Codebreaking at Bletchley

Rod Downey
Victoria University
Wellington
New Zealand

Downey's research is supported by the Marsden Fund, and this material also by the Newton Institute, Cambridge, and the Institute for Mathematical Sciences, Singapore.

Singapore, August/September 2015

Turing

- I wish to give you some idea as to how the codebreaking efforts at Bletchley Park helped the Allies win WWII.
- Turing has become a larger than life figure following the movie "The Imitation Game".
- which followed Andrew Hodges book "Alan Turing : The Enigma",
- which followed the release of classified documents about WWII.
- I will try to comment on aspects of Turing's work mentioned in the movie.
- I will give extensive references if you want to follow this up, including the excellent Horizon documentary.
- Posted to my web site. Type "rod downey" into google.

Turing Award

- The equivalent of the "Nobel Prize" in computer science is the ACM Turing Award.
- It is for life work in computer science and worth about $1M.
- Why? This award was made up (1966) was well before Bletchley became public knowledge.
- (Aside) Prof. D. Ritchie (Codebreaker)-from "Station X, Pt 3"

  Alan Turing was one of the figures of the century. —— There were great men at Bletchley Park, but in the long hall of history Turing's name will be remembered as Number One in terms of consequences for mankind.

Why?

- Actually that is another story involving the conceptual basis for the digital computer.
- What I will do
- In this talk I will look at other work.
- The Codbreaking effort was one of the first large datamining efforts, and the combined effort of 10,000 workers.
- Involved the combined talents of classicists (e.g. Archaelogists), mathematicians, and others.

Cryptography

- I will try to give a brief overview of the history of ciphers.
- Caesar cipher. (Though I can't believe it was ever used) Substitute e.g. move every letter 4 places. $A \to D, B \to E$, etc.
- The Vigenère Cipher. (Bellaso 16th century) Use a key word to do the substitution.
- Key word GOLD corresponds to 7, 15, 12, 4. so "Too much hype" would become

t	o	o	m	u	c	h	h	y	p	e
G	O	L	D	G	O	L	D	G	O	L
Z	C	Z	P	A	Q	S	K	E	D	P

- If you choose a random key the same length as the message, then this is a one time pad and is secure, but has its own problems. (For example, for "Too much hype" you would need a key of length 11.)

Breaking ciphers

- What about the Vigenère Cipher?
- Historically, it was used by the French, Confederates in the American Civil War, and others with long keys, and they called it le chiffre indéchiffrable (French for 'the indecipherable cipher').
- You can buy now an app for the iphone and solve this in seconds.
- Broken using statistical analysis (Chi-squared) based on the that certain letters (like "e") are much more common than others. (The Kasiski Attack)

Chi-squared

- Suppose that there are n objects being put into q boxes, where the probability that each object goes into the ith box is p_i.
- Then the expected number of objects in the ith box is $e_i = np_i$.
- Now suppose that the actual number of objects in the ith box is a_i.
- For example if there were only 3 letters in the alphabet (e.g. $\{a, b, c\}$, with probabiities $\frac{1}{2}, \frac{1}{8}, \frac{3}{8}$ then you would anticipate that if you had a text of 100 letters, likely 50 would be a, around 12 b, and 37 c.
- Then the chi-squared statistic is

$$\chi = \sum_{i=1}^{q} \frac{(a_i - e_i)^2}{e_i}.$$

- The larger the value of χ, the more surprised we would be. Statistics students would know that we eventually become sufficiently surprised that we cease to believe that the original probabilities are correct.

For Vigenére Cipher

1. Guess a key length i.
2. Find the 26 chi-squared statistics for the message consisting of all letters whose distance is a multiple of i apart.
3. If the key length is not i, then all of the values should be relatively large and we have made the wrong guess. and we can move on to $i + 1$. Otherwise we have a low χ and we can hope that we have the right key length and, indeed, the first letter of the key.

- Interestingly, in a recently de-classified paper, Turing is carefully explaining the above to administrators.
- One of the main ideas of the WWII codes used by Germany and Japan were to have a "perfect spread" of letters so that the statistical attack above is impossible.
- More subtle (Bayesean) Statistics were basic to the Bletchley park attacks and war planning.

History

- Cryptanalysts were crucial in the first world war;
- Also in subsequent period. Iain Lobban, 2012 Director GCHQ:

  (With exceptions Germany and Russia diplomatic services who only used one time pads), every single encryption system used by foreign governments to protect their communications with UK-based representatives were broken and read.

- From a letter to the ministry

  These were the cryptanalysists and a rummier lot I have seldom met.

- 1925 Enigma machine patented in London. Originally for commercial purposes.
- 1926, Edward Travis, deputy director, goes to Berlin and buys one from the manufacturer.

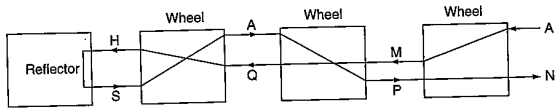
Enigma

Enigma

The process of cyphering is simple and quick. The message is 'typed' on a normal keyboard and as each letter is pressed, another letter is illuminated on a lampboard containing the 26 letters of the alphabet. The series of letters illuminated on the lampboard form the cypher text and the recipient of the cypher message, in possession of an identical machine, types out the cypher text and the decoded message appears on the lampboard.

Wheels

The main scrambler unit consists of 3 (later 4) wheels and an Umkehrwalze which I shall refer to henceforth as the Reflector—an admirable American translation. These wheels have on each side 26 contacts which we will for convenience label A to Z. The contacts on the one side are wired in an arbitrary and haphazard fashion to the contacts on the other. Each wheel is, of course, wired differently. The reflector has 26 contacts which are wired together arbitrarily in pairs. What happens when one of the letters of the keyboard is pressed may be seen from the following diagram.



The current in this example enters the right hand wheel at A and leaves it at M, A being wired to M in this wheel: it enters the middle wheel at M and leaves it at Q, and so on until it reaches the reflector, where it turns around and returns through the wheels in a similar fashion, eventually leaving the right hand wheel at position N and lighting the appropriate lamp in the lampboard. Pressing a key may light up any bulb except that which is the same as the key pressed—for a letter to light up itself it would be necessary for the current to return through the wheels by the same route as it entered and, from the nature of the reflector, this is clearly impossible. This inability of the machine to encypher a letter as itself is a vital factor in the breaking of Enigma. It should also be noted at this point that the machine is reciprocal, that is to say that, if at a given position of the machine N lights up A, then A will light up N.

Each time a key is pressed the right-hand wheel moves on one so that if, in the position immediately following our example above, the same key is pressed, the current will enter the right-hand wheel at B and not A, and will pursue an entirely different course. Once in every 26 positions, the right hand wheel moves the middle wheel over one so that when the right hand wheel returns to position

Enigma

- There were also a plug board (to change the meanings of the letters) akin to one time pads, plus other similar features on the rims.
- Rotors chosen from collections.
- 3 rotor (airforce), 4 rotor (naval), 12 rotor (high level Lorentz="tunny").
- Also protocol books, books for key setting in paper that the ink would dissolve from, etc.
- If you want a seminar on how these things worked try `https://www.youtube.com/watch?v=mcX7iO_XCFA`, for an early 3 rotor one.
- Germans had absolute faith in the unbreakability of Enigma.
- Maybe 100 years from now, they'll be saying this about modern public key encryption.....!

- Back in GCHQ Hugh Foss demonstrated how commercial Enigma was vulnerable, and then Dilly Knox gave methods to break.
- Based around flawed protocol. Repetition of initial setting.
- Used for Spanish Civil War for messages between Hitler and Franco *a*.
- Broken in 1937 using Knox methods and "Jeffries' Sheets".

Poland

- The German military modified Enigma and these methods no longer worked. Elizabeth Rakus-Anderson (The Polish brains behind the breaking of Enigma):

  > *Cryptologists could easily recognize an Enigma cipher by its perfect spread of letters. There was no correlation with natural letters and statistical calculations based on frequencies of letters were completely useless.*

- Strictly speaking, this is not quite true as we later see.
- Work was done in Poland. (1929) Lecturer presents authentic Reichswehr ciphergrams for students to solve and recruits those who did. Marian Rejewski, Henryk Zygalski and Jerzy Różycki.
- Used mathematics (specifically group theory) for trying to solve military Enigma, reliant on dumb wiring of Keyboard to Rotor 1, and a flawed protocol.
- Zygalski sheets then
- Invented the Bombe which is kind of an Enigma machine reverse engineered

Two gifts to the Allies

- 1939, Poles reveal the method they use to solve the current version of Enigma.
- Give two current Enigma machines which were delivered by the Poles to the British in diplomatic luggage.
- Also a hidden message:

  Iain Lobban: The Poles had taken a different route and had recruited mathematicians rather than classicists to become cryptanalysts....It was this information which crystallized the crucial insight by Alasdair Denniston, ...the forthcoming war.. needed a new sort of cryptanalyst to complement the existing staff.... first names ...Alan Turing, Gordon Welchman and Max Newman.

- All this begun in 1939.
- 1939-1940 Turing worked with Knox and the Poles.
- Turing requests to tackle the (most complex) Naval Enigma.

Breaking Enigmas

- This was the work of 10,000 people, and there were differing Enigmas.
- All broken because of operator errors, chance discoveries, lost Enigma machines, code books, etc. data mining!
- Mainly "cribs" Postulates about the underlying plaintexts, e.g. German obsceneties, Heil Hitler, Good Morning, To and ending with a from, etc. Accurate because of the vast amount of work studying communication traffic.
- Hut 6 breaks Airforce Enigma using the Herival Tip.
- Part of the Airforce protocol was to set the rings in the rotors (from a book), and the move the rotors to a random position. (Like a keyless lock for a bike.) Operators were lazy.
- Part of the protocol was to send each day a 3 letter random string for the settings. Some operators would always set (things like) HIT LER, perhaps encoded. Someone always sent to first 3 letters of his name and that of his girlfriend.
- Bear in mind that this was a continuous contest between codebreakers and codemakers; the Germans changing things all the

- For example, sometimes false messages were sent. Once they received a false message containing no L's.
- Guess that the lazy operator was having a smoke and pressed L without taking the finger off.
- Why? A flaw in Enigma is that no letter repeats.
- Guess a longish crib. Try to match up. If any letter matches it is wrong
- For example *ABBACTARMDVSSWT* guess *BOBO*
- One of the key ideas: Eliminate what is not possible.
- Similar Welchman's idea of exploiting the symmetry: if $A \to N$ then $N \to A$.

Turing at Bletchley

- Mainly in Hut 8 on the difficult Naval Enigma and later Lorentz.
- Realized that the Germans were using bigrams. (one letter to 2)
- Many technical and fundamental contributions.

Iain Lobban (director GCHQ, 2012)

> *Turing's way was to take other people's ideas, develop and build on them, and pass the product on to other people to be the foundation for the next stage. He took the idea of the electromechanical processing of the Poles but developed their idea into something radically different. When Welchman later enhanced the Bombe with a diagonal board, Turing was the first to congratulate him on his major improvement. Turing was part of the team, shared in the success of the team.*

Turing at Bletchley

Hugh Alexander (History of Naval Enigma)

> *There should be no question in anyone's mind that Turing's work was the biggest factor in Hut 8's success. In the early days he was the only cryptographer who thought the problem worth tackling and not only was he primarily responsible for the main theoretical work within the hut but also shared with Welchman and Keen the chief credit for the invention of the Bombe. It is always difficult to say that anyone is absolutely indispensable but if anyone was indispensable to Hut 8 it was Turing. ....many of us in Hut 8 felt that the magnitude of Turing's work was never fully realised by the outside world.*

The Imitation Game

- I was so annoyed that I am prejudiced. Its veracity is along the lines of Braveheart, but better than Rambo II.
- (The most appalling) Turing working with Cairncross and being blackmailed. They worked in different parts of Bletchley, and apparently never met.

  > *(Alex von Tunzelmann-Historian) The wartime codebreaker and computing genius was pursued for homosexuality, but nobody, until film-makers came along, accused him of being a traitor*

- MI6 head Menzies interacting with Turing and knowing about Cairncross. No evidence at all.
- 4 people in Hut 8 doing everything, what did the other 9,996 do? Why do Hollywood movies always have the world saved by one or two people? (At least they weren't re-written as American.)
- Turing doing the work on the Bombe which is disturbingly called Christopher.

- The horrendous mixing of the universal TM and the Bombe.
- Everyone except Turing and Joan Clarke seems stupid.
- The decision of how to use Ultra decriptions was determined by Hut 8. This is obviously nonsense. (It did indicate the use of mathematics in decision making.)
- Peter Hilton had no brother on a fleet.
- Denniston was a good guy had no conflict with Turing. In fact it was he who recruited Turing and even set up Bletchley.
- Joan Clark did not do the crossword test. She was recruited.
- Turing's most cited work (as per 2012) is in biology, which he did whilst being "treated" for homosexuality. He had no loss of intellectual power due to his "treatment" and it had finished 9 months before his death.

- Joan Clark did not visit him post Bletchley.
- The implication that there was one break and then all was simple.
- The implication that all the materials were destroyed after the war. There were many many bombes (200) including the much faster US based ones. (But not Colossus) Churchill (and presumably the Americans) kept much of the materials secret, but destroyed the material at Bletchley. Also, after the end of World War II, the Allies sold captured Enigma machines, still widely considered secure, to developing countries.
- Turing was unpopular. Apparently he was quite social if a bit eccentric, with quite a sense of humour and a raucous laugh; but did not suffer fools. Was shy with women.
- The security at Bletchley was lax... very far from this.
- The Churchill letter. There was a letter but it was asking for more resources particularly Wrens, and was by many people including Turing.
- The silly subplot with the detective, and his apparent belief in Turing being a Russian spy.
- There are many more.

- For some see `http://www.historyvshollywood.com/reelfaces/imitation-game/`

  Alex von Tunzelmann

  > *Historically, The Imitation Game is as much of a garbled mess as a heap of unbroken code. For its appalling suggestion that Alan Turing might have covered up for a Soviet spy, it must be sent straight to the bottom of the class.*

- also `http://www.nybooks.com/blogs/nyrblog/2014/dec/19/poor-imitation-alan-turing/` A Poor Imitation of Turing-Christian Caryl

  > *.... either you embrace the richness of Turing as a character and trust the audience to follow you there, or you simply capitulate, by reducing him to a caricature of the tortured genius. ... In their version, Turing (played by Benedict Cumberbatch) conforms to the familiar stereotype of the otherworldly nerd: he's the kind of guy who doesn't even understand an invitation to lunch*
  >
  > *—- To be honest, I'm a bit surprised that there hasn't been more pushback against The Imitation Game by intelligence professionals, historians, and survivors of Turing's circle. But I think I understand why. After so many years in which Turing failed to get his due, no one wants to be seen as spoiling the party.*

There are some examples of this last point. Jack Copeland (Noted NZ based Turing Scholar, from Canterbury)

> *It gets the crucial outlines of the story right, correctly saying for example that it was Turing who invented the fundamental logical principles of the modern computer (actually a point seldom acknowledged in the history books). The movie brings out the mammoth importance of Bletchley Park's attack on the German Naval ciphers, an incredible operation that helped save possibly as many as 7 million or more lives. And it correctly places Turing at the center of this.*

As you see I disagree, but see `http://www.huffingtonpost.com/jack-copeland/oscars-for-the-imitation-_b_6635654.html?utm_hp_ref=entertainment&ir=Entertainment`

Colossus

- Towards the end of the war, allies began to recieve a strange new code, they called tunny.
- This turned out to be the highest level code and was based on a 12 rotor version of Enigma.
- This fact was deduced by Bill Tutte based purely on the messages received, amazingly.
- It was realized that too hard to solve even with mechanical mega-bombe.
- Tommy Flowers gave a plan for a large scale valve computer.
- Experts claimed it impossible (lots of social comment here).
- Turns up with one 9 months later! 2,400 valves.
- Flowers' work never really celebrated in his lifetime.

Other work of Turing

- Conceptual basis of modern computers.
- Lots of technical work in logic.
- Proofs of equivalence of the models of computation. (JSL papers)
- Undecidability of other systems.
- Work in number theory.
- Proposed methods for symbolic verification of programs. Symbolic verification has grown into modern model checking, though not really using Turing's ideas.
- Proposed methods of logically constructing programs.
- First computer chess program (1950). See the webcast of Kasparov's talk in Manchester, Turing 100 conference.

Model checking

- The world is full of hardware and algorithmic processes.
- It is good to know that they don't have catastrophic failures.
- Turing proposed methods for symbolic verification of programs. This has grown into modern model checking.-logic again
- Idea : represent processes by symbols, and have a transition "calculus" and then verify by calculation.
- Began with things like Hoare logic ("logic is the calculus of computer science").
- Modern life would be impossible without it. It is very bad if any of the embedded hardware in e.g. a plane fails.
- Works well for hardware, still in development for software.
- Can be applied to e.g. industrial processes.

Machine Intelligence

- Famous unpublished paper on this from a sabbatical at Cambridge.
- His boss (Charles Darwin) thought it was a "schoolboy paper". Would not let it be published. Now it is regarded as a classic.
- Later famously posed the Turing Test.
- Often mis-quoted as saying machine intelligence by the end of the 20th century. Actual quote (from a radio discussion with Max Newmann) "at least 100 years."
- Emphasized optimization as a key strategy for artificial intelligence, and realized in his chess program.

Machine learning

- Huge numbers of things are now modeled by machine learning.
- Huge databases exist and are being “mined”.
- Modern life would be impossible without it. Modern medicine, weather prediction, Internet, DNA analysis, evolution of things like language, etc
- Uses optimization, statistics combinatorics etc.
- Currently one of the most important areas of research in CS.
- We have shown that expert systems are readily modelable, Watson, etc. This the future of many things in e.g. medicine.

Some Other Things Left Out

- "Rounding-off Errors in Matrix Processes" Ill-posed problems and "the other" theory of computation.
- He was the first to properly study complexity of matrix algorithms like determinant computations when dividing by near zero quantities.
- This was centered in numerical analysis
- Morphogenesis: How do leopards get their spots?
- Suggests a simple mechanism based on partial differential equations.
- 20 years(!) before experimental verification.
- diffusion/reaction equations.
- Basically stable, but under perturbation creates a feedback loop.

Partial differential equations

- These are equations which model continuous processes
- Modern life would be impossible without it.
- E.g. Any scanning device, any modeling in physics, modeling continuous industrial processes, computer graphics (e.g. Avatar etc), electronics, materials science, etc.

Summary

- One of the single most important papers of the 20th century was written by Turing who provided a conceptual basis for what are now computers.
- This came from an (apparently) obscure problem in logic. Would a granting agency have supported it I wonder?
- Currently one of the most important problems in all of science is an apparently obscure problem in logic. In Japan, there is a multi-million dollar grant to try to solve it.
- Codes were broken by mathematics and Turing was a leader.
- Lessons for us: Science has become intensely mathematical, and computers ever more ubiquitous. Now is the age of mathematics and computing.

Viewing

- I will post these notes to my home page and you can follow up.
- Excellent videos related to Turing and Bletchley.
- Most excellent Horizon programme, with interviews with Hodges, Gandy, Joan Clark etc. (Only slightly annoying in its reference to only Turing solving the decision problem.)
  `https://m.youtube.com/watch?v=gyusnGbBSHE`
- Episode 2 of 4 The Goose That Laid the Golden Eggs (Churchill's comment)
  It is a 1990s Channel 4 production. A number of cryptanalysts of Bletchley park and women who worked there are interviewed (some of whom interacted with Turing) and even some German operators of the enigma machines.
  `https://www.youtube.com/watch?v=_jgiywQrAzc`
  Episode 3 of 4 - The Ultra Secret
  `https://www.youtube.com/watch?v=xjM7bJNAITo`

- Episode 4 of 4 - The War of the Machines `https://www.youtube.com/watch?v=J4MBwIl4Ybo` Very interesting, especially the Wren point of view. Unfortunately confuses programmable computer with large scale computer. Interview with Tommy Flowers. Interesting social commentary about Winterbotham's leaking of Ultra 30 years on and commentary about "special" cyber relationships between the UK and the US.

- Turing's cathedral. Lecture by George Dyson about Los Alamos, von Neumann, development of computers. Very American-centric, and a bit slow if you don't know much about computers. Implicit commentary on the involvement of the military with the development of science.
  `http://m.youtube.com/watch?v=stSm1cvwn00`
- Uncovering Colossus-Prof. Brian Randall (somewhat technical) "Colossus, the world's first electronic computer, was built during World War II, but kept secret for more than 30 years. Professor Brian Randell tells the story about how he stumbled across a reference to its existence and eventually led to the UK government lifting the veil of secrecy surrounding this pioneering computer in 1975. Prof Brian Randell's presentation was given in the new Colossus Gallery in The National Museum of Computing on 7 February 2013. "
  `https://www.youtube.com/watch?v=Yl6pK1Z7B5Q`

Some Books

- Alan Turing: The Enigma ... Hodges.
- Many books by Jack Copeland, either as author or editor. For example.
  1. The Essential Turing (as editor, many articles by professional historians)
  2. Alan Turing's Electronic Brain (as editor, many articles about ACE and development of computers)
  3. Turing : Pioneer of the Information Age
  4. (Not really a book but good for those who don't want to pay) Copeland-Proudfoot article in the online Rutherford Journal `http://www.rutherfordjournal.org/article040101.html`
- Alan Turing: Life and Legacy of a great thinker. Christof Teutscher (ed)
- Turing's Legacy, Rod Downey editor, concentrates on developments stemming from Turing's work in logic.
- (not a book but a play) Breaking the Code -Hugh Whitemore.

Forbidden Fruit

Thank You