Historical Note

ALAN TURING: A NOTE ON HIS ROLE AS WORLD WAR II CRYPTANALYST

***Rahat Afreen**
**Department of MCA, Millenium Institute of Management,*
Dr. RafiqZakariaCampus,Aurangabad, Maharashtra
**Author for Correspondence*

ABSTRACT

Alan Mathison Turing is well known to the world of computer for the concept of Turing Machine- A conceptual machine presented by him which proves that automatic computation cannot solve all mathematical problems – also called as Halting Problem of Turing Machine. He was attributed as the founder of Computer Science. But, until late 20th century, his contributions in the field of Number Theory, Cryptography, Artificial Intelligence and more importantly how his ideas protected England in the times of world war II were unknown.

Key Words: *Alan Turing, Enigma, Bombe, Colossus, Tunny, ACE*

INTRODUCTION

Alan Turing was born on 23rd June 1912 in Paddington, London. His father Julius Mathison Turing worked for Indian Civil Services at Orrisa for British government in India. But he and his wife decided to keep their children back in England for education. He got his education from Sherbrone School, Sherbrone and did his higher education from King's College Cambridge where he later became a fellow. He had an interest in the field of mathematics and presented numerous papers on famous problems of mathematics. At the age of 24 Turing wrote a paper entitled "On Computable Numbers, with an Application to the Entscheidungs problem". Turing (2005) this paper basically gave an elegant way to model a computer from mathematical concepts. It is in this paper that he proposed the concept of a virtual machine that we today call as Turing machine. This was a breakthrough, because it allowed the tools of mathematics to be brought to bear on questions of computation. Turing's paper is more remarkable because he wrote it in 1936, a full decade before any computer actually existed. The word "Entscheidungs problem" in the title refers to one of the 28 mathematical problems posed by David Hilbert in 1928 as challenges to mathematicians of the 20th century. Turing justified that there is no solution to Entscheidungs problem.

World War II Contribution

In the Decade of late 1930's the world was foreseeing the shadows of World War II. During these sensitive times, Turing realizes that preserving military secrets will be of utmost important. He proposed the use of Number Theory to encrypt military related communication. During those times, various countries were already using cryptography to encrypt army related communications. But these techniques were simple substitution cipher type techniques. Here alphabets of a language forming some message are moved forward and/or backward in such a way that same input alphabet will give different output alphabet each time, but in a fixed pattern. The pattern is reversed for those who are authorized to receive and decode the message so that they can retrieve original message from encrypted text. This was done mechanically. The most obvious example is the Enigma machine designed by Germans. Let us go through a short overview of Enigma as Turing and Enigma are very closely related. This machine was similar to typewriter, but without paper and with an illuminated output panel consisting of 26 German alphabets to show encrypted letters one by one. The concept was to provide multiple rotating wheels inside containing 26 alphabets on each of their two surfaces. Whenever any alphabet is punched from keyboard, these set of wheels rotate forming a different pattern every time and changing the path of flow of current. Then the current flows in reverse direction but via a different path. This gives a different output alphabet for same input each time. At the beginning, there were in total five wheels and any three of them were selected for each time. Also, the Enigma used by German Air Forces had eight wheels and five of them are selected for one setting. These wheels were connected to each other using spring loaded connections. There were also further complex settings provided in the form of Stecker Board which has 26 two way sockets representing German alphabets. This Stecker Board gives the machine operator an option to directly couple any two alphabets. The pairs of alphabets which are connected in such way are called steckered where as rest are called unsteckered. So, in choosing a basic set-up for the machine, there was a choice from the 60 possible wheel orders, 17, 576 ring-settings for each wheel order and 159 million million million daily possible settings of stecker board. The output is shown by glowing the alphabet on output panel. The general procedure was to key in the message letter by letter and note down he output letters from output panel. Then the message was transferred using any available communication medium. Germans used Morse codes on radio Carter (2010), Ellsbury (1998). Such method of secret communication where text is scrambles to make non understandable code has its origin dated back to the times of Julius Caesar. Schneier (2008) various other countries like Japan also had similar encryption machines for war time communications **'**Japanese Cryptographic' Machines.

Now what Turing proposed was a totally different concept. His idea was to translate the text into mathematical form and do mathematical calculations on them. This concept is based on the fact that there are certain groups of operations in mathematics which are hard to reverse. For example exponentiation vs. logarithm. It is easy to calculate $X^y = Z$, but difficult and time consuming to get exact value of $log_X Z=y$. Turing proposed use of prime numbers as the prime number multiplication and factorization problems bear same property. Today, number theory and use of prime numbers is the basis for numerous public key cryptosystems, digital signature schemes, cryptographic hash functions, and digital cash systems. Whenever we do net banking, order something on Flipcart, appear for an online technical certification exam, a number theoretic algorithm is there to protect sensitive data.

Below is an explanation of Turing's Idea; first, translate a text message into an integer so we can perform mathematical operations on it. This step must not make a message harder to read. One approach can be-replace each letter of the message with two digits (A = 01, B = 02, C = 03, etc.) and string all the digits together to form one huge number. For example, Devadas and Lehman (2005) the message "victory" could be translated as:

"V I C T O R Y"→ 22 09 03 20 15 18 25

Turing's code requires the message to be a prime number, so we may need to pad the result with a few more digits to make a prime. In this case, appending the digits 13 gives the number $22090320151825\underline{13}$, which is a prime.

Now here is how the encryption process works.

Assume:

m is the un-encrypted message (which we want to keep secret and yet send out to some of our friend),

m' is the encrypted message and

k is the key.

Before sending any secret messages the sender and receiver agree on a secret key, which is a large prime number **k**.

Encryption: The sender encrypts the message m by computing:

m'= m · k

So, the message is a prime number and key is a prime number. When you multiply two primes you get some integer value.

Decryption: The receiver decrypts m' by computing:

m= m'/k

So, that is a simple division.

Historical Note

For example, suppose that the secret key is the prime number k = 22801763489 and the message m is “victory”. Then the encrypted message is:
m’= m · k
= 2209032015182513 · 22801763489
= 50369825549820718594667857
On the receiving end, it will be decrypted by dividing the message by the key **k**.
Here the secrecy is achieved by the mathematical property of prime factorization. Given a number Z which is the product of exactly two very large prime numbers, X, Y it is a mathematically ‘Hard’ problem to factorize Z to find out X and Y. the difficulty increases with the size of numbers. Lutus (2008) Thus, without proper key, what is visible to intruder; in this case German Army is the encrypted message = **m** · **k**, which is meaningless. Longer the key size more secure the system will be. Recovering the original message **m** requires factoring **m’**. Despite immense efforts, no really efficient factoring algorithm has ever been found. Only Number Field Sieve is available Pomerance and Carl (1996) which has a considerably large computing time. Here, Turing used his own discovery that there exist problems that no computer can solve.
But this technique has a major flaw; the same key must not be reused. Consider the below example;
If the same key is used to send two different messages m_1^* and m_2^*, then two encrypted messages will be:

$$m_1^* = m_1.k \qquad \text{And} \qquad m_2^* = m_2.k$$

The greatest common divisor of the two encrypted messages, m_1^* and m_2^*, is the secret key k. And, there are a lot of easy methods to compute the GCD of ‘two’ numbers efficiently. So after the second message is sent, the intruder can recover the secret key and read every Message. . But Turing’s Code remains unbreakable because, the actual technique used by him was much secure and based on Modular Arithmetic, which uses a subset of numbers which are ‘Relatively Prime’. Today, the famous public key algorithm RSA also uses the same concept. Rivest *et al.,* (1978).

The Bombe

Soon after devising his code, Turing disappeared from public view, and decades passed before the world learned of his whereabouts and achievements. He was officially working at the Government Code and Cypher School at Bletchley Park, England. The contribution of Allen Turing to Britain Army’s Secret Communication System is the reason why Britain remains undefeated despite of several attacks by Germans. Based on Turing’s suggestions, British Army has designed a machine called Bombe which was capable of breaking the encrypted messages generated by German Enigma. Below is the comparative description of Bombe vs. Enigma;
While Enigma was similar to a typewriter, Bombe was housed in a cabinet of 7’ X 6’ X 6’2” size. Enigma has at least five or more rotors and Bombe has at an average 108 drums mounted on shafts arranged in three 12X3 arrays. Enigma rotors were placed one after another in a sequence, each having 26 contacts representing German Alphabets. Drums of Bombe have four concentric circles each with 26 contacts to represent German Alphabets. So there are 104 electrical contacts in each Bombe drum. The outer fourth circle resembles Stecker board of Enigma. Bombe was capable of analyzing cipher text messages of Enigma to find out daily settings of rotors and some of the steckers. Bombe was capable of behaving like 108 Enigma machines working at once, thus finding possible Enigma settings at higher speed. Thus, Bombe was a kind of task oriented computing machine designed to do multiprocessing-a term which is even today coupled with advanced computer science disciplines. Turing’s further contributions for Bombe were cryptanalytical techniques he proposed to analyze ciphertext to retrieve original message or plaintext. In simple terms, Turing gave the algorithm on which Bombe operated. Three methods of analysis were suggested called as ciphertext only attack, discriminant attack and probable phrase attack. Out of these three, the last one, that is, probable phrase attack was used to design Bombe and proved successful. In this technique a ciphertext is matched against a known or guessed portion of plaintext. This has become possible because of many mistakes done in German communication. First mistake was some

of the encrypted communication was about weather and same messages were forecasted by German weather boats. Now, Allies have same text in original and encrypted format, so Turing worked out to find the relationship between them. Also, German army communication used to begin and end in a fixed pattern like we do in letter writing, these patterns were well known to British experts and they took an advantage of it. Some settings of Enigma were also not changed frequently, resulting into fixed patterns of wheel/stecker orders and become helpful in cryptanalysis.

Thus, Turing's major contribution was in developing computers to assist in breaking codes of German army. The critical reason behind Germany's loss was made public only in 1974: the British had broken Germany's naval code, Enigma. Through much of the war, the Allies (countries fighting against Germany and their friend countries) were able to route convoys Barratt (2002) around German submarines. This helped them to listening into German communications. These communications were captured and sent back to Bletchley Park, Hut-8, where Turing and his team will do "cryptanalysis" of the message. The original messages recovered by them helped the British Army to make certain major decisions which played a key role in bringing World War II to an end. The British government didn't explain how Enigma was broken until 1996. When the analysis was finally released (by the US), the author was none other than Alan Turing.

He also helped in the designing of the computer called COLOSSUS in 1934. Every aspect of it was also kept secret by British Government. COLOSSUS was designed to break German telegraphy based encryption machine Tunny. Tunny was a type of teleprinter used to send and receive encrypted Morse Codes. It is based on Enigma and has 12 encryption wheels. The British engineer Thomas H. Flowers designed COLOSSUS. He was an assistant of Turing in Bletchley Park. Later in 1942, Turing helped him by providing cryptanalytical methods to support COLOSSUS. These methods are known as 'Turingery'. Turingery For post World War II some refer COLOSSUS as dead end- being practically of no use but some refer it as one of the first embedded computers-a domain specific computer designed for one dedicated task. After working on Bombe and COLOSSUS, Turing was convinced that a general computing machine can be designed. So, in 1946 he presented a theoretical design for Automatic Computing Engine (ACE). But, Turing was not able to convince his colleagues that this design can actually be implemented in electronics as Bombe and COLOSSUS were still strictly war time secrets. So he has to compromise on designing a smaller version of actual presented design known as Pilot Model ACE. Rather, Von Neumann's design of EDVAC presented in 1947 got much publicity. But the fact was that Von Neumann was also inspired by Turing's ideas.

After knowing the actual history, experts in the field of computers comment that history of computer needed to be rewritten not only by attributing Alan Turing for his work but also considering the fact that Domain Specific Computers arrive earlier than General Purpose Computers.

DEATH AND CENTENARY

Turing Died at the early age of 41. A half eaten apple infected with potassium cyanide was found beside him. Whether his death is a suicide or an accident or a murder is still a topic of argument. There are various facts that contrast each other like; he was doing experiment on potassium cyanide. His mother was of catholic belief and strictly opposed that his son committed suicide. She considered it as an accident. But, Turing always used to recite couplets from "*Snow White and the Seven Dwarfs*" which are,

"Dip the apple in the brew,
Let the sleeping death seep through".

He has also confessed being involved into "gross indecency" which was a punishable act in those days in England. As a punishment, he was sentenced to be treated with female hormones which not only developed female characteristics into him but also slowed his mind. This is widely considered as an obvious cause for him to attempt for suicide. But the punishment was stopped a year before his death. He showed no signs of attempting suicide as he has prepared a list of tasks to be completed at the weekend.

Historical Note

His knowledge on war time military communication and knowing exactly how the entire system works was also considered a threat for his life. There are a lot of such twisting facts.

In the year September 2009 then-British Prime Minister Gordon Brown issues posthumous apology for the way Turing was treated. Porter (2009*)* He said, "*I'm proud to say sorry to a real war hero* " Brown (2009)

The year 2012 was celebrated as a Turing Centenary year marking his 100th birthday. Numerous events were organized to offer respect and tribute to the great mathematician. Apart from various conferences, the events include exibition at London Science Museum from May 21st to May 31st with a display of Turing's Pilot ACE computer 'Math In The News', release of Turing's war time work to public access Brown M (2012) an also some events in India 'Alan Turing Centenary Year Celebration @ CSE IITK'. Various respected scientist like Stephen Hawking and others are still supporting the demand that Turing should be legally pardoned Rosen (2012). An e-petition in this regard has also been filed Jones (2012), but it is not considered by British Government yet.

These bitter facts belonging to Turing fail to overshadow his contributions to the modern era of computing and its various disciplines which are still raw and to be explored.

ACKNOWLEDGEMENT

My sincere thanks to Dr. S.C. Mehrotra, My Ph. D Guide, whose guidance always encourages me to explore new aspects of research and study.

REFERENCES

Alan Turing Centenary Year Celebration @ CSE IITK. *Alan Turing Centenary Year Celebration Program* [online] Available: http://www2.cse.iitk.ac.in/~csemeet/turing/program.php [Accessed 12 February 2013].

Barratt J (2002). *Military History Online- The Convoy System – Origins* [Online] Available: www.militaryhistoryonline.com/wwii/atlantic/convoy.aspx [Accessed December 2012].

Brown G (2009). *Gordon Brown: I'm proud to say sorry to a real war hero* [Online] Available: Telegraph Media Group Limited Available: http://www.telegraph.co.uk/news/politics/gordon-brown/6170112/Gordon-Brown-Im-proud-to-say-sorry-to-a-real-war-hero.html [Accessed 12 February 2013].

Brown M (2012). *GCHQ releases Alan Turing's secret wartime papers (Wired UK)*
[Online] Available: http://www.wired.co.uk/news/archive/2012-04/20/turing-papers [Accessed 8 December 2012].

Carter F (2010). "*The Turing Bombe*", The Rutherford Journal- *The New Zealand journal for the history and philosophy of science and technology* ISSN 1177-1380 [Online]
Available: http://www.rutherfordjournal.org/article030108.html [accessed December 2012].

Devdas S and Lehman E (2005). *Number Theory* Lecture Notes, Mathematics for computer science 6.042/18.062j.

Ellsbury G (1998). *The enigma and the Bombe* [online]
Available: http://www.ellsbury.com/enigmabombe.htm [Accessed December 2012].

Japanese Cryptographic Machines (No Year). *Bletchley Park Jewls Japanese Cryptographic Machines* [Online] Available: http://www.mkheritage.co.uk/bpt/japcdsch2.html [Accessed 14 February 2013].

Jones W (2012). HM Government-*Grant A Pardon to Alan Turing* [online] Available: epetitions.direct.gov.uk/petitions/23526 [Accessed December 2012].

Lutus P (2008). *PrimeNumbers Exploring a Unique Class of Numbers* [online] Available: http://arachnoid.com/prime_numbers/index.html [accessed 14 February 2013].

Math in the News. *Science Museum Celebrates Turing Centenary with Pilot ACE* [online] Available: http://mathdl.maa.org/mathDL/?pa=mathNews&sa=view&newsId=1328 [Accessed 12 February 2013].

Pomerance, Carl (December 1996). "*A Tale of Two Sieves*". Notices of the AMS **43**(12) 1473-1485. [Online] Available:http://www.ams.org/notices/199612/pomerance.pdf [Accessed 2006].

Porter A (11 September 2009*).* *Gordon Brown issues posthumous apology to Bletchley Park codebreaker* [online] Telegraph Media Group Limited Available: http://www.telegraph.co.uk/news/uknews/6170089/Gordon-Brown-issues-posthumous-apology-to-Bletchley-Park-codebreaker.html [Accessed February 13 2013].

Rivest, R, Shamir A, Adleman L (February 1978). *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*" Communications of the ACM **21**(2) 120-126.

Rosen RJ (18 Dec 2012). *Stephen Hawking Calls for Alan Turing's Pardon- Rebecca J Rosen- the Atlantic* [online] Available: http://www.theatlantic.com/technology/archive/2012/12/stephen-hawking-calls-for-alan-turings-pardon/266438/ [Accesses 13 February 2013].

Schneier B (2008). "*Applied Cryptography Protocols, Algorithms and Source Code in C*", Second Edition, Wiley- India Edition.

Turing AM (1936). *On Computable Numbers, with an Application to the Entscheidungs problem* Proceedings of the London Mathematical Society, Series **2**(42) 230-265 [online] Available: http://www.abelard.org/turpap2/turpap2.htm[Accessed December 2012].

Turingery. Turingery-PoolParty Linked Data Server – Taxonomies, Thesauri, vocabularies [online] Available:http://www.w3.org/2004/02/skos/core#definition [Accessed 14 February 2013].