A History of Factoring in the Real World

Paul Leyland
Brnikat Ltd

Part I — Ancient History

The beginnings

- ~450BCE, Pythagorean mystics classified integers:
  - 1 monad (unity) generator of numbers
  - 2 dyad (diversity, opinion) first female number
  - 3 triad (harmony = unity + diversity) first male number
  - 4 (justice, retribution) squaring of accounts
  - 5 (marriage) = first female + first male
  - …
- Discovery of incommensurable numbers:
  - Some numbers are irrational — immeasurable by ratios
  - Some numbers are prime — immeasurable except by unity

Almost completely uninteresting

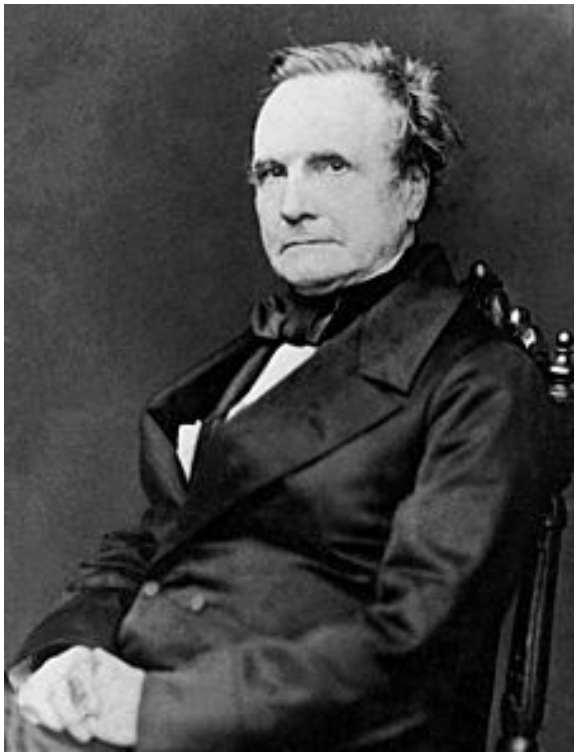
- Everyone else had little or no interest in primes and composites, or in integer classification at all
- No known records at all in Egyptian, Babylonian and Chinese mathematics
- A few unimportant results in Indian documents

Almost completely useless

- Only use for around 2000 years is reducing factors to lowest terms
  - 2/3 + 4/5 - 13/60 =
  - 40/60 + 48/15 - 13/60 =
  - 75/60 =
  - (3*5*5)/(2*2*3*5) =
  - 5/(2*2) =
  - 5/4

Part II — Mediæval History

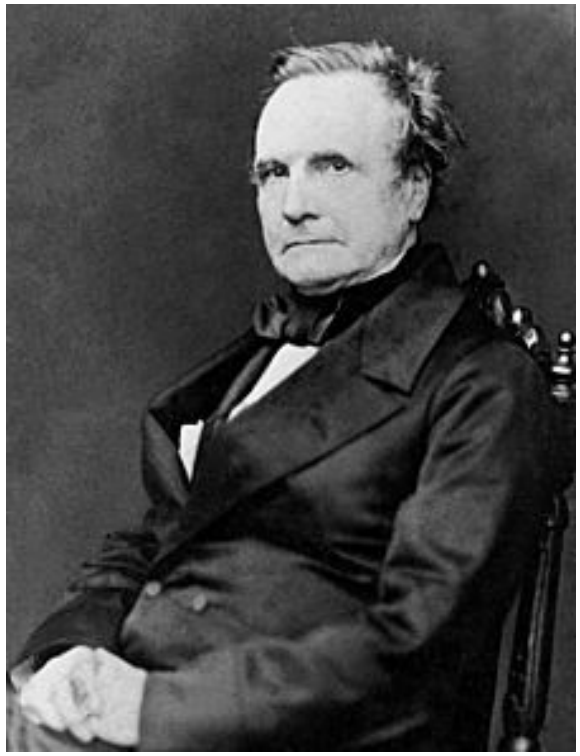
Three cryptographers



Three cryptographers

Alberti

Vigenére



Babbage

Cryptography and Z_N

- Encode letters as small integers
- Generate key stream
- Ciphertext = plaintext + keystream in $\mathbf{Z}_N$

- Alberti: keystream as repetition of key word
  - "Vigenére cipher"
- Babbage: find patterns and factor separation
  - "Kasiski analysis"

Example of Kasiski analysis

Location:	01234 56789 01234 56789 01234 56789
Keyword:	RELAT IONSR ELATI ONSRE LATIO NSREL
Plaintext:	TOBEO RNOTT OBETH ATIST HEQUE STION
Ciphertext:	KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

Bigram	Locations	Separation	Factors
KS	0, 9	9	3, 9
SM	1, 10	9	3, 9
ME	2, 11	9	3, 9

Keyword is probably 3 or 9 letters long, so solve as
3 or 9 monalphabetic ciphers

Three from the computer era

Three from the computer era

Three from the computer era

Three from the computer era

Bill Tutte

Tommy Flowers

Adolf Hitler

Tutte & *Tunny*, Flowers & *Colossus*

- Tutte @ Bletchley Park given job of breaking teleprinter cipher codenamed *Tunny*
- First spotted patterns of separation 574 bits
- 574 = 2*7*41 suggests a 41-tooth rotor
- Similar approach to reverse-engineer rest of the German cipher machine
- Tommy Flowers designed and built *Colossus* to break *Tunny* traffic at high speed

Part III — Modern History

Slightly interesting and almost useful

~1850 — ~1950 mechanical calculators made larger factorizations easier

~1950 — ~1975 electronic computers made large factorizations possible

Interest in new algorithms: rho, P-**1**, P+**1**, CFRAC, …

“Useful” for stress-testing hardware

“Useful” for marketing

And another three ...

And another three ...

Rivest

Shamir

Adleman

Interesting and useful, at last

- With RSA , factoring becomes useful
- In consequence, factoring becomes interesting
  - to computer scientists
  - to economists
  - to politicians
  - to industrialists
  - to lawyers
  - to hobbyists
  - perhaps, even, to mathematicians?

Predictions

- **Mersenne** (1644): “quemadmodum & agnoscere num dati numeri 15, aut 20 caracteribus constantes, sint primi necne, cum nequidem sæculum integrum huic examini, quocumque modo hactenus cognito, sufficiat”
- **Rivest** (1977, reported by Gardner): Factoring a 125 digit integer with the best available methods on a computer much faster than anything presently available would take 40 quadrillion years
- **Knuth** (1981): “It is inconceivable at this time that such an N [250 digits] could be factored”

Rivest's Law

- Rivest's Law: It is foolish to predict when an integer of any particular size may be factored

RSA ubiquitous and very important

- RSA certificates are everywhere:
  - Signed financial transactions
  - Signed software for authenticity detection
  - PGP, etc., keys
  - Smart cards
  - Networking infrastructure security
  - …
- First are worth gigabucks **daily**
- Second are worth gigabucks to some suppliers

Factoring for profit

- Definitely legal: solving challenges
- Possibly legal: factoring clients' integers for a fee
- Definitely illegal: fraud, extortion, …

Challenges

- Scientific American, 1977. RSA-129 factored in 1994 and $100 prize donated to charity
- RSA Data Security Inc. pay multiple $10k in period 1991 – 2005. Several world-record factorizations occurred in this effort.
- Simon Singh paid £10,000 in 2000 for the factors of a 512-bit integer in *The Code Book*

Honderd dollar voor twee priemgetallen

Illustratie Jack Prince

Wat zegt het nieuwe record nu over de veiligheid van RSA als zodanig? Merkwaardigerwijs toont het eerder de kracht ervan dan de zwakte

kunnen spionnen de boodschap niet achterhalen.

Als sleutelgetal van RSA wordt altijd het produkt gebruikt van twee grote priemgetallen. Dat produkt, de zogenaamde *modulus*, hoeft niet geheim te blijven, maar de twee priemgetallen waaruit het is samengesteld wèl. Zou een spion namelijk die priemgetallen kennen, dan zou hij daarmee

werd geïntroduceerd, schreef Martin Gardner er een artikel over in *Scientific American*. Daarin publiceerde hij als uitdaging voor zijn lezers een sleutelgetal van 129 cijfers en een 'cryptogramgetal', dat wil zeggen de vertaling in RSA-geheimschrift met behulp van die sleutel van een stukje Engelse tekst. De vercijfer- en ontcijfermethodes wer-

In 1977 schatte Ronald Rivest de tijd die nodig zou zijn voor het kraken van het sleutelgetal, dat inmiddels bekend staat als RSA-129, op 40 biljard jaar, en velen meenden daarom destijds dat die honderd dollar wel nooit geïnd zouden worden. Maar inmiddels heeft de technologie niet stilgestaan, terwijl ook de wiskundigen niet stil hebben gezeten. Het gevolg is dat Rivest reeds zeventien jaar na dato de honderd dollar van de bank kon halen om ze aan codebreker Arjen Lenstra te overhandigen. Die zal zijn prijs echter moeten delen met ongeveer 1700 computerhobbyisten over de hele wereld die via het internationale computernetwerk Internet allemaal hun steentje aan de ontbinding heb-

Factoring as a social activity 1

- RSA-129 project: 600 people for 8 months in 1993-4, co-ordinated by email & Usenet
- Numerous ad hoc groups contribute to Cunningham project: Mullfac, NFSNET, etc
- CWI, the Cabal, EPFL, NTT, Le High, Sun, BSI, Bonn University, MS Research, INRIA, and many others, solved several RSA challenge factorizations 1995-2009

Factoring as a social activity 2

- Berkeley Open Infrastructure for Network Computing (BOINC)
  - yoyo@home general ECM factoring
  - NFS@home
- ECMNET client/servers for various projects
- Mersenneforum.org
  - Chat
  - Co-ordinating projects
  - Reporting results

Factoring as a social activity 3

- Made possible by generous release of software
  - LIP, GMP, gwnum arithmetic libraries
  - Factor-by-email, Fafner, ECMNET, BOINC, cabald/cabalc, NFSNET client-server harnesses
  - CWI suite
  - GMP-ECM
  - GGNFS
  - Msieve
  - Yafu
  - and much more

Factoring and PPE

Factoring and PPE

- Oxford University created an undergraduate degree course in the 1920's called *Philosophy, Politics and Economics*, widely known as PPE

Philosophy

- Should we be entrusting so much to RSA?
- NIST recommended minimum key sizes
  - 1024 bits up to 2010 at latest
  - 2048 bits up to 2030 at latest
  - 3072 bits thereafter
- Mozilla will reject all <1024-bit certificates from 2014-01-01

Politics — 1

- “Cryptowars” of 1990’s — governments attempt to make secure communications illegal without access to keys
- 1998: Digital Millennium Copyright Act in US makes it illegal to circumvent cryptographic protection

Politics — 2

- Blacknet, 1993: anonymous information trading by way of PGP-encrypted public messages
- “Blacknet” key created with 384-bit modulus
- Encrypted mail posted with that key
- 1995: Gillogly, Lenstra, Leyland & Muffett factor “Blacknet” key, and in secret
- Embarrassing visit from the Feds …

Politics — 3

- Texas Instruments protect calculator operating systems with 512-bit RSA signatures
- 2009: Keys factored and signatures forged
- TI sends in the lawyers armed with DMCA

Economics

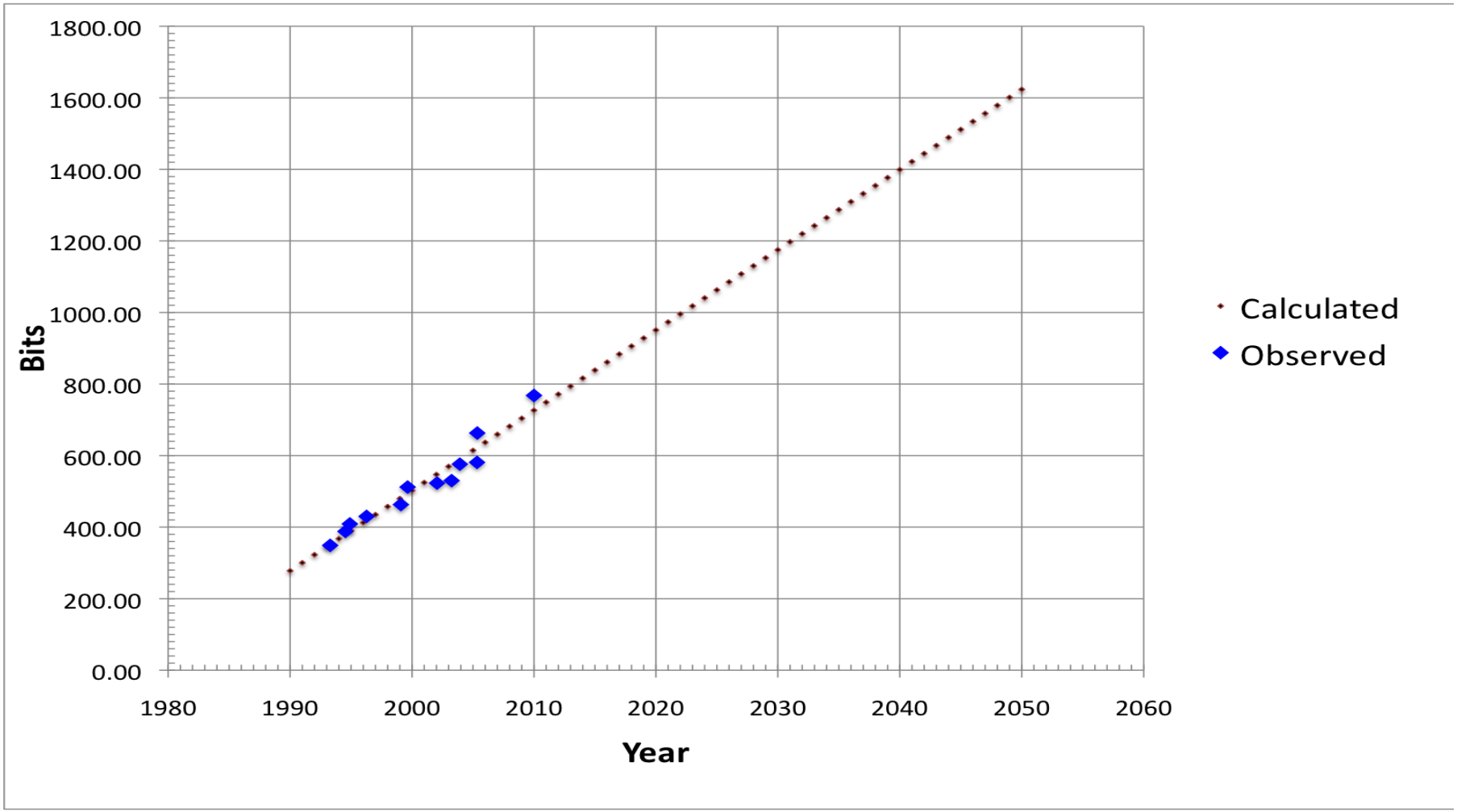
- CREST set up in mid 1990's with 512-bit keys
- 1995: Anderson & Leyland wrote to the Bank of England suggesting that this was unwise
- 1999: RSA-512 was factored
- January 2000: Leyland invited by BoE to give consultancy on RSA security

Part IV — Future History

Record GNFS factorizations

Number	Size in bits	Date factored
3,367- c105	349	1993-04-??
p(11887)	388	1994-07-18
p(13171)	409	1994-11-26
RSA-130	430	1996-04-10
RSA-140	463	1999-02-02
RSA-512	512	1999-08-22
2,953+ c158	523	2002-01-19
RSA-160	530	2003-04-01
RSA-576	576	2003-12-03
11,281+ c176	581	2005-05-02
RSA-200	663	2005-05-09
RSA-768	768	2009-12-12

Record GNFS factorizations



Prediction

The first 1024-bit hard factorization will occur in

2023

Prediction

The first 1024-bit hard factorization will occur on

2023

March 29th

Prediction

The first 1024-bit hard factorization will occur at

2023

March 29th

12:32 p.m.

Questions?