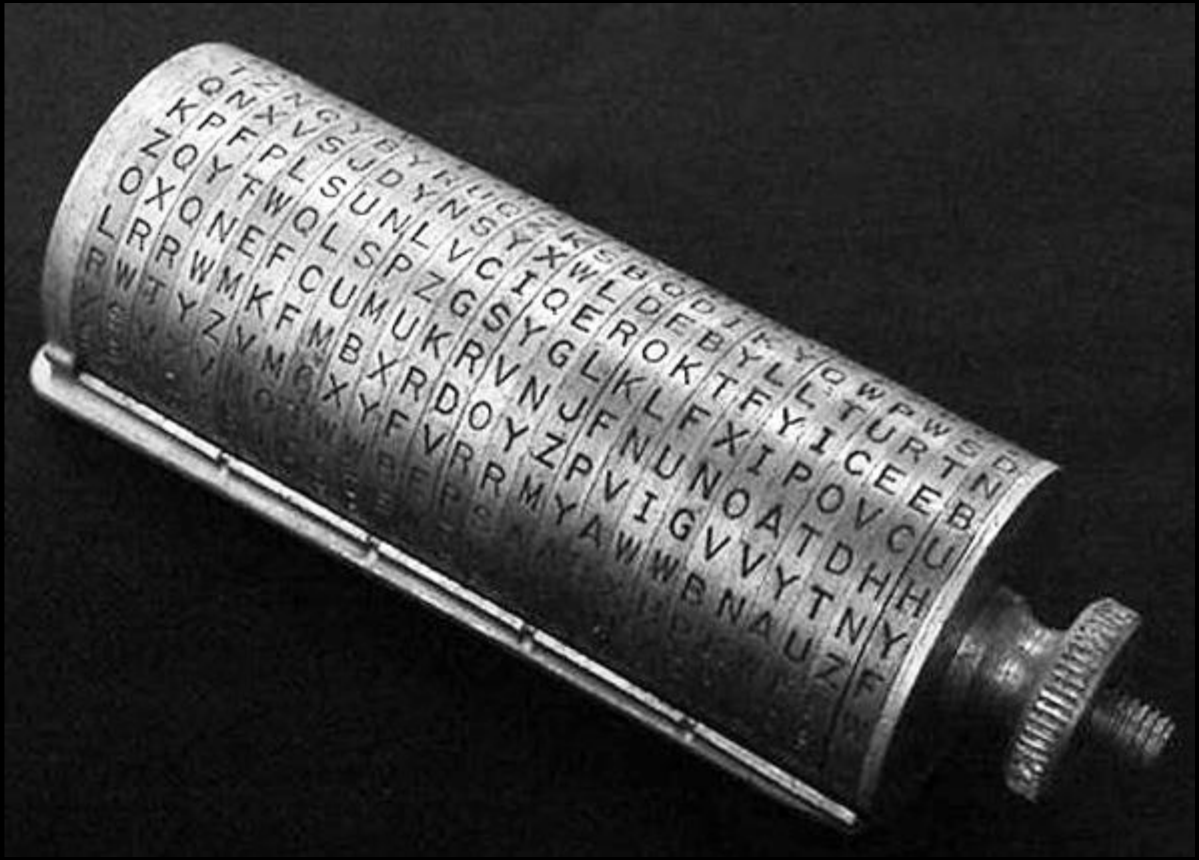
*AKA Bazeries Cylinder. Re-invented by Étienne Bazeries in 1891.

Jefferson’s Wheel Cipher

36 wheels giving 36! Possibilities. 36! = 3.7199 x 10^{41} or about 2^{128}

Jefferson Wheel Model M-94

Used by U.S. Military 1922-1943



American Civil War
(The Confederacy)

- Transmission by paper, semafore and telegraph
- Simple letter substitution
- Vigenère table (aka Vicksburg Square) used with only three code words:
  - manchester bluff
  - complete victory
  - come retribution
- Common dictionaries with words numbered

CONFEDERATE STAT
TWENTY DOLLAR
Will pay
on demand
Richmond
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
CSA
SS

American Civil War

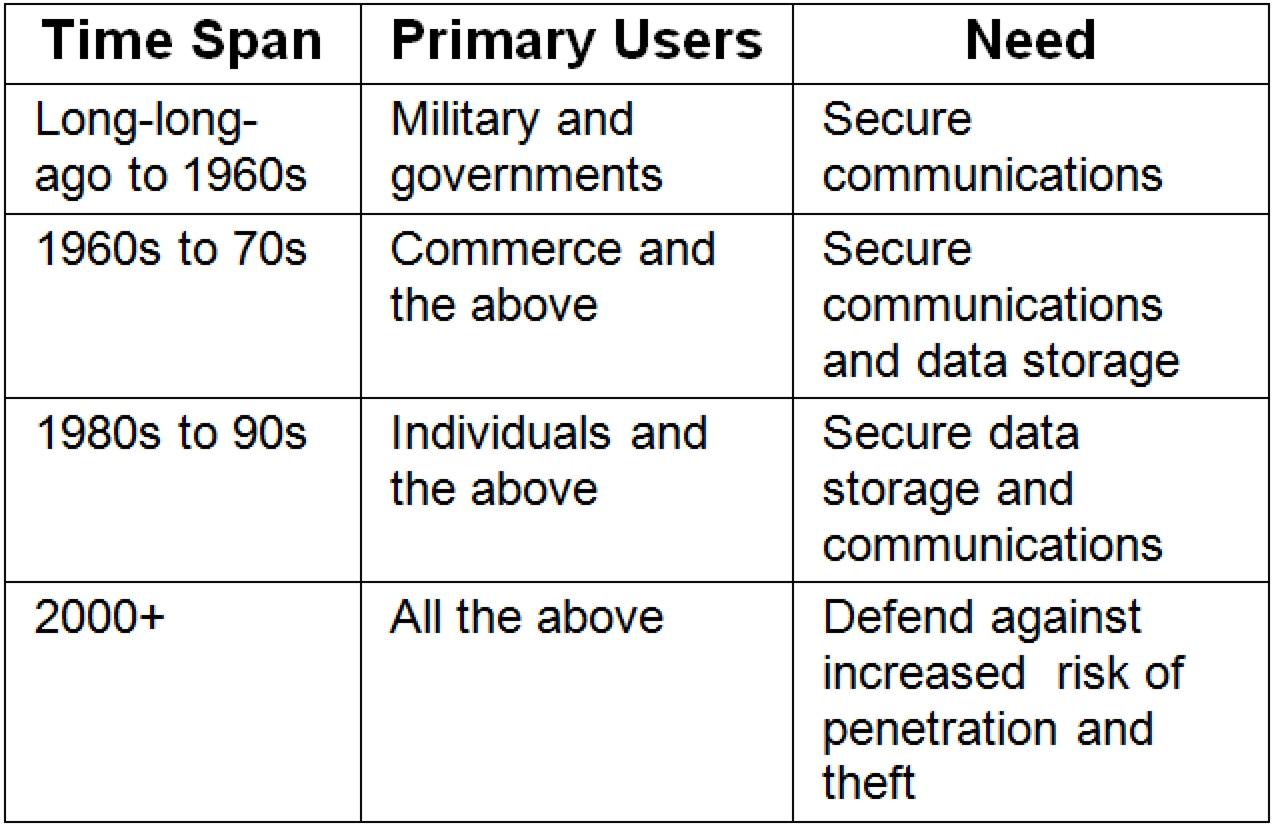
(The Union)

- Transmission principally by telegraph
- Stager Transposition code (aka route cipher)
- For an example see ℹ

20th Century

- Many advances in cryptography
- Even greater advances of cryptanalysis
  - World War 1: British successful in breaking German codes
  - World War 2: British even greater success in breaking German codes
  - World War 2: Americans very successful in breaking Japanese codes

Society’s Need and Use of Cryptology



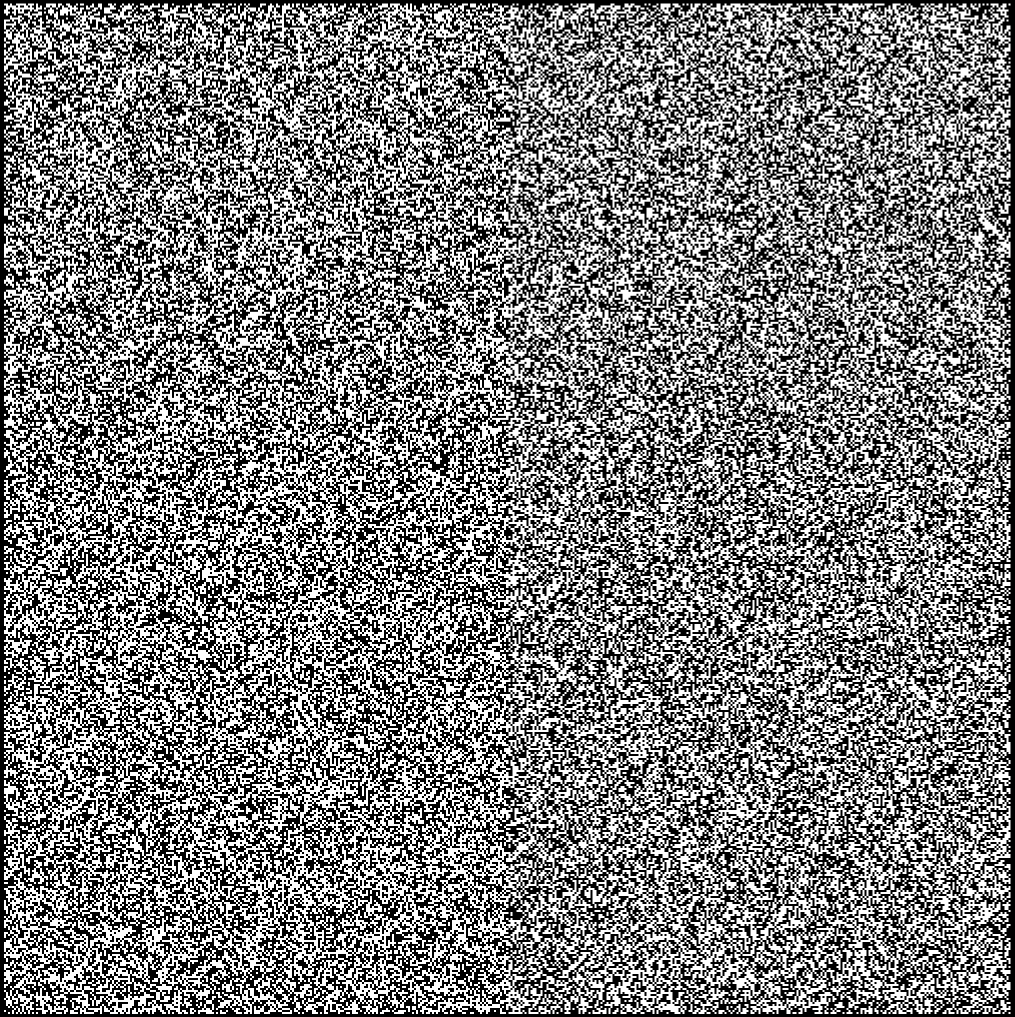
Time Span	Primary Users	Need
Long-long-ago to 1960s	Military and governments	Secure communications
1960s to 70s	Commerce and the above	Secure communications and data storage
1980s to 90s	Individuals and the above	Secure data storage and communications
2000+	All the above	Defend against increased risk of penetration and theft

Modern Cryptology

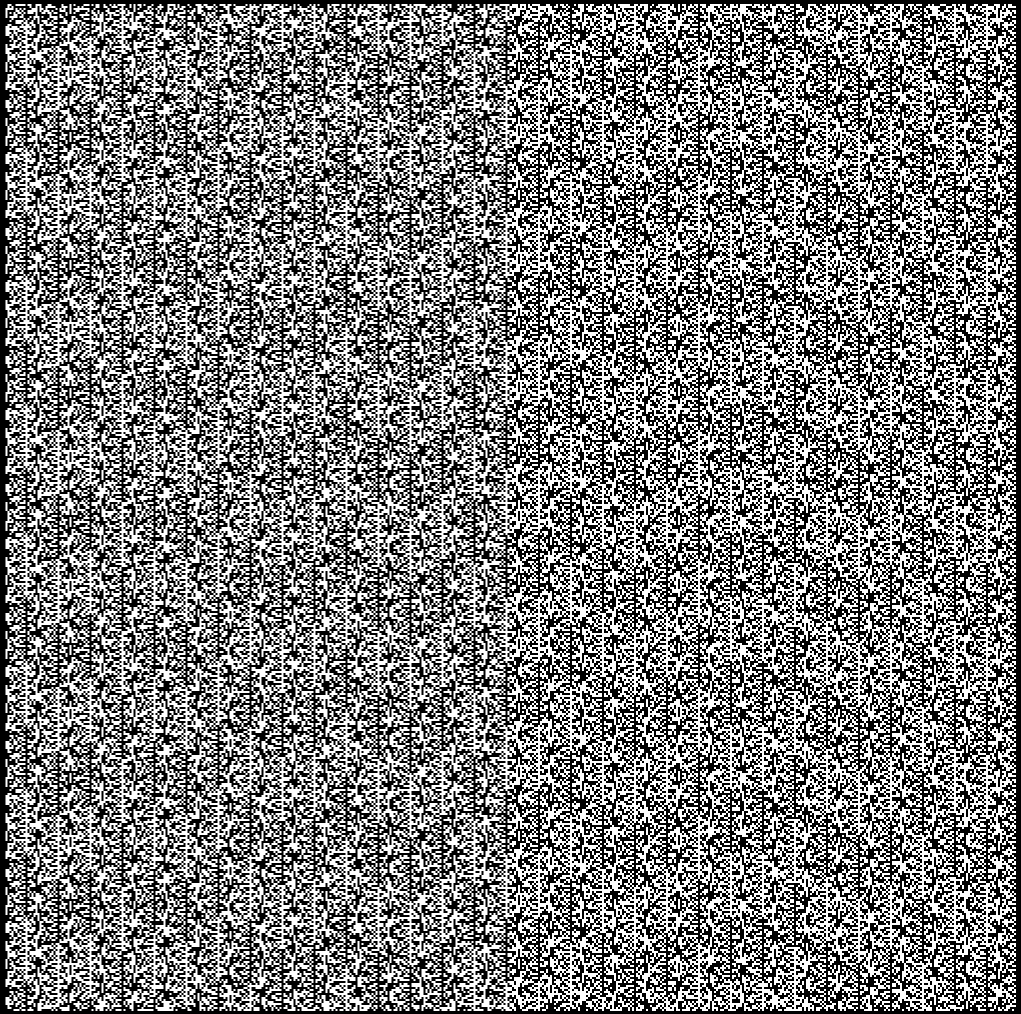
- Reliance on computers—algorithms to encrypt and decrypt
- Transmission: Internet, satellite, radio & landlines
- Considerations for keys:
  - Randomness
  - Key size
  - Security of keys
  - Skilled use of crypto systems
- Symmetric encryption (aka secret key)
- Asymmetric encryption (aka double key or public)

The Achilles Heel of Cryptology

- John Anthony Walker
- USN Chief Warrant Officer
- Spied for Soviet Union for 1968-1985, provided cryptological keys
- Enabling Soviets to decrypt ~1 million USN messages
- Soviets knew precise location of all USN submarines
- Sentenced to life in prison without parole



Created by a true random number generator (TRNG)
From: random.org ⓘ (atmospheric noise)



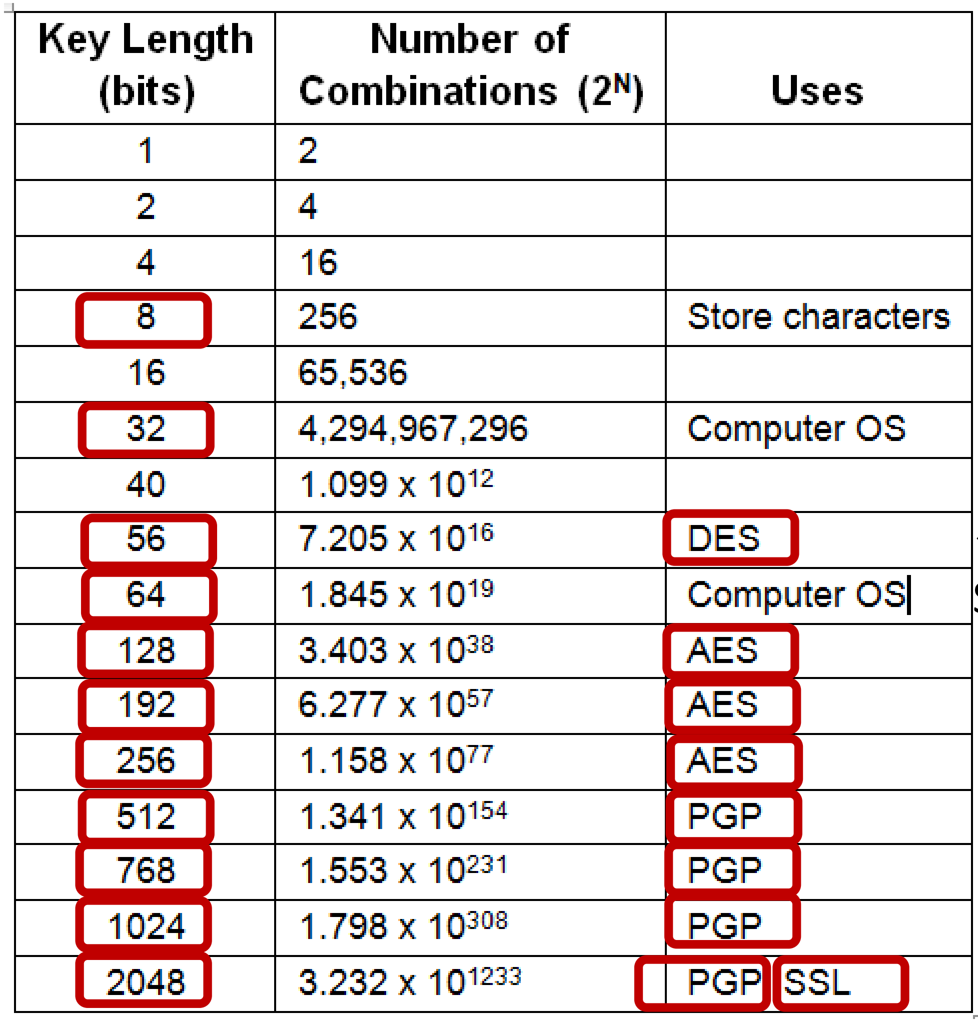
Created by a pseudo-random number generator (PRNG)
Microsoft Windows using rand( )

Importance of Key Size

- Keys are used to encrypt/decrypt information
- Strength of a key is a function of length, complexity and unpredictability
- Many (most) keys are 128-256 bits
  - 128 bits (16 letters) = disentablishment
  - 256 bits (32 letters) = Auslandsreisekrankenversicherung*

***[Foreign] Travel Health Insurance**

Key Length and Number of Combinations



Key Length (bits)	Number of Combinations (2^N)	Uses
1	2	
2	4	
4	16	
8	256	Store characters
16	65,536	
32	4,294,967,296	Computer OS
40	1.099×10^{12}	
56	7.205×10^{16}	DES
64	1.845×10^{19}	Computer OS
128	3.403×10^{38}	AES
192	6.277×10^{57}	AES
256	1.158×10^{77}	AES
512	1.341×10^{154}	PGP
768	1.553×10^{231}	PGP
1024	1.798×10^{308}	PGP
2048	3.232×10^{1233}	PGP SSL

Sweet spot →

← Data Encryption Standard (1977)

← Advanced Encryption Standard (2001)

← Pretty Good Privacy (1991+)

Secure Socket Layer ↑

Number of atoms in the observable universe = 10^{78} to 10^{82} = 2^{260} to 2^{273}

Key Size Isn’t Everything

- Heartbleed Bug: April 2014
- Vulnerability in OpenSSL cryptographic software
- Allowed access to user names and passwords, secret keys, etc.
- ~17% of of secure Web servers vulnerable
- Change user names and passwords
- See ℹ ℹ ℹ for more information

Data Encryption Standard (DES)

- 1970s: Developed by IBM
- 1977: Accepted by NBS & NSA for sensitive government information and commerce
- 56-bit key
- Suspicions of a backdoor
- 1999: Broke by Electronic Frontier Foundation in 22 hours 15 minutes

Advanced Encryption Standard (AES)

- 2001: Specification established by NIST*
- 128, 192 and 256-bit key length
- Symmetric key (same key to encrypt/decrypt)
- Approved by NSA for sensitive information
- Used worldwide in commerce and browsers
- Competitors to AES
  - Serpent
  - Twofish, Threefish and Blowfish
  - Salsa 20

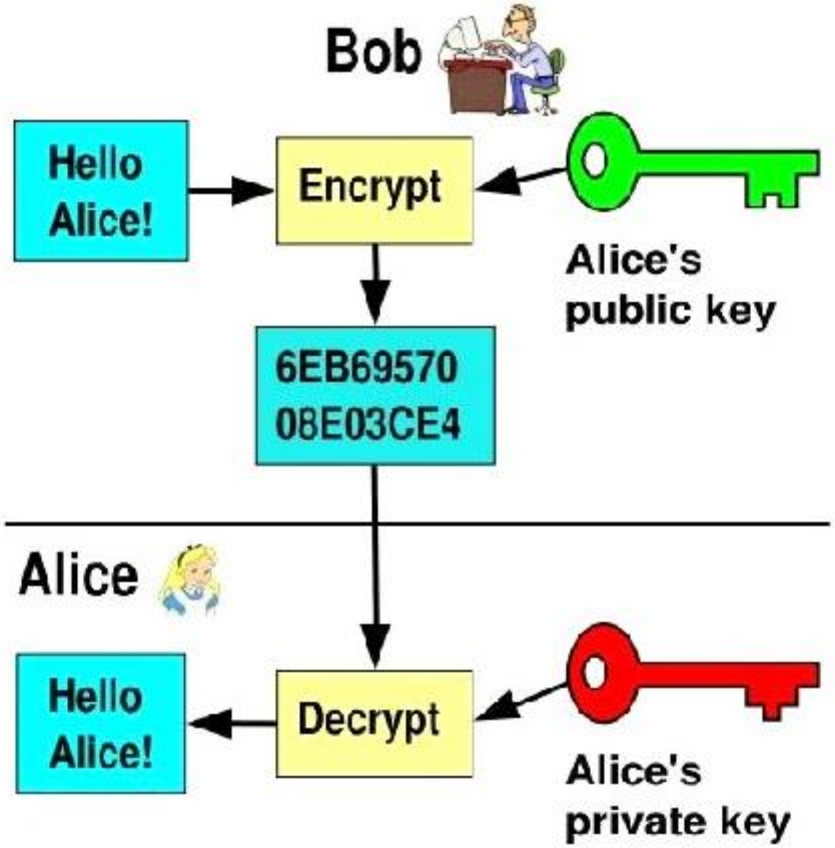
***National Institute of Standards & Technology. Formerly NBS, National Bureau of Standards**

Public Key Encryption
(PKE)

- 1976: Diffie and Hellman publish seminal paper on “double key” (asymmetric) cryptography*
- 1978: Merkle and Hellman develop first PKE system “the knapsack”
- 1978: **R**ivest, **S**hamir and **A**dleman develop the RSA system
  - Uses two large prime numbers to generate keys
  - RSA technology owned by EMC

*W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory, 22 (1976), pp. 644-654

Bob Communicates With Alice
(securely)



U.S. Export of Cryptology

- In the 1960’s cryptographic information was regarded as a “munition” and a Federal license was required for its export (key size >40 bits)
- 1970s: increasing need for encryption for commercial purposes
- 1991: Phil Zimmermann published PGP on the Internet: 3-year federal investigation follows
- 2009: Federal export restrictions still apply (“rogue states” and terrorist organizations)

Pretty Good Privacy ⓘ

(PGP)

- Complex hybrid cryptosystem see ⓘ
- Uses
  - Encrypt/decrypt files, directories, disk partition
  - Secure e-mail
  - Digital signatures

Pretty Good Privacy (cont.)
(PGP)

- Colorful complex history, see ⓘ
- Complex to implement
- 2010: Acquired by Symantec (Norton)
- 2013: Video Phil Zimmermann speaking* ⓘ

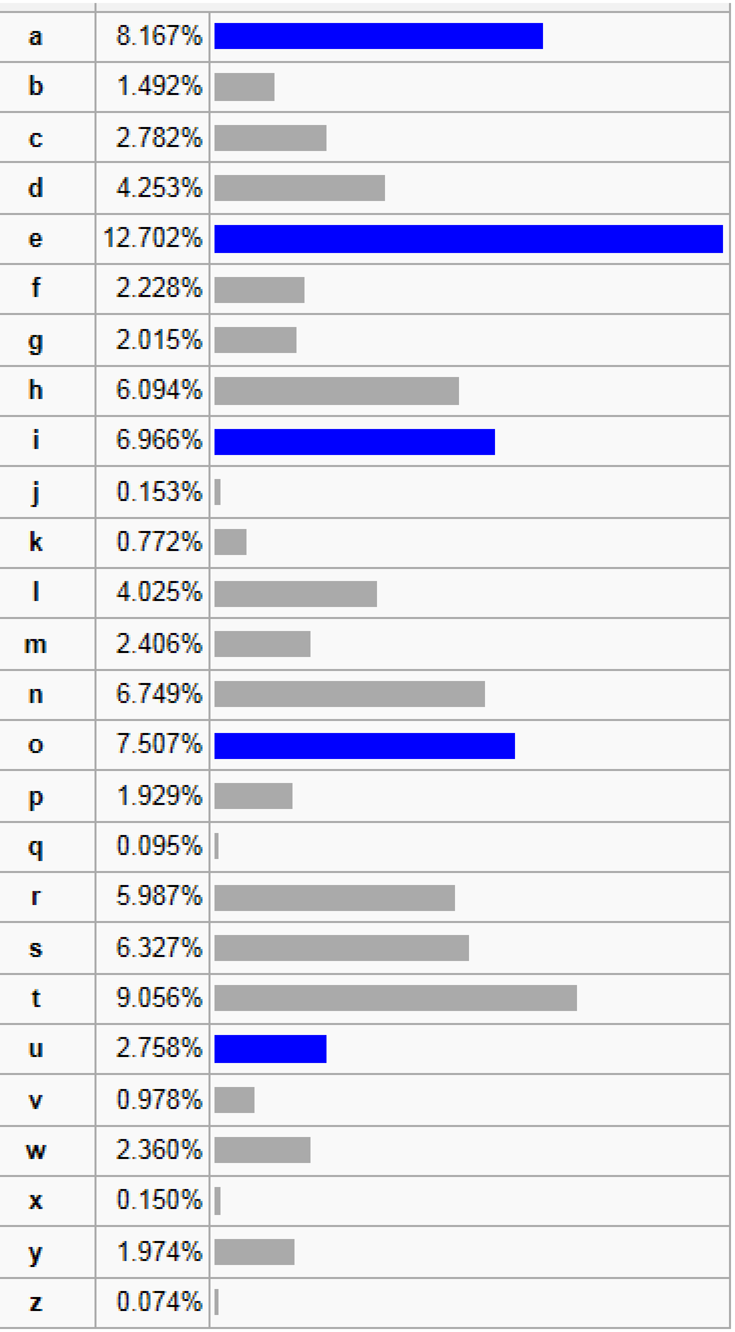
***Skip the first 9 minutes of this 57-minute video**

International Use of Cryptology

- Use, import and export of cryptology is very complex ⓘ ⓘ
- No controls: South & Central America, Bangladesh, Iceland, Syria, Ghana, Kenya, Kazakhstan
- Not allowed or tightly controlled: Bahrain, Belarus, Myanmar, China, Egypt, India, Iran, Iraq, Israel, Morocco, North Korea, Pakistan, Russia, Thailand, Tunisia, Vietnam, Saudi Arabia

Cryptanalysis

- Until ~1939, code breaking was a manual operation
- Today breaking of encrypted information is done using computers
- A simple example of a manual method easily adopted for computers…



a	8.167%	
b	1.492%	
c	2.782%	
d	4.253%	
e	12.702%	
f	2.228%	
g	2.015%	
h	6.094%	
i	6.966%	
j	0.153%	
k	0.772%	
l	4.025%	
m	2.406%	
n	6.749%	
o	7.507%	
p	1.929%	
q	0.095%	
r	5.987%	
s	6.327%	
t	9.056%	
u	2.758%	
v	0.978%	
w	2.360%	
x	0.150%	
y	1.974%	
z	0.074%	

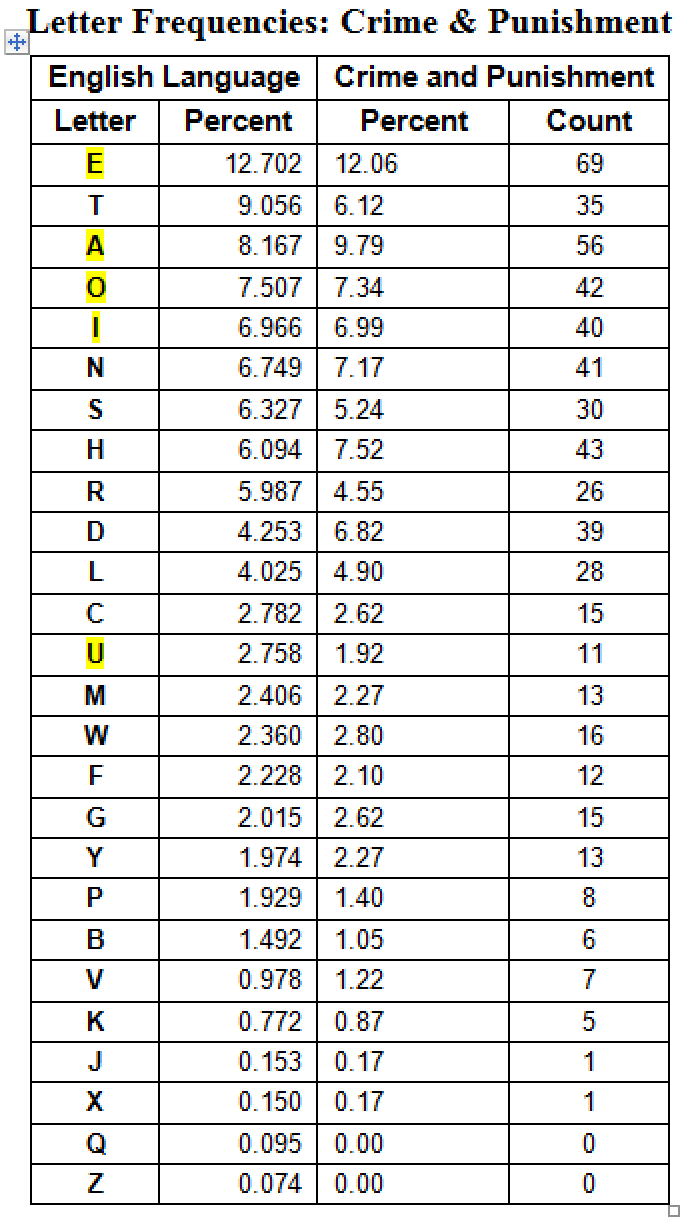
Frequency of letters in the English language

Crime and Punishment by Fyodor Dostoevsky
(132 words, 572 letters)

On an exceptionally hot evening early in July a young man came out of the garret in which he lodged in S. Place and walked slowly, as though in hesitation, towards K. bridge. He had successfully avoided meeting his landlady on the staircase. His garret was under the roof of a high, five-storied house and was more like a cupboard than a room. The landlady who provided him with garret, dinners, and attendance, lived on the floor below, and every time he went out he was obliged to pass her kitchen, the door of which invariably stood open. And each time he passed, the young man had a sick, frightened feeling, which made him scowl and feel ashamed. He was hopelessly in debt to his landlady, and was afraid of meeting her.

Encryption done by letter substitution
T = A, W = E, P = B, etc.

Analysis of *Crime and Punishment*



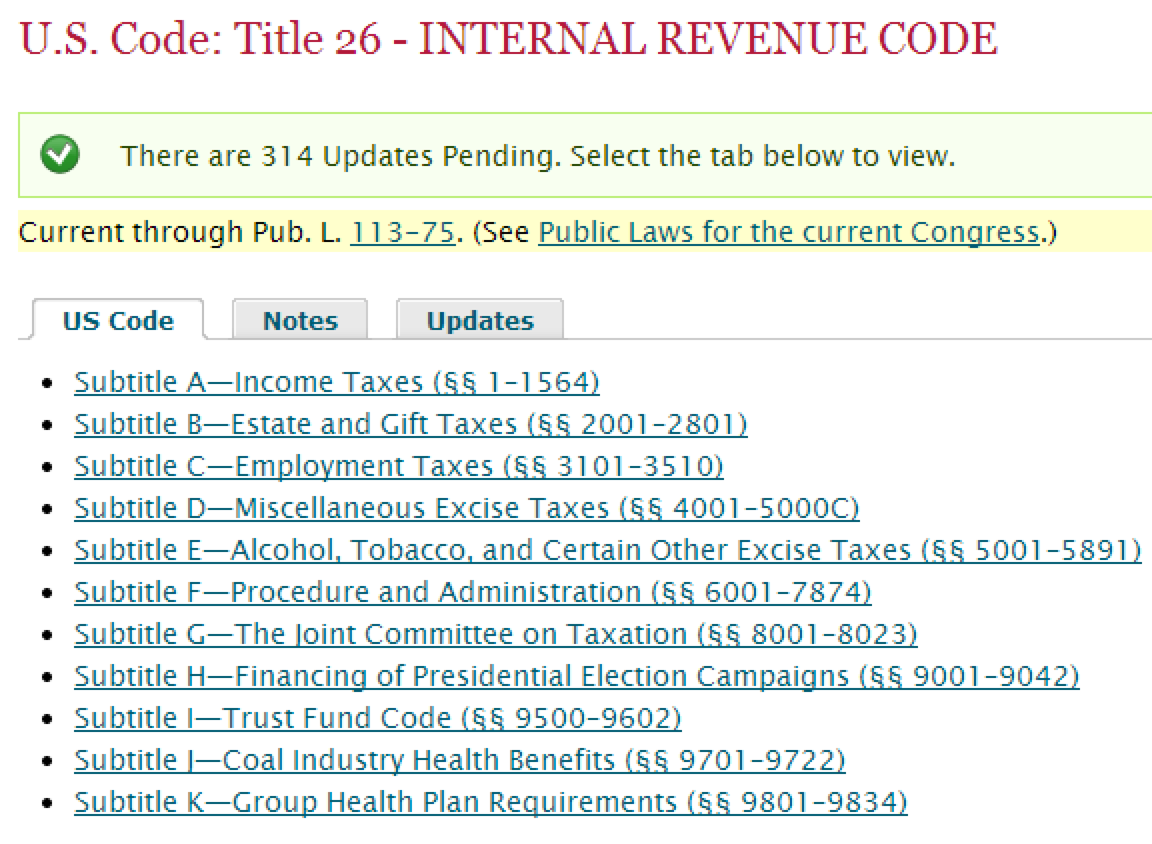
Letter Frequencies: Crime & Punishment

English Language		Crime and Punishment	
Letter	Percent	Percent	Count
E	12.702	12.06	69
T	9.056	6.12	35
A	8.167	9.79	56
O	7.507	7.34	42
I	6.966	6.99	40
N	6.749	7.17	41
S	6.327	5.24	30
H	6.094	7.52	43
R	5.987	4.55	26
D	4.253	6.82	39
L	4.025	4.90	28
C	2.782	2.62	15
U	2.758	1.92	11
M	2.406	2.27	13
W	2.360	2.80	16
F	2.228	2.10	12
G	2.015	2.62	15
Y	1.974	2.27	13
P	1.929	1.40	8
B	1.492	1.05	6
V	0.978	1.22	7
K	0.772	0.87	5
J	0.153	0.17	1
X	0.150	0.17	1
Q	0.095	0.00	0
Z	0.074	0.00	0

- Frequency of letters (132 words, 572 letters)
- Vowels quickly identified
- Frequency of letter pairs [SS-4, EE-4, TT-1, FF-0, AN-15, TH-10, ER-5, ON-5]
- Frequency of first letter in words

An Unbreakable Code?

- The U.S. Tax Code



U.S. Code: Title 26 - INTERNAL REVENUE CODE

There are 314 Updates Pending. Select the tab below to view.

Current through Pub. L. 113-75. (See Public Laws for the current Congress.)

- Subtitle A—Income Taxes (§§ 1-1564)
- Subtitle B—Estate and Gift Taxes (§§ 2001-2801)
- Subtitle C—Employment Taxes (§§ 3101-3510)
- Subtitle D—Miscellaneous Excise Taxes (§§ 4001-5000C)
- Subtitle E—Alcohol, Tobacco, and Certain Other Excise Taxes (§§ 5001-5891)
- Subtitle F—Procedure and Administration (§§ 6001-7874)
- Subtitle G—The Joint Committee on Taxation (§§ 8001-8023)
- Subtitle H—Financing of Presidential Election Campaigns (§§ 9001-9042)
- Subtitle I—Trust Fund Code (§§ 9500-9602)
- Subtitle J—Coal Industry Health Benefits (§§ 9701-9722)
- Subtitle K—Group Health Plan Requirements (§§ 9801-9834)

- And the winner is…

One-Time-Pad

- First described in 1882; patented in 1917
- Secure **if** the one-time-pad…
  - is created in a truly random manner
  - hasn’t been compromised (stolen)
  - any part of the one-time-pad is used only once for encryption
- Mathematically proven undecipherable

One-Time-Pad (cont.)

- Vulnerabilities:
  - true random generation is not trivial; see ℹ
  - distribution can be problematic
  - can be unknowingly compromised (stolen)
  - rigorous discipline must be exercised in its use

One-Time-Pad (cont.)

q9W9dctDPhm3iwxUJ9x8A4JFPYRrRXRfcnhu4d

2zPbMe5bu3bksk2E7uokkUe6jrccWQtTT43jDff

DKC4a3iXVaSpSuvZ97SMcCtWpqpCEuLEm5FH2i

wegZENgDncz2hfBPY5uYPjg8jxiBE7pWDa5Rqb

BdNLmY8iRkzLAUuA4jz4Me4goxvNU94FxCBaw

j5CMpeqSN5k2ixdyNvbntQ8mxo8w6GyfqgJqe7

AJGsiQaLimDxBF2t7yNmW6eNX666GqdsV8hF

QpYywW2kZzoEY88FAFdu5CWHckST73RtHp7A

gDRp7knWtpGTxRorZ4HPPEDTfRRF86oQJCEreD

One-Time-Pad (cont.)

- Alice wants to send a private message to Bob
- Both Alice and Bob have the same randomly generated one-time-pad
- Alice encrypts her message with the one-time-pad and sends it to Bob
- With the one-time-pad, Bob decrypts the message to get the plaintext

One-Time-Pad (cont.)

- Alice’s message to Bob: Go home! (plaintext)

Letter	G	o	(space)	h	o	m	e	!
ASCII	71	111	32	104	111	109	101	33

OT-Pad	p	C	Z	j	f	H	z	P
ASCII	112	67	90	106	102	72	122	80

- Adding the two (71+112) = 183, etc…

Encrypted Message	·	^{2}	z	Ò	Õ	µ	ß	q
ASCII	183	178	122	210	213	181	223	113

See ⓘ for an 8-bit ASCII table

One-Time-Pad (cont.)

- Bob decrypts the message by subtracting the same one-time-pad values…

Encrypted Message	▪	²	z	Ò	Õ	µ	ß	q
ASCII	183	178	122	210	213	181	223	113
OT-Pad	-112	-67	-90	-106	-102	-72	-122	-80

- To get the plaintext…

Letter	G	o	(space)	h	o	m	e	!
ASCII	71	111	32	104	111	109	101	33

Some Thoughts and Recommendations

- Encrypt sensitive information
  - Provides a means to secure privacy
  - Helps prevent identity theft
  - Makes disposal of obsolete equipment easier
- No such thing as 100% assurance of security
- Encryption software is readily available—free and for fee
- Typically can be set up in 15-30 minutes

Thoughts and Recommendations (cont.)

- Be very carefully in choosing a master password
- When in doubt, encrypt
- Make several copies of your encrypted information and store apart from your computer

Choosing a Master Password

- Password (passphrase) suggestions:
  - Minimum 16 characters (128 bits)
  - Something easy to remember
  - A mixture of upper/lower case letters, symbols and numbers
- Examples

#MyBrotherIsAnIdiotIQ=45 [24 chars]

BKutfYwZtf2PVa7b [16 char; but you won’t remember it]

Choosing a Master Password (cont.)

- Don’t share you password with ***anyone***
- Store the master password in your bank safe-deposit box*
- Don’t use the password for anything else

***If you forget your master password your goose is ~~cooked~~ cremated**

Encryption Software for Home Computers

Name	Encryption Functions	Systems	Price	Source	Comments
TrueCrypt	Files, folders, disks, Multiple devices	Windows, OS X, Linux	Free	ⓘ	Easy to install and use. Open source
Cryptainer	Files, folders, disks, Multiple devices	Windows	Free $30-$70	ⓘ	Easy to install and use. Proprietary
BitLocker	Complete disk drive. Multiple devices	Windows only	Free	ⓘ ⓘ	Part of OS. Proprietary
FileVault	Only complete disk drive	OS X only	Free	ⓘ ⓘ	Part of OS. Proprietary
GNU Privacy Guard (GnuPG)	Files, e-mail,	Windows, OS X, Linux, Unix	Free	ⓘ ⓘ ⓘ	Complex. Public/private key encryption. Open Source
WinZip 18	Files, folders, e-mail	Windows, OS X, iOS, Android	$29.95	ⓘ	Proprietary
7-Zip	Files, folders, e-mail	Windows, OS X, Linux, Unix	Free	ⓘ	Open Source

Encryption for E-Mail

- Third-party applications
  - Sendic for Microsoft Outlook (free and $5/month) ℹ
  - Symantec Desktop Email Encryption ($175/yr) ℹ
  - CryptoMailer 5 ($100/yr) ℹ
  - Voltage Security Cloud SecureMail ($99/user/year) ℹ
  - HushMail (free, $35/yr and $50/yr) ℹ
- Many other secure e-mail services for business ℹ

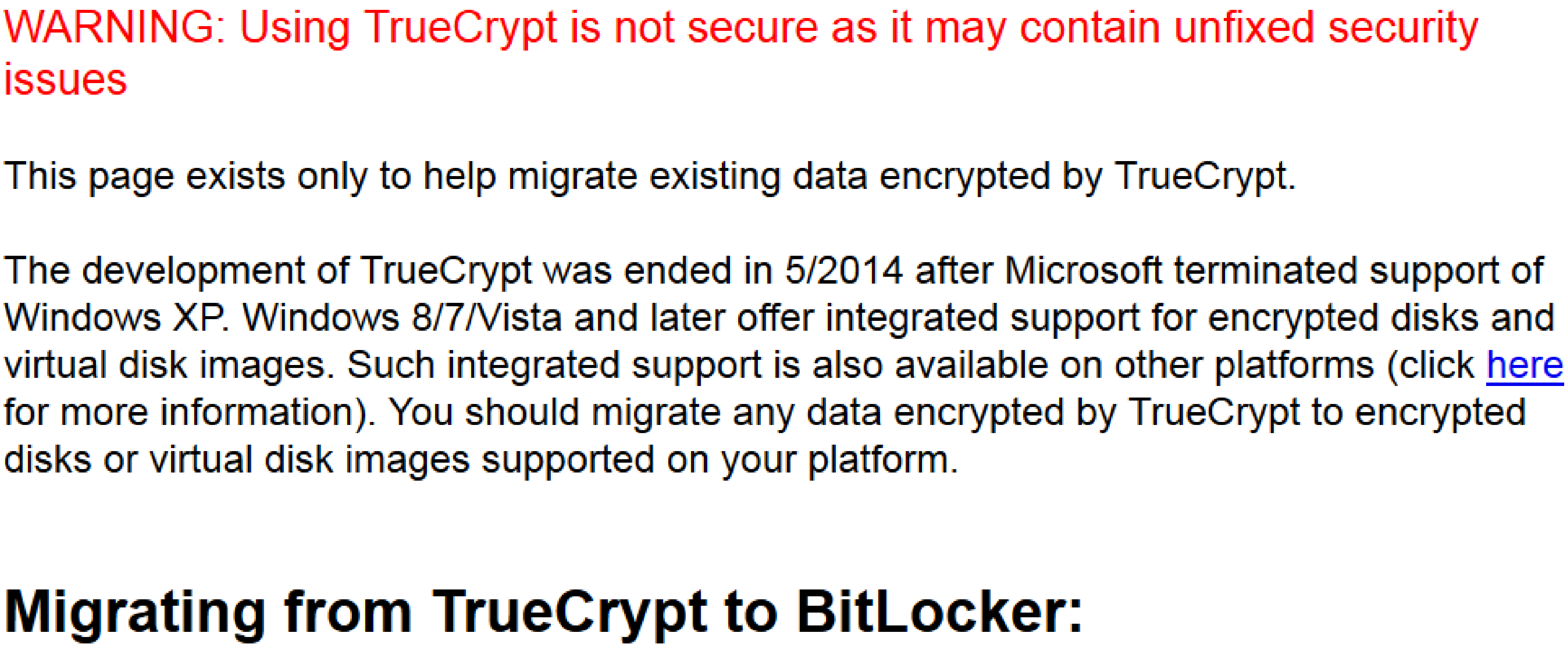
Encryption for E-Mail (cont.)

- Outlook, Apple Mail and Thunderbird
  - Encrypted attachments (TrueCrypt, Cryptainer, WinZip, GnuPG)
  - Exchange of public/private keys via a digital ID (certificate) used within an application

The "Demise" of TrueCrypt

From: http://truecrypt.sourceforge.net/ (May 28, 2014)

<u>Do not download</u> TrueCrypt from this Web site: For balanced explanations see:



WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues

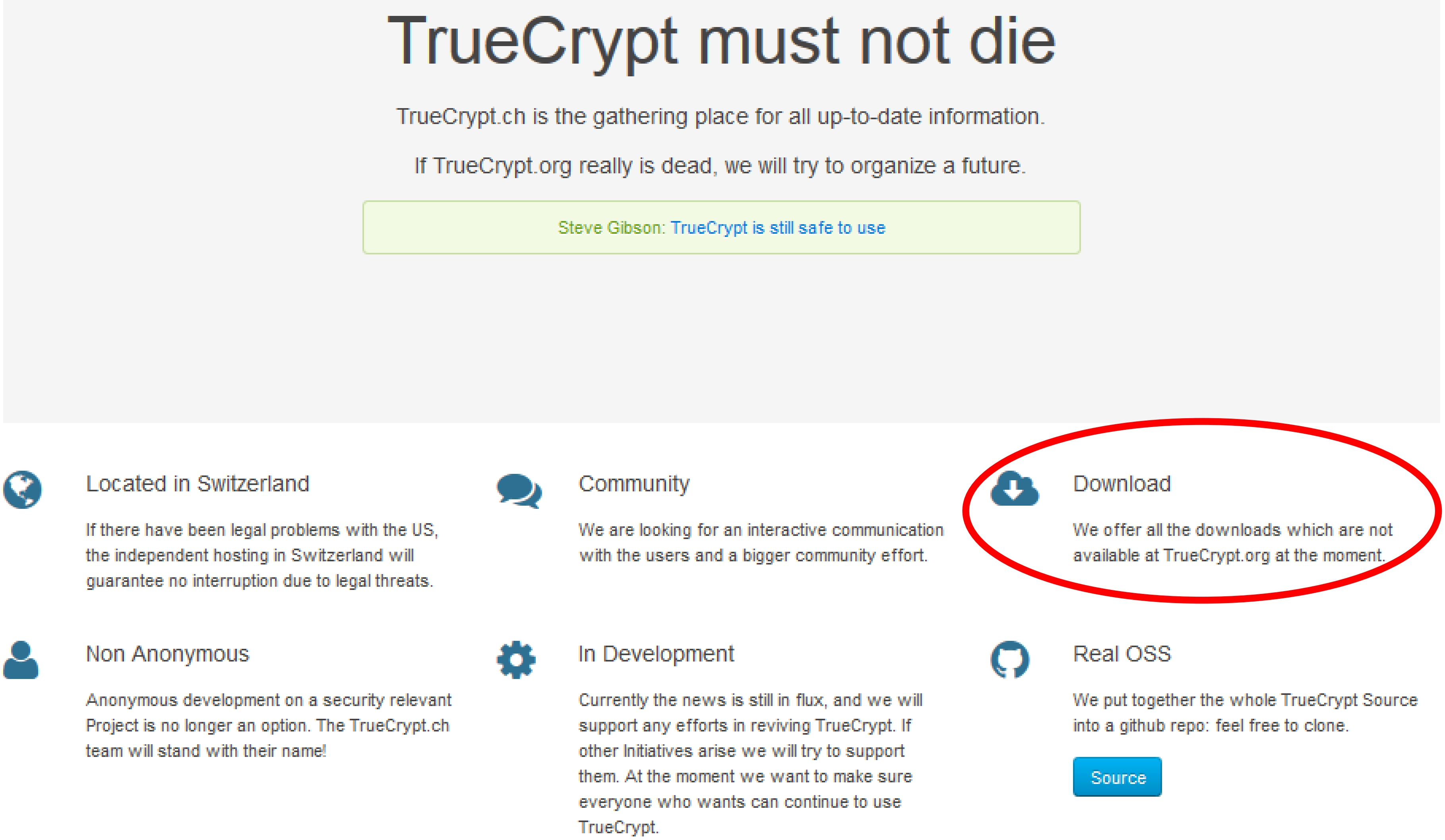
This page exists only to help migrate existing data encrypted by TrueCrypt.

The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windows XP. Windows 8/7/Vista and later offer integrated support for encrypted disks and virtual disk images. Such integrated support is also available on other platforms (click here for more information). You should migrate any data encrypted by TrueCrypt to encrypted disks or virtual disk images supported on your platform.

Migrating from TrueCrypt to BitLocker:

TrueCrypt Lives!

From: http://truecrypt.ch/ (June 2, 2014)



TrueCrypt must not die

TrueCrypt.ch is the gathering place for all up-to-date information.

If TrueCrypt.org really is dead, we will try to organize a future.

Steve Gibson: TrueCrypt is still safe to use

Located in Switzerland

If there have been legal problems with the US, the independent hosting in Switzerland will guarantee no interruption due to legal threats.

Community

We are looking for an interactive communication with the users and a bigger community effort.

Download

We offer all the downloads which are not available at TrueCrypt.org at the moment.

Non Anonymous

Anonymous development on a security relevant Project is no longer an option. The TrueCrypt.ch team will stand with their name!

In Development

Currently the news is still in flux, and we will support any efforts in reviving TrueCrypt. If other Initiatives arise we will try to support them. At the moment we want to make sure everyone who wants can continue to use TrueCrypt.

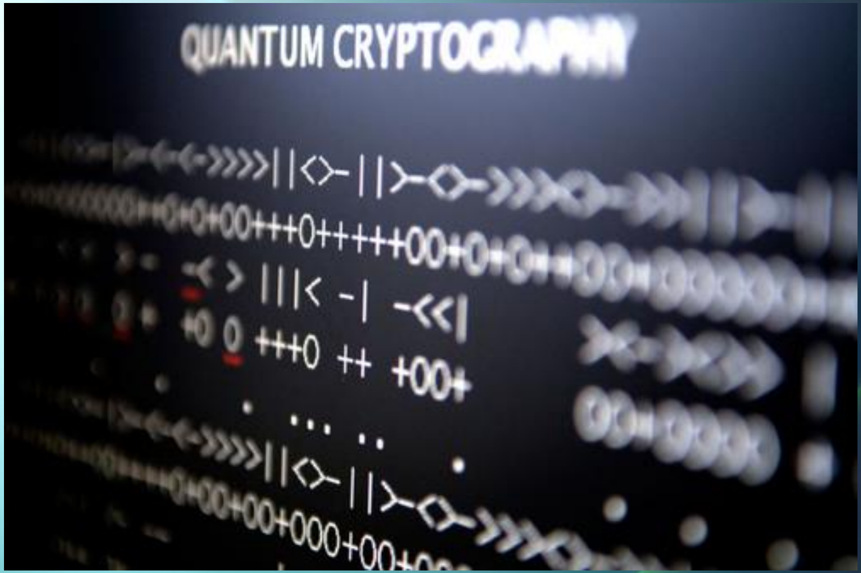
Real OSS

We put together the whole TrueCrypt Source into a github repo: feel free to clone.

Future Cryptology

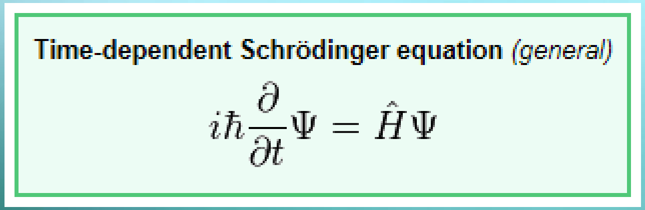
- What’s coming down the pike…

Cats & Quantum Cryptography



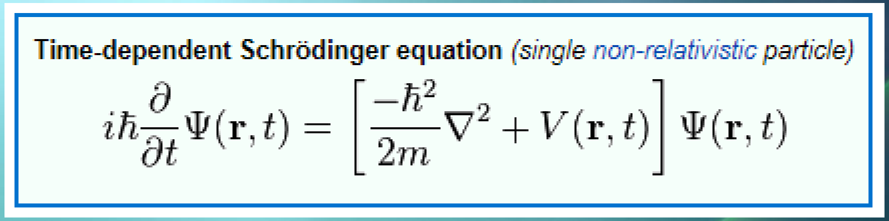
Erwin Schrödinger

- Austrian physicist 1887-1961
- 1933 Nobel Prize in physics with Paul Dirac
- Schrödinger equations (quantum mechanics)…



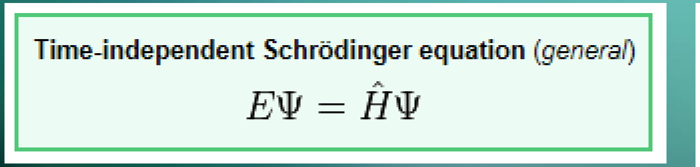
Time-dependent Schrödinger equation *(general)*

$$i\hbar\frac{\partial}{\partial t}\Psi = \hat{H}\Psi$$



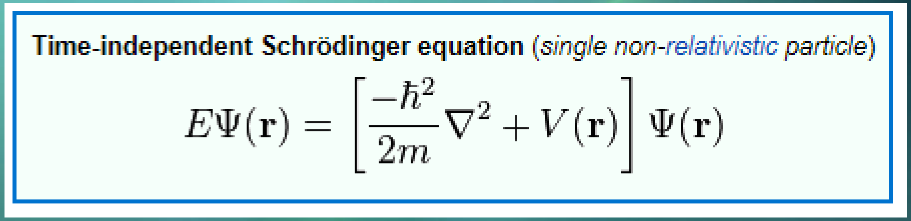
Time-dependent Schrödinger equation *(single non-relativistic particle)*

$$i\hbar\frac{\partial}{\partial t}\Psi(\mathbf{r},t) = \left[\frac{-\hbar^2}{2m}\nabla^2 + V(\mathbf{r},t)\right]\Psi(\mathbf{r},t)$$



Time-independent Schrödinger equation *(general)*

$$E\Psi = \hat{H}\Psi$$



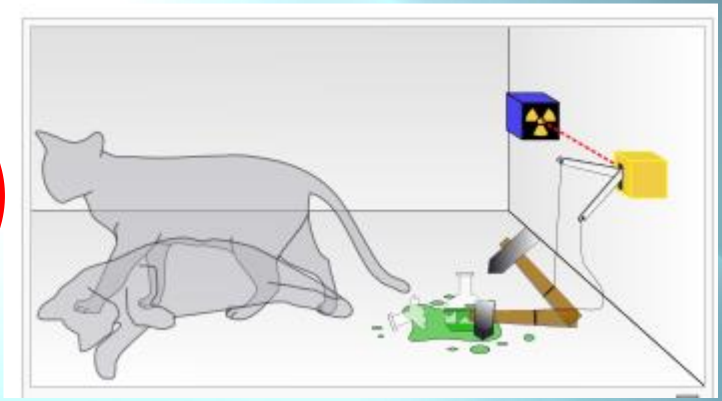
Time-independent Schrödinger equation *(single non-relativistic particle)*

$$E\Psi(\mathbf{r}) = \left[\frac{-\hbar^2}{2m}\nabla^2 + V(\mathbf{r})\right]\Psi(\mathbf{r})$$

Schrödinger's Cat

(A Thought Experiment)

What if a cat behaved Like a sub-atomic particle?



A cat, flask of poison, radioactive source and a detector in a box

The detector detects radioactivity and shatters the flask

The poison kills the cat… **or does it?**

The cat is simultaneously alive <u>and</u> dead

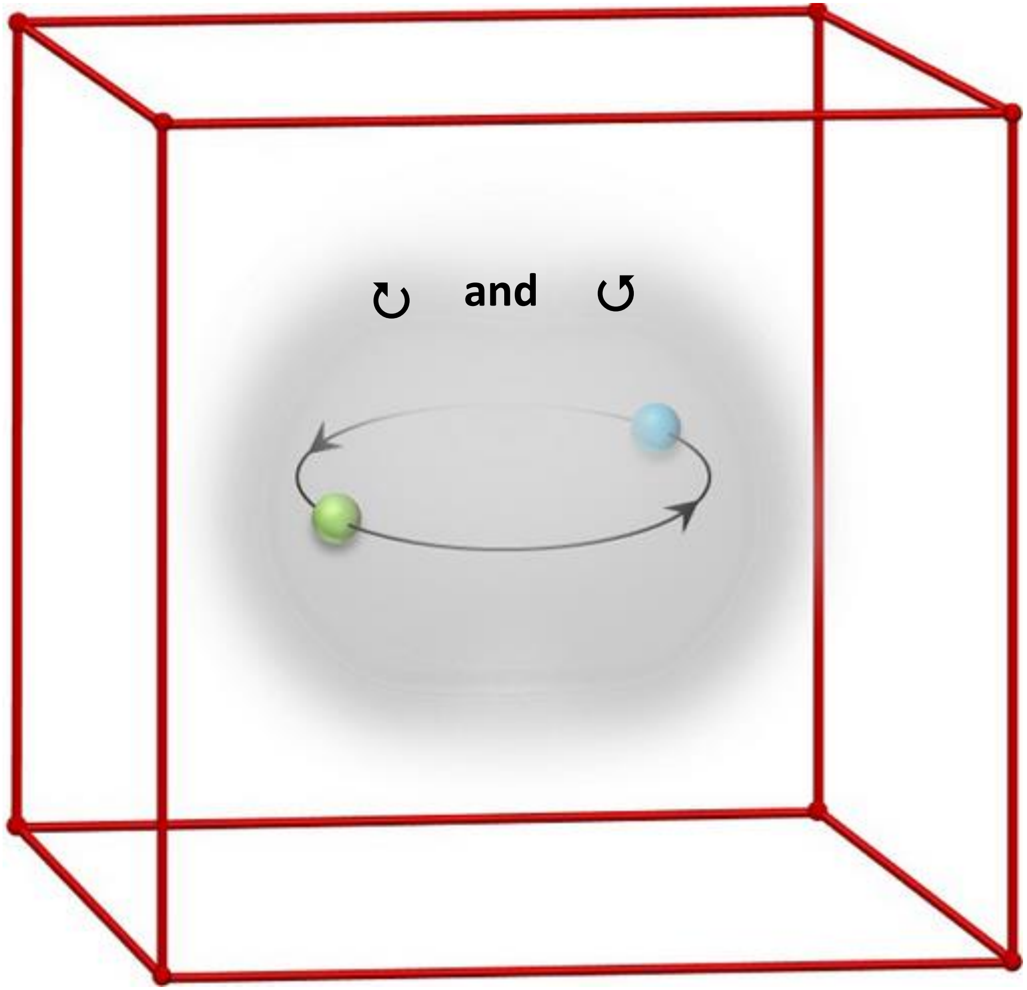
This is known as “superposition”

“And for show and tell today, little Erwin here has brought his cat”

Bits & Qubits

- A classical bit has a value of 0 or 1
- A quantum bit (qubit) has a value of 0 and 1 simultaneously (“superposition”)
- A photon can act as a qubit; it has two spin states ↻ and/or ↺

A Particle (photon) in a Box

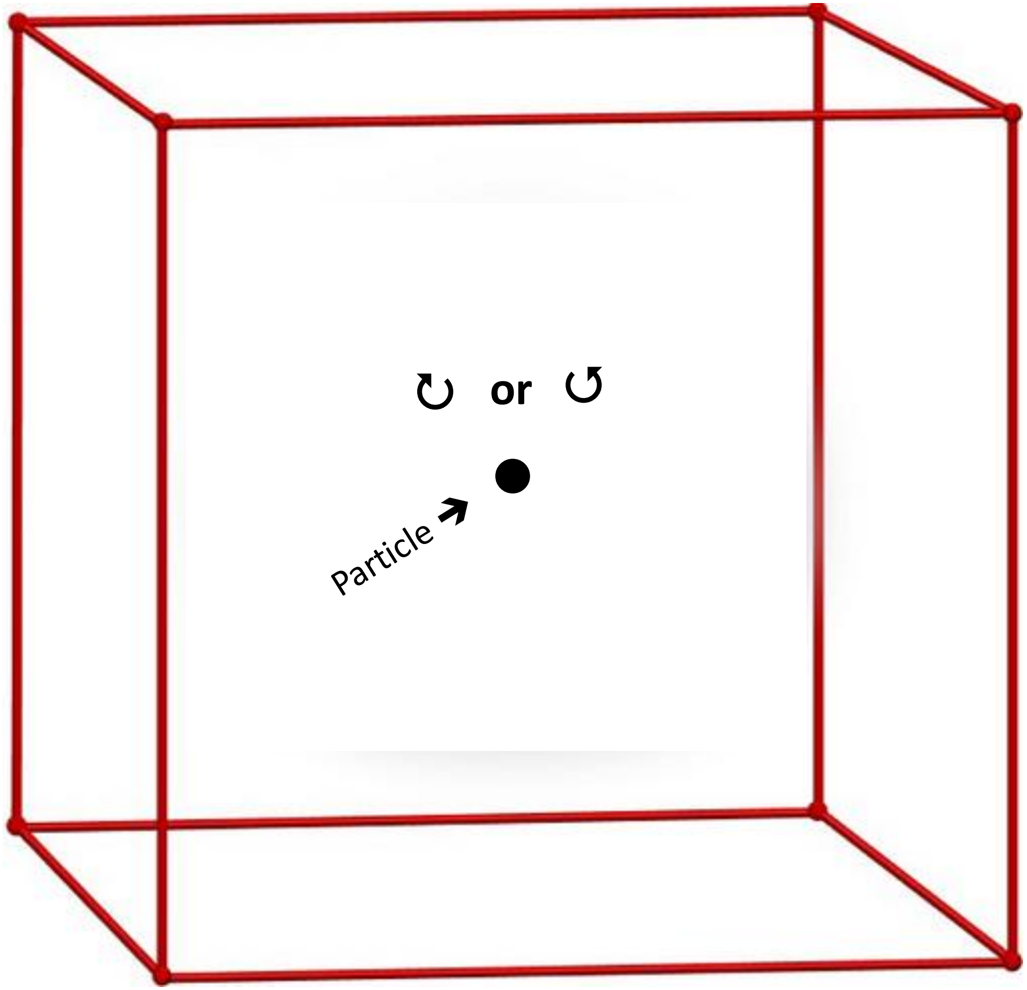


↻ and ↺

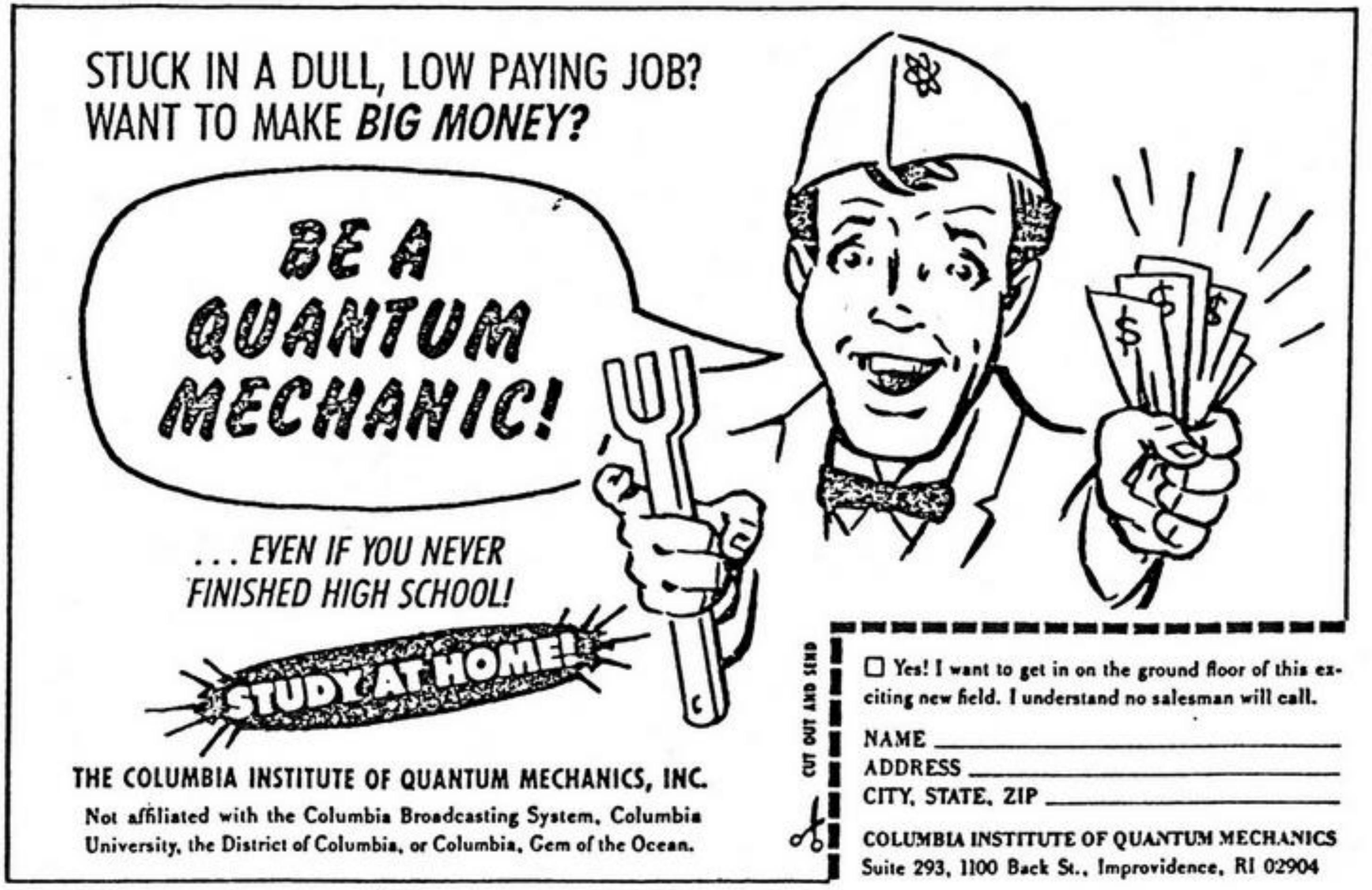
State of superposition

A Particle (photon) in a Box

Look at the particle in the box…



Now that you understand quantum mechanics…



STUCK IN A DULL, LOW PAYING JOB?
WANT TO MAKE *BIG MONEY?*

. . . EVEN IF YOU NEVER FINISHED HIGH SCHOOL!

THE COLUMBIA INSTITUTE OF QUANTUM MECHANICS, INC.

Not affiliated with the Columbia Broadcasting System, Columbia University, the District of Columbia, or Columbia, Gem of the Ocean.

□ Yes! I want to get in on the ground floor of this exciting new field. I understand no salesman will call.

NAME ______________________________
ADDRESS ____________________________
CITY, STATE, ZIP _____________________

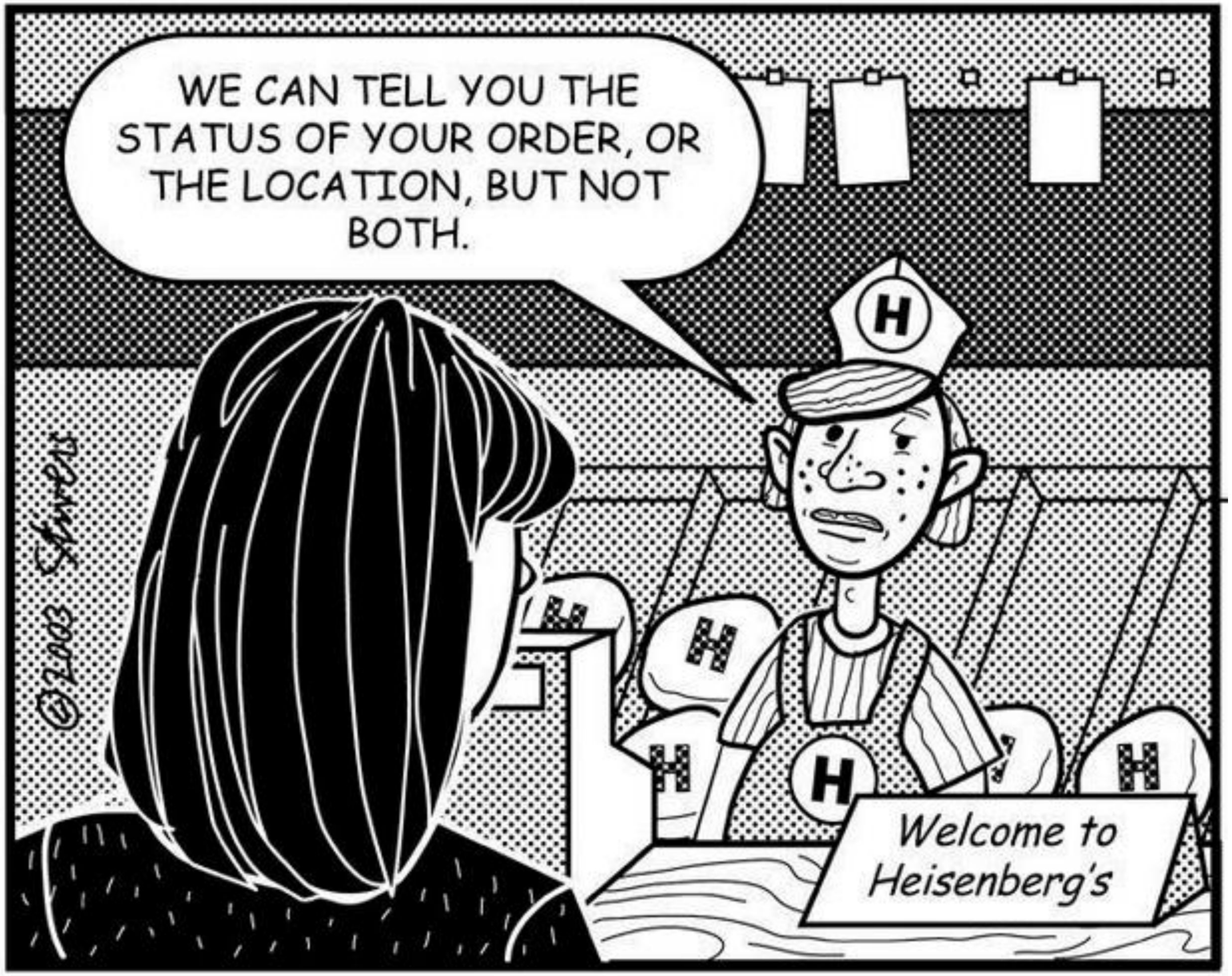
COLUMBIA INSTITUTE OF QUANTUM MECHANICS
Suite 293, 1100 Back St., Improvidence, RI 02904

Heisenberg’s Uncertainty Principle

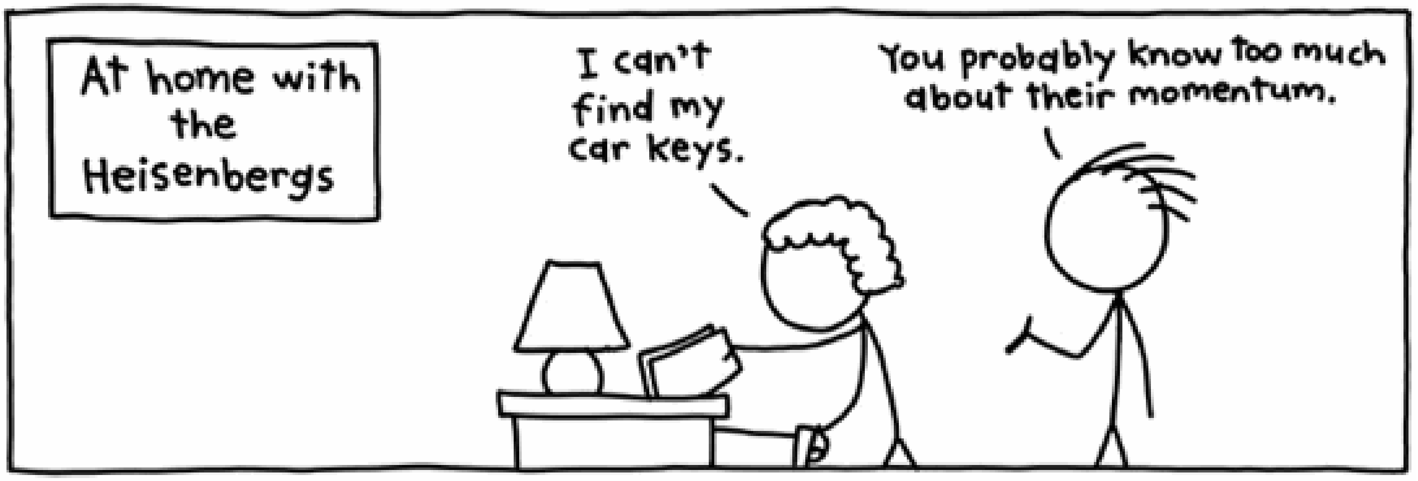
- It's impossible to know both an [sub-atomic] object's position and velocity at the same time
- “The more precisely the position of a [sub-atomic] particle is determined, the less precisely the momentum is known in this instant, and vice versa.” 1927

Werner Heisenberg 1901-1976, German physicist. Nobel Prize in physics 1932

Now that you understand Heisenburg's uncertainty principal...


WE CAN TELL YOU THE STATUS OF YOUR ORDER, OR THE LOCATION, BUT NOT BOTH.
Welcome to Heisenberg's
©2003 Shivers
H

You’ll smile if you truly understand Heisenburg’s uncertainty principal…


At home with the Heisenbergs
I can't find my car keys.
You probably know too much about their momentum.

Frau
Heisenberg

Herr Dr.
Heisenberg

Alice Sends Message to Bob

(via quantum encryption)

- Alice sends the key as a series of photons for which the spin is known (polarized light)
- The spin of each photon is represented by 1 for (↻)or 0 (↺)
- The encryption key is 0110
- Repeated transmission with the same result confirms transmission has not been intercepted
- QKD—**Q**uantum **K**ey **D**istribution

Alice Sends Message to Bob (cont.)

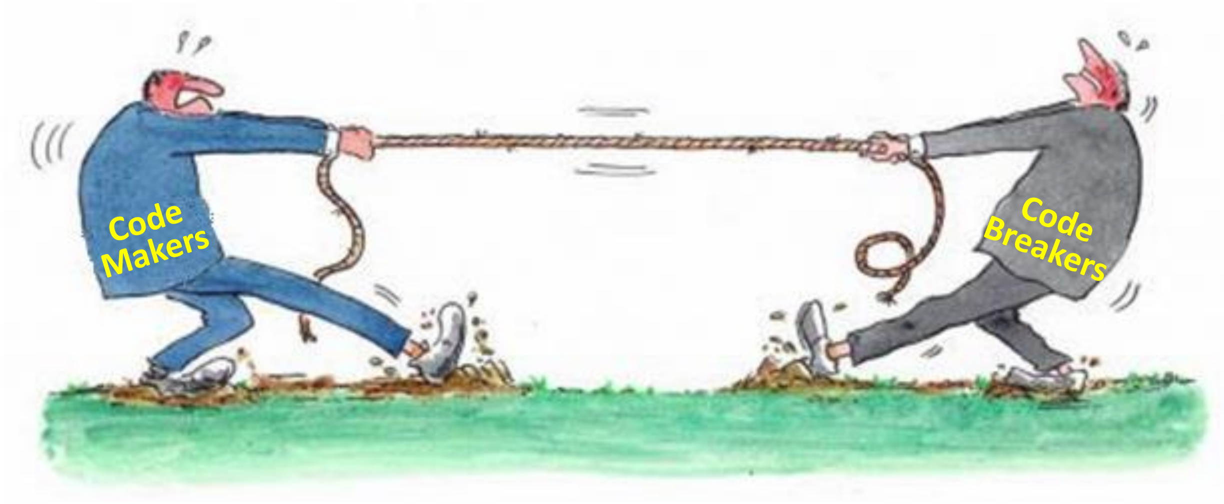
(via quantum encryption)

- The plain text is 1011
- Alice adds the encryption key (0110) to the plain text to get the cipher text 1101
- The enciphered text is transmitted to Bob either by traditional or quantum transmission
- Bob subtracts the encryption key 0110 from the enciphered text (1101) to get the plain text 1011

Organizations Involved in Quantum Cryptography

- Swiss Quantum ⓘ
- Tokyo QKD Network ⓘ
- Battelle ⓘ
- Max Planck Institute ⓘ
- Los Alamos National Labs ⓘ
- National Security Agency ⓘ
- Scientific paper ⓘ
- Quantum cryptography system hacked ⓘ

Constant Strife & Competition



Books on Cryptography

- *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, David Kahn, revised 1996, Scribner, New York, 1181 pp.
- *Codes, Ciphers & Other Cryptic & Clandestine Communications*, Fred B. Wrixon, 1998, Black Dog & Leventhal, New York, 704 pp.
- *ICSA Guide to Cryptography*, Randall K. Nichols, 1999, McGraw-Hill, New York, 837 pp.
- *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*, Steven Levy, Viking, New York, 2001, 356 pp.
- *The Emperor's Codes: The Breaking of Japan's Secret Ciphers*, Michael Smith, Penguin Books, New York, 2000, 335 pp.
- *Disappearing Cryptography: Information Hiding; Steganography & Watermarking*, 2nd Ed., Peter Wayner, Morgan Kaufmann Publishers, New York, 2002, 412 pp.
- *Between Silk and Cyanide: A Codemaker's War 1941-1945*, Leo Marks, The Free Press, New York, 1998, 614 pp.
- *Cryptography: A Very Short Introduction*, Fred Piper and Sean Murphy, Oxford University Press, Oxford, 2002, Kindle Edition.

Thanks for your attention!

I forgot the password for the file where I keep all my passwords.
www.maxine.com
JWagner
11-14