International Journal of Research in Engineering, Science and Management
Volume 6, Issue 6, June 2023
https://www.ijresm.com | ISSN (Online): 2581-5792

How to Solve Unbreakable Codes: World War II Edition; Version 202.3

Olivia Dhandhayuthapani*
Undergraduate Sophomore Student, Georgia State University, Atlanta, United States of America

***Abstract*: We cannot imagine a life without the Internet. Cyber data security has become a main concern for anyone connected to the web. The security and privacy of information are maintained by encryption. Decryption techniques are also equally important to check the robustness of encryption. So, this paper is an exploration of the feasibility of using current technologies like Machine Learning and Blockchain concepts to break the encryptions, with special reference to the Enigma encryption.**

***Keywords*: Artificial Intelligence, Blockchain, Cryptography, Cryptology, Encryption, Enigma, Decryption, Machine Learning, Neural Network.**

1. Introduction

Forensics, specifically Cyber Forensics, Cyber Security and their related fields are always interesting topics to debate about. Movies and series with this background are favorites, especially The Imitation Game and The Code. The Imitation Game, where the protagonist Alan Turing pushes the frontiers of Mathematics to reach the realms of modern-day computer science, while decrypting the Codes of Enigma, is a fascinating watch. Enigma has always been a captivating subject to cryptographers and fans of cryptology. The basic tenet of his genius was that it was possible to change the function of a mechanical machine simply by changing the symbols one feeds into it. So, it was during my third time around this movie that I decided to explore the feasibility of current technologies like Machine Learning and Blockchain concepts to break the Enigma or similar encryptions. One wonders how fast Marian Rejewski and Alan Turing would've broken the "unbreakable" code today with new advancements in technology.

The Enigma machine (Figure 1) is a cipher device developed from previous encrypting machines in the mid-twentieth century for considerable use by Germany during World War II for strategic purposes. The Enigma machine was thought to be capable of enciphering even the most sensitive messages through the war. The invention of this machine was a game changer in the field of Cryptography. After much trial and error, it was realised that the group theory offered a better chance at deciphering the codes. It was theorised that the Enigma encryption for each letter could be defined mathematically by permutations.

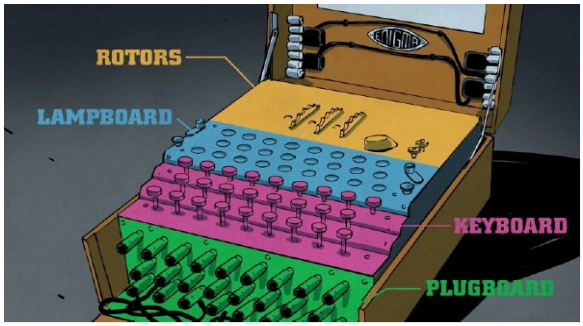


Fig. 1. Enigma Machine *(Source: Steven Dufresne, 2017)*

The Enigma was an electro-mechanical rotor mechanism that scrambles the 26 letters of the alphabet and was first developed in 1918. Essentially, the mechanism had a keyboard and rotating rotors, a lamp and a reflector. In simple terms, it is the constant movement of the rotors that result in cryptographic transformation after each key press. The actual decipherment of a letter is performed electrically. When a key is pressed, current flows through the various components and ultimately lights one of many lamps, indicating the output letter (Hart et al., 1999). For example, when encrypting a message 'DATA', when the operator presses A key, the D lamp might light. The operator would then proceed to encipher other letters (Figure 2).

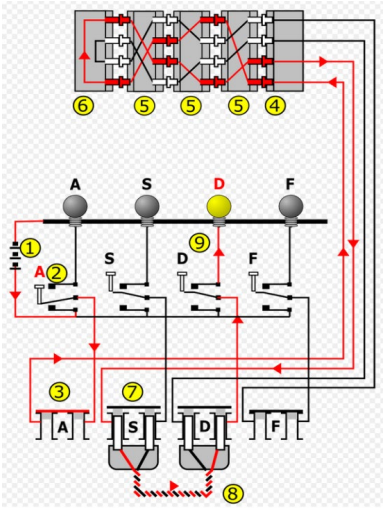


Fig. 2. Enigma wiring diagram showing flow of current when key is pressed. The A key is encoded to the D lamp. D yields A, but A never yields A *(Source: Telenet)*

*Corresponding author: oliviamars2003@gmail.com

The machine/rotor settings were changed every day during wartime. The secret key lists were distributed in advance, to ensure security.

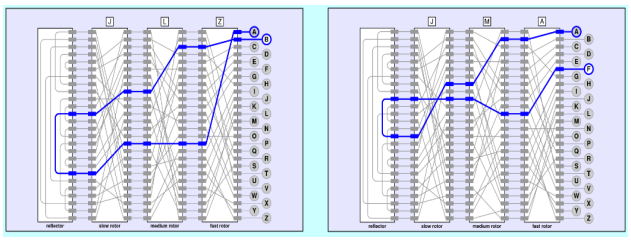
Can Enigma be broken today with new information technology like Machine Learning and Blockchain?

Mathematical discovery or reasoning and intuition are important to practicing Maths. An agreed proof initially itself is not necessarily always possible, because reasoning is the first step towards proving the theorem or hypothesis. On this premise, this article explores the feasibility of using Machine Learning and Blockchain technology for decryption. Attempts have been made to decode the Enigma keys using AI, but it has not been totally successful. The approach proposed here is novel, innovative and incorporates the interoperability between Machine Learning and Blockchain. Machine language is complemented by Neural Network technology which can understand data, identify patterns and linkages, predict outcomes and is self-learning, all with minimal human intervention. Blockchain is basically a digital ledger that records the provenance of digital assets in blocks that are linked together using cryptography and has made huge advances in cryptography (Idrees et al., 2021).

The Approach of Machine Learning, Neural Network for Enigma Decryption

The Enigma machine utilised symmetric cryptography. The cipher uses symmetric keys and the cipher text of a character is dependent on the key and the state of the machine. The idea of using Machine Learning methods to decrypt enigma text is therefore a natural extension of the application of Artificial Intelligence and Machine Learning.

In the Machine Learning field, a Neural Network is a set of algorithms that recognises underlying relationships in a dataset through a process that simulates the human brain (Fuzellier, 2019) as depicted in Figure 3. Recurrent Neural Networks (RNN) are the key to dealing with sequential data and are specifically well suited for problems requiring a memory of past events, like making predictions based on time series data (Brownlee, 2017). Based on this very premise, when data is fed into an RNN after it has decrypted certain "test sets", it is expected to be far more capable of recognizing a pattern and decrypting the encrypted text much quicker. The decryption process should be a sequence-to-sequence translation task using a Neural Network based model. It is hypothesised in this paper that its decryption could be faster and successful based on the relevance of the current technologies as well as the similarity in the network linkages (Figure 3). Based on further research, algorithms have to be developed and tested.



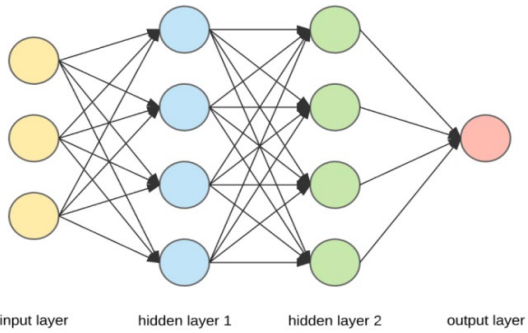


Fig. 3. Similarity between the Enigma and the Neural Network concept *(Source: Researchgate and Stanford publications)*

When considering a neural network programmed to decrypt Enigma, in the name of paying tribute to history, the test sets could be the ones already known to Polish scientists in the 1940's - primarily that every message started with an update on the weather and ended with a phrase declaring loyalty to Germany. After the RNN has successfully decrypted these "test sets", it will be able to solve encrypted messages very efficiently and the Enigma code can be broken to give real-time plaintext. Simpler RNN formulation (Figure 4):

$h_t = W f(h_{t-1}) W^{(hx)} x_{[t]} \hat{y}_t = W^{(s)} f(h_t)$, *where h(t) is a function of the previous hidden state h(t-1)*

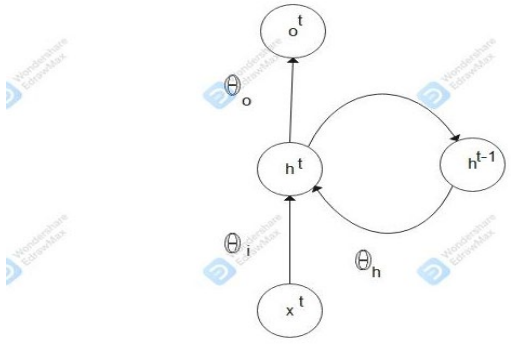


Fig. 4. Recurrent Neural Network architecture constructed using Wondershare edrawmax

In the simplest terms, this is how an RNN evolves over time;
$o_t = f(h_t;\theta)$ where $h_t = g(h_{t-1},x_t;\theta)$

These equations can be extrapolated for decryption, based on the number of known and unknown variables. The application of machine learning in the domain of cryptanalysis can open up new avenues, since any complex cipher system has a large key space. The commonality between the current technologies is being sought based on the premise that cryptanalysis can be used for synthesising solutions in the field of cryptography.

The approach of Blockchain for enigma decryption:

A blockchain is an expanding list of records, called blocks that are networked together using cryptography. It is a system of recording information which makes it least susceptible to change or hacking by unauthorised parties. A blockchain is like a ledger that facilitates recording of asset transactions and

tracks their identity and transfer in a business network.

Blockchain technology is mainly based on cryptography technology. Many facets of cryptography research is used for it, but research in the reverse direction, i.e. blockchain research used for cryptanalysis, has not been done and is an exceedingly novel proposition, not proposed in any forum to the best of the author's knowledge. Symmetric and Asymmetric key cryptography and Hash Functions that don't make use of keys, but a cipher to generate a hash value of a fixed length from the plaintext, are important components of Blockchain. If this approach is successful, then it may become a game changer in cryptography. At present, this is higher order research, but this paper is limited to only exploring feasibilities and providing insights into feasible solutions.

2. Way Forward

Today, in the digital world connected by the World Wide Web, cyber security, whether it is in daily life or aspects of national security, is of paramount importance. Cyber forensics too, is fast developing. Here, cryptology/encryption plays an important part to ensure information reaches the intended, as codes and ciphers keep evolving. Computer technology is an inherent part of this field, because understanding "Randomness" is a unique trait required for cryptology. The understanding of the history of encryption will also be the foundation for developing sophisticated unbreachable encryption systems, for testing the software backdoors, for preventing invasion of privacy, national security and related applications.

References

[1] Abdel-Karim Al Tamimi, Performance Analysis of Data Encryption Algorithms, 2008.
[2] Andonov, S., Dobreva, J., Lumburovska, L., Pavlov, S., Dimitrova, V., & Popovska Mitrovikj A, Application of Machine Learning in DES Cryptanalysis, 2020.
[3] Andrew Hodges, Alan Turing: The Enigma,1983
[4] Borowska, A., & Rzeszutko, E, The cryptanalysis of the Enigma cipher.The plugboard and the cryptologic bomb, 2014.
[5] Brain Hart and Michelle Lombard, The Enigma Cipher, 1999.
[6] Chris Christensen, MAT/CSC Permutation Ciphers, 2015.
[7] Curie TC, How 2000 Droplets broke the Enigma Code in 13 Minutes, 2018.
[8] Graham Ellsbury, The complexity of the Enigma, 1998.
[9] Greydanus, S, Learning the Enigma with Recurrent Neural Networks, 2017.
[10] Jason Brownlee, A Gentle Introduction to Long Short-Term Memory Networks, 2017.
[11] Maxence Fuzellier, Neural Networks Fundamentals, 2019.
[12] Perusheska, M. G., Dimitrova, V., Popovska-Mitrovikj, A., & Andonov, S, Application of Machine Learning in Cryptanalysis Concerning Algorithms from Symmetric Cryptography, 2021.
[13] Prasad, K., &Kumari, M, A review on mathematical strength and analysis of Enigma, 2020
[14] Sheikh Mohammad Idrees, Mariusz Nowostawski, Roshan Jameel and Ashish Kumar Mourya, Security Aspects of Blockchain Technology Intended for Industrial Applications, 2021.
[15] Tang, L., Lee, N., & Russo S, Breaking Enigma, 2018.
[16] Thomas W. Edgar, David O. Manz, Science and Cyber Security, Research Methods for Cyber Security, 2017.
[17] https://cryptii.com/pipes/enigma-machine
[18] https://wenku.baidu.com/view/3e556b5269dc5022abea0094.html