# THE FINE LINE BETWEEN CRYPTOLOGY AND MACHINE TRANSLATION

**AYDAN SALMANOVA**
Baku Engineering University
Pedagogy/Translation
*nadyasalman210@gmail.com*
BAKU, AZERBAIJAN

## ABSTRACT

Today, most of us write in manners that we cannot peruse or ever would like to fathom; of course, composting is transposed into indescribable, encoded passages of "secure" data. However, on this research paper, I would like to touch upon the history of machine translation, indicating how its sources are to be found in the development of cryptanalysis or code cracking. Everything is starting with the letter of theologian, philosopher, and mathematician Marin Mersenne and René Descartes about creating an artificial universal language for making translation among the languages. Then these histories discover their epitome in Warren Weaver's persuasive memorandum. In this memorandum, Weaver built up a "cryptographic and translation" thought, drawing on his insight into the Second World War code cracking to dispatch the cutting edge field of machine translation. Anxious to discover new uses for the decryption strategies created amid WWII to decipher the Enigma code and Weaver suggested that cryptographic procedures be connected to the errand of translation.

**KEY WORDS: translatıon, cryptology, machıne translation**

## INTRODUCTION

The rapid developments in technology have affected almost every area and offered new opportunities and facilities. It's possible to see the impact of technology from the economy to health, from architecture to defense industry, from art to sport and so forth. Innovative advances have prompted extraordinary changes in translation as a method for interlingual correspondence. On the one hand, translation scientists and translators in an attempt to benefit from the advantages provided by technology and on the other hand, try to apply all these innovations to their own fields.

Nowadays, when we throw a glance to the possibilities offered by the technological developments in the translation field, we can see many software and ancillary resources have been brought into service from translation tools to translation memory, from word counters to convention applications, from content research tools to social media applications and all these innovations are based on computers and internet technologies.

Technological advances provide translators with a lot of opportunities. If we list some of them, making fast and consistent translation may take first place on the list. It gives translators a hand to shorten the project duration and save the translators' time, get more projects and earn higher revenue. Likewise, these technologies have increased productivity and quality in translation, supported international communication, and demonstrated the growing need for innovative technological solutions to the age-old problem of the language barrier. (5)

## METHOD OF RESEARCH

I have searched the archeology of the machine translation and crypto and cipher machines that existed during the Second World War in order to determine the connection between translation and cryptology on this research paper.

So, have you ever thought about the history of machine translation and have you ever known that the history of machine translation is related to cryptology? Let's make a journey into the history of machine translation.

Although the first systems of MT were built on the first computers in the years right after World War II, the history of MT does not begin, as often stated, in the 1940s, but some hundred years ago.(8,1) In order to judge current developments in MT properly, it is important to understand the historical development.(8,1)

In a letter dated 1629 to theologian, philosopher, and mathematician Marin Mersenne, philosopher, mathematician and physicist René Descartes proposed an artificial universal language, with equivalent ideas in different tongues sharing one symbol and mentioned a dictionary to translate among the languages.(6) Although this proposal was not taken into consideration, Descartes was known as the founder of the initial idea about MT. The three centuries after Descartes, the first attempts in machine translation was started in the 1930s. There have been other such proposals, but first definite legitimate forerunners of MT are contained in the two patents applied for simultaneously in 1933, in France and Russia.(2,2) In both cases, the patents were for electromechanical devices capable of being used as a translation dictionary.(2,2) Then, the patent granted to Georges Artsrouni on 22 July 1933 was for what he called a 'mechanical brain' ( cerveaui méchanique), a general-purpose device with many potential applications.(2,2) During the years of the Second World War, parties made intense efforts to obtain confidential information belonging to each other. For this purpose, they invented various crypto decoding machines. Now it's interesting to you that " what is the cryptography or encryption or decryption?" I will give you short information about them for understanding better the rest of the text. Cryptography is the investigation of strategies used to impart and store data safely without being blocked or available by outsiders. Cryptography is an expansive field with applications in numerous basic aspects of our lives. Cryptology is the study of cryptography and cryptanalysis.(4,2) However, cryptography and cryptanalysis are ontologically different from each other. Cryptography is made up of encryption and decryption. Encryption of a message means the information in it is hidden so that anyone who's reading or listening to the message, can't understand any of it unless he/she can break the encryption.(3,6) Nevertheless, decoding is the way toward taking encoded or scrambled content or other information and changing over it once again into content that you or the PC can peruse and get it. Cryptanalysis, on the other hand, is the investigation of ciphertext, figures, and cryptosystems with the point of seeing how they work and finding and improving methods for crushing or debilitating them. In the early 1930s, the German military adopted a new encryption protocol based on an existing commercial, diplomatic, and military device called Enigma(11,1) and it was the most famous one. An Enigma machine allowed for billions and billions of ways to encode a message, making it incredibly difficult for other nations to crack German codes during the war — for a time the code seemed unbreakable.(10) The security of the Enigma cipher was dependent on the secrecy of the initial set up of the machine.(12) There were 3 rotors chosen of a possible 5 and each rotor had 26 possible starting positions and given that there are 3 rotors chosen of 5 and their ordering matters this lead to 60 possible rotor setups.(12) Further, each rotor was set to a starting position out of the 26 letters giving a possible 26x26x26= 17,576 message keys.(12) This ultimately led to a possible $17576 \times 60 = 1{,}054{,}560$ initial rotor setups.(12) Likewise, in World War II, the decipherment of the German Enigma code is regarded as a crucial point.(12) The British group around Alan Turing, situated in Bletchley Park, was in charge of this dire undertaking and accomplished the breaking of the code by methods for measurable strategies that were prepared on registering machines. Without their insight, the researchers established the frameworks for pragmatic MT.

What's more, those histories then find their epitome in Warren Weaver's persuasive "Translation" memorandum. He started this work around 200 of his colleagues, many of whom had been engaged during the Second World War on cryptographical work in July 1949. Then he prepared a report and proposed a translation method. Moreover, he outlined the prospects and suggested various methods; the use of war-time cryptography techniques, statistical methods, Shannon's information theory, and the exploration of the underlying logic and universal features of languages, "the common base of human communication".(9,4) Together, these chronicles uncover a portion of the manners in which that different hardware was created to "break" obscure content, be it an unknown dialect or ciphertext. All things considered, this history additionally indicates a more profound, ontological connection among language and cryptology. Furthermore, Warren Weaver found information about war-time that determining the source language of an intercepted message than cryptanalysing it took a long time of American cryptanalysts. According to these two facts, Weaver comprehended that language was

extremely a "code",(15,13) and just expected to make sense of the way toward interpreting and recoding for deciphering something from one language into another. Therewithal, Warren Weaver was impressed by Germany's use of the pioneering Colossus computers to solve the military codes produced by mysterious cryptographic machines, which constitute the concept of machine translation. That's why Warren Weaver said:

"I have a text in front of me which is written in Russian but I am going to pretend that it is really written in English and that it has been coded into some strange symbols. All I need to do is to strip off the code in order to retrieve the information contained in the text."(7,1)

Weaver likewise realized that from the two wars ground-breaking new devices for cryptanalysis were accessible, for instance, as the effective "Bombe," Heath Robinson, and so forth. Weaver offered two depictions of his structure for the "cryptographic-translation" thought. To start with, he noticed how the ex-German "diminished the message to a segment of five-digit numbers," yet was fruitless in inferring the plaintext on the grounds that the message was still "coded" in Turkish; in any case, when redressed for word dividing, the first Turkish was uncovered. Second, Weaver depicted a strategy for deciding the measurable semantic character of language, which he doled out an estimation of N. The fundamental estimation of N would change as per the language to be interpreted, just as the particular type of composing. In this way, contended Weaver, writings would have contrasting likely N esteems, showing their semantic character. To help in interpretation, for the littlest semantic unit (the word), the estimation of N could likewise be determined against adjoining words.

After a few years, a group of researchers at Georgetown University made the first machine translation with IBM partnership in 1954. In this translation which was made by IBM 701 mainframe computer, known as the Georgetown Experiment, the system memory consisted of 6 grammar rules and 250 words. Between the years of 1958 and 1966, the concept of computerized translation was introduced with the Systran system carried out by the US Air Force during the Cold War. This system, which emerged with the desire to obtain the secret information of the Soviets during the Cold War years and to give them an advantage over their enemies, was working on listening to the communications and solving the cryptos and finding a response to the solved words. However, there had not been any significant developments in the last decade. Nevertheless, works in the field of machine translation continued during the 1970s. The Systran project, implemented by the US Air Force, was purchased and put into practice by the European Union. By the 1980s, be that as it may, completely programmed superb machine interpretation was at long last a reality, and beginning to discover noteworthy use inside governments and private associations. During the 1990s, look into fundamentally moved far from realist approaches that had tried to comprehend hidden etymological guidelines crosswise over the source and target languages, and rather utilized substantial language corpora and modern insights.

Following this pattern, as of late Google has risen as an innovator in the field, with its capacity to use huge stores of information gathered from the web and over its customized administrations, related to its mastery in algorithmic translation preparing and AI. Likewise, be that as it may, Google's way to deal with machine interpretation has, maybe conclusively, disjoined the current strain among realist and empiricist approaches, which had existed together in the accounts of machine interpretation and cryptanalysis since its most punctual days. In fact, Google openly declares that they do not employ linguists,(13) and has even created inter-language dictionaries programmatically, without relying on the intuitions of humans or underlying linguistic rules.(14) Their methodology has been, apparently, very effective, and mirrors incline in current cryptanalysis as well.

## CONCLUSİON

Cryptographic machines that gained momentum during the Second World War also impacted the field of translation and paved the way for the emergence of various projects in this field. Although the desired results are not obtained from the initial efforts, we see that the computers and the Internet have been used widely in the field of translation, especially after the nineties. Particularly, we have witnessed that studies in the field of machine translation which we called computer language translation

gained success and we have witnessed extremely successful translations of structurally similar language pairs. Today, machine interpretation and cryptanalysis have little job for etymologists or discerning models of language. "Calculating," for machine interpretation and cryptanalysis both, is currently the standard.

**REFERENCES**


1. John Hutchins. The first public demonstration of machine translation: the Georgetown-IBM system, 7th January 1954. P.1-10(**PDF**)
2. W. John Hutchins. Two precursors of machine translation: Artsrouni and Trojanskij. International Journal of Translation 16, no.1(2004) P.14(**online article**)
3. Keijo Ruohonen. Mathematical Cryptology. CreateSpace Independent Publishing Platform, September 2014. P.1-10, (Translation by Jussi Kangas and Paul Coughlan),(**PDF**)
4. Cheng-Jing Kuo. Cryptography. P.1-34 (**research paper**)
5. Stephen Doherty.The impact of translation technologies on the process and product of translation. International Journal of Communication. February 2016, https://www.researchgate.net/publication/284725157_The_impact_of_translation_technologies_on_the_process_and_product_of_translation (**online article**)
6. Jeremy Norman. Descartes Discusses the Idea of an Artificial Language, http://www.historyofinformation.com/detail.php?entryid=2868 (**online article**)
7. Rod Johnson. Contemporary Perspectives in Machine Translation. Human translation, machine translation. Papers from 10th annual conference on computational Linguistics, Odense, Denmark, 22-23 November 1979,ed. Suzanne Hanon and Vigo Hjørnager Pedersen. P.1-15 (**research paper**)
8. Daniel Stein. Machine Translation, Past, Present and Future. P.1-9 https://pdfs.semanticscholar.org/731b/6eafa28982e958e11a7b15458cd9d0c73c1a.pdf?_ga=2.206901395.1272980175.1554058037-1400295672.1553172344 (**research paper**)
9. Retrospect and Current Status of Machine Translation in India. Chapter 4. P.1-10 (**PDF**)
10. Enigma Machine, https://brilliant.org/wiki/enigma-machine/ (**online article**)
11. Eric Roberts. The Enigma Machine. February 3, 2016. P.1-7(**PDF**)
12. Enigma: Cryptography, World War and Alan Turing, ed. Keshav Dhandhania https://www.commonlounge.com/discussion/fedea6d1cac94be1b4fb066e5557e5e1 (**online article**)
13. Thomas Schulz, "Translate This: Google's Quest to End the Language Barrier," Spiegel Online September 13, 2013, sec. International, http://www.spiegel.de/international/europe/google-translate-has-ambitious-goals-for-machine-translation-a-921646.html (**online article**)
14. Nataly Kelly, "Why Machines Alone Cannot Solve the World's Translation Problem," Smartling, January 9, 2014, https://www.smartling.com/2014/01/09/machines-solve-worlds-translation-problem/. (**online article**)
15. Quinn Dupont. The Cryptological Origins of Machine Translation, from al-Kindi to Weaver. University of Washington Seattle. 13 April, 2018. P.1-20. (**online article**)