Deep Learning Based Analysis of Key Scheduling Algorithms of Advanced Ciphers

Narendra Kumar Patel
M.Tech CSE Cyber Security
VIT Bhopal University 466114
narendra.k91630@gmail.com

Hemraj Shobharam Lamkuche
School of Computing Science Engineering
VIT Bhopal University 466114
hemraj.lamkuche@gmail.com

Abstract :

In the realm of modern information technology, the Advanced Encryption Standard (AES) and the PRESENT cipher play pivotal roles in securing data and enabling confidential transactions. AES is widely recognized for its versatility and application across various domains, while the PRESENT cipher excels in lightweight cryptographic scenarios. This paper undertakes a dual examination, focusing on the Key Scheduling Algorithms (KSAs) of both AES and the PRESENT cipher, crucial components responsible for generating round keys in their respective encryption processes. Through a simplified analysis employing deep learning techniques, particularly utilizing a Neural Network model, our research aims to unravel the intricacies of these KSAs, shedding light on their behaviors, strengths, and potential vulnerabilities. By discerning patterns and weaknesses within both ciphers through the application of a deep learning neural network trained on comprehensive datasets, our study contributes insights crucial for identifying potential exploitable avenues by malicious entities, emphasizing a proactive defense strategy against evolving threats.

Moving beyond vulnerability assessment, this paper proposes security enhancements for both AES and the PRESENT cipher, advocating for a proactive approach to safeguard cryptographic systems. The application of machine learning, specifically deep learning, to detect patterns and unearth cryptographic keys within systems reliant on both AES and the PRESENT cipher provides a novel perspective. This comprehensive framework not only advances our understanding of these cryptographic algorithms but also presents a proactive defense strategy against potential threats in diverse security contexts.

Keywords: Advance encryption standards(AES), PRESENT Cipher , Deep learning , Neural Network, Key scheduling algorithm(KSA), Data security

Introduction

The history of Advanced Encryption Standards (AES) and the PRESENT cipher unfolds against the backdrop of an imperative to enhance data security, echoing the timeless adage that "necessity is the mother of invention." At the close of the 20th century, the burgeoning exchange of information over computer networks underscored the importance of safeguarding data privacy. The Data Encryption Standard (DES), widely utilized since the 1970s, faced obsolescence in the wake of modern cyber threats, prompting the U.S. National Institute of Standards and Technology (NIST) to initiate a competition in 1997. This global challenge invited cryptographers and mathematicians to submit encryption algorithms that excelled in security, efficiency, and versatility.

Following a meticulous selection process, the Rijndael encryption algorithm, conceived by Belgian cryptographers Vincent Rijmen and Joan Daemen, emerged triumphant and was officially adopted as the AES standard by NIST in 2001. AES, serving as a specialized lock in computer networks, employs a secret key and relies on a critical component known as the Key Scheduling Algorithm (KSA). This algorithm acts as a unique recipe, transforming the secret key into a complex set of characters that serve as the foundation for securing digital data. In parallel, the PRESENT cipher was developed as a response to the inadequacies of existing encryption standards, emphasizing efficiency without compromising security in lightweight cryptographic scenarios. Both AES and PRESENT employ secret keys and unique Key Scheduling Algorithms, pivotal components in their encryption processes.

This research paper ventures into a novel dimension by incorporating Deep Learning techniques to scrutinize the security strengths and potential vulnerabilities of the Key Scheduling Algorithms of both AES and PRESENT. Deep Learning, akin to a super-smart computer brain, has the capability to unveil intricate patterns and secrets in data that might elude conventional analysis methods. Through the application of Deep Learning Techniques, the study aims to provide a comprehensive analysis of the security strengths, weaknesses, and potential patterns based vulnerabilities in the Key Scheduling Algorithms of both AES and PRESENT, contributing to an enhanced understanding of their cryptographic robustness in diverse security contexts.

AES Cipher

The AES (Advanced Encryption Standard) Cipher is a method of securing digital information which transfer over the internet and in digital assets . It functions like a digital lock, which is safeguarding our data during transmission over the internet or when stored on digital devices. In this cipher technique our normal message is considered as plain text, and AES transforms it into ciphertext as a secret code. For unlocking this message requires a specific key, which must be known only to the intended person. AES is most important for online security because it makes very hard or impossible for unauthorized individuals from decrypting this shared private information. Our information may any type such as passwords or messages which will be used by only authorized person. AES provides us very strong mechanism for securing and encrypting our data.

AES Keys and Rounds

AES Encryption/ Decryption rounds depends on what type of key size we are using for encryption and decryption process . In generally we can say that If the key size is larger of encryption process then It is much more secure way compare to less size of key encryption process .

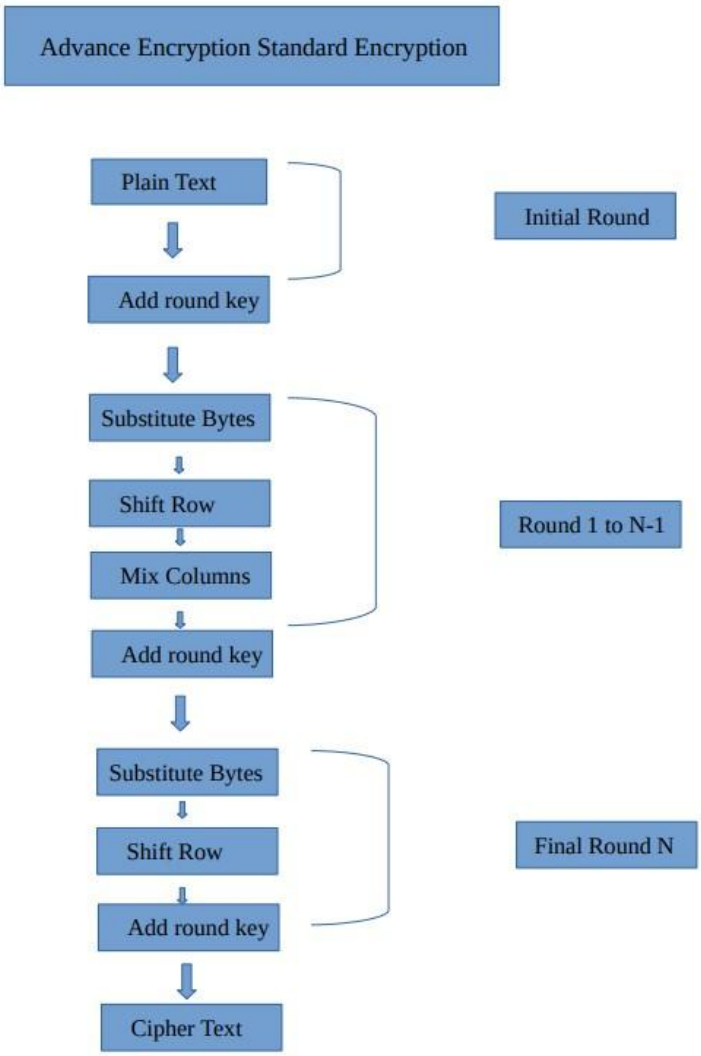
Based upon rounds and keys there are three type of AES Encryption and Decryption which are being used based upon selection and our need -

(i) 128 Bit key – 10 Rounds : It uses 128 bit block size of keys and total 10 rounds for encryption and decryption process .
(ii) (ii) 192 Bit key – 12 Rounds : It uses 192 bit block size of keys and total 12 rounds for encryption and decryption process .
(iii) (iii) 256 Bit key – 14 Rounds : It uses 256 bit block size of keys and total 14 rounds for encryption and decryption process.

Encryption Process of AES

There are multiple number of steps which AES use for Encrypting the our given input data.

Following is Representation of AES Encryption Process. In the diagram N can be any value from the 10,12,14 which represents it which type of AES Encryption we are doing -



[Figure – AES Encryption Process]

For understanding in better way lets see each step one by one-

(i) Initial Round : In the initial round, AES takes the input data (plain text) and combines it with the first round key. This is the first step to create the cipher text. AES apply a substitution-permutation network (SPN) structure for encryption.
(ii)
(iii) Sub-Bytes : This step involves replacing each byte of data with a corresponding byte from the AES S-box, which is a predefined substitution table and it is constant for any AES Encryption .
(iv) Shift Rows : This step rearranges the bytes within each row of the data matrix.

(iv) Mix Columns : In this operation, the columns of the data matrix are mixed using mathematical transformations.

(v) Add Round Key : The round key for the current round is XORed with the data.

(vi) Final Round : The final round is similar to the other rounds but leave the Mix Columns step. It includes Sub Bytes, Shift Rows, and Add Round Key operations. After all the rounds are completed, the plain text data is transformed into cipher text, which is the encrypted form of the plain text. This transferred Cipher text is decrypted on other side using same reverse process and finally recipient get the plain text in secure way.

Key Scheduling Algorithm of AES

The heart of AES is its Key scheduling algorithm which makes it much more secure than other ciphers. Following is process for generating AES-128 Bits round keys :

1. Key Expansion:

   a. Begin with the original 128-bit key.

   b. Initialize an array to store the round keys.

   c.The first round key is the original 128-bit key.

2. Round Constants:

   a. Initialize a list of round constants (Rcon). There are a total of 10 round constants for AES-128, which are used to generate the round keys.

3. Key Expansion Loop:

   a. The key expansion loop consists of multiple iterations (10 in the case of AES-128).

4. Word Transformation:

For each iteration, take the last 4 bytes (32 bits) of the current round key. And Perform a series of transformations

a. Rotate: Circularly shift the bytes in the word to the left by one byte.

b. Sub Bytes: Apply the S-box substitution to each byte.

c. XOR with R-con: XOR the first byte of the word with the corresponding round constant from R-con.

d. XOR the first byte of the word with the first byte of he previous round key.

e. XOR the remaining three bytes with the corresponding bytes from the previous round key.

5. Expand Key:

The newly generated 32-bit word is XORed with the 32-bit word located 4 bytes earlier in the round key. This result is the next 32-bit word for the round key.

6. Store Round Key:

Add the newly generated 128-bit round key to the Round Keys array.

7. Repeat:

Repeat this process for a total of 10 iterations to generate 10 round keys for use in the encryption rounds.

This is how AES-128 Bits keys being generated

PRESENT Cipher

The present cipher is a cryptographic algorithm used to secure information by transforming it into a coded format. Unlike traditional methods, it operates on smaller units of data, typically one bit at a time. This unique approach enhances its efficiency and security. The present cipher is celebrated for its resistance to various attacks, ensuring robust protection for sensitive data. Its simplicity and effectiveness make it a popular choice in modern cryptography, offering a reliable means of safeguarding information in digital communication. As technology evolves, the present cipher stands as a key player in the ongoing quest for secure and efficient data encryption.

PRESENT Keys and Rounds

The present cipher employs a key schedule to generate a series of subkeys crucial for encoding information. These subkeys, along with the chosen key size, contribute to the algorithm's security. The key size, often 80 or 128 bits, determines the complexity of potential key combinations, enhancing resistance against brute-force attacks. With a standard of 31 rounds, each involving key mixing and permutation operations, the present cipher achieves a delicate balance between security and computational efficiency.

Key Scheduling Algorithm of PRESENT

The Key Scheduling algorithm in PRESENT involves a series of precise operations to generate round keys. Following are general steps to generate 80 bit round keys for each round -

Initialization:

- The user inputs an 80-bit key into the key register (K).
- Let K=K79-K78-K77 …K1-K0.

· **Round Key Generation:**

- For each round i, the left-most 64-bits of the current key register are taken as the round key kr for that round.
- kr=k63k62…k0=K79K78…K16.

· **Key Rotation:**

- After every round i, the key register is rotated by 61-bit positions to the left.
- Let K′K′ be the rotated key register.

· **Key Update:**

- The rotated key register (K′K′) is updated by passing the leftmost 4 bits through the S-Box.
- The round-counter value i is XORed with bits K19-K18-K17-K16-K15 with the least significant bit of the round-counter on the right.
- The result of the XOR operation is then used to update the key register.

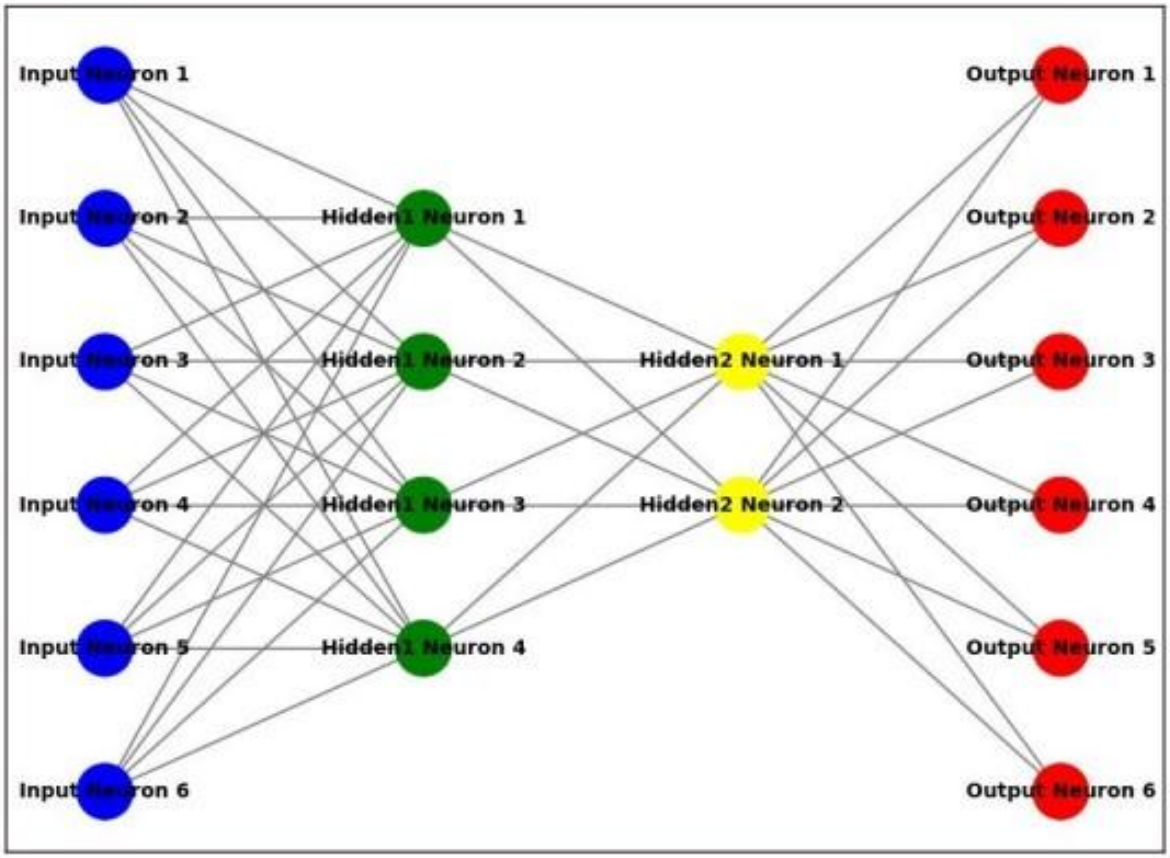
By this process every round key register get updated and it uses for next round.

Deep Learning

In this modern technology world we can not ignore the power of AI and Deep Learning. Deep learning is like teaching computers to learn on their own, just like we teach kids. It is something like when we see any object again and again then our mind become able to identify similar type of object in very short time. In deep learning, we give lots of data in array and matrix form to model , like cat and dog pictures, and our deep learning models then tries to find patterns by itself. It uses artificial neural networks, which are like virtual brains. These networks have layers of tiny decision , makers that work together to understand the data. Once our model trained using various data and techniques then it can identify similar pattern and can generate results. This helps in many things, like recognizing our voice or faces in photos. Deep learning is an important part of artificial intelligence which makes our technology smarter and it also becoming more helpful in our daily life.

Neural Network

As the name suggest neural network it is a computer system which is designed to behave like the human brain. It is made of many interconnected nodes, like how our human neurons are connected in our brain, and it can process information and learn from this information. These network nodes work together to analyse data, recognize patterns, and make decisions. For example neural networks can be used to understand our spoken language, it can be also used to identify different objects in images, or predict trends based on input data. Neural network used in various tasks that involve analysis of complex data and they also have become important in machine learning and artificial intelligence. Just like our brain neural network adapts and learns from the given data and perform task which can done by human in the given situation . Neural networks can also be trained to improve their performance which makes them powerful tools for various applications. Following is structure of neural network which have one input layer with 6 neurons and two hidden layer with 4 and 2 neurons respectively and one output layer with 6 neurons. We can increase or decrease layers and neurons based upon need.



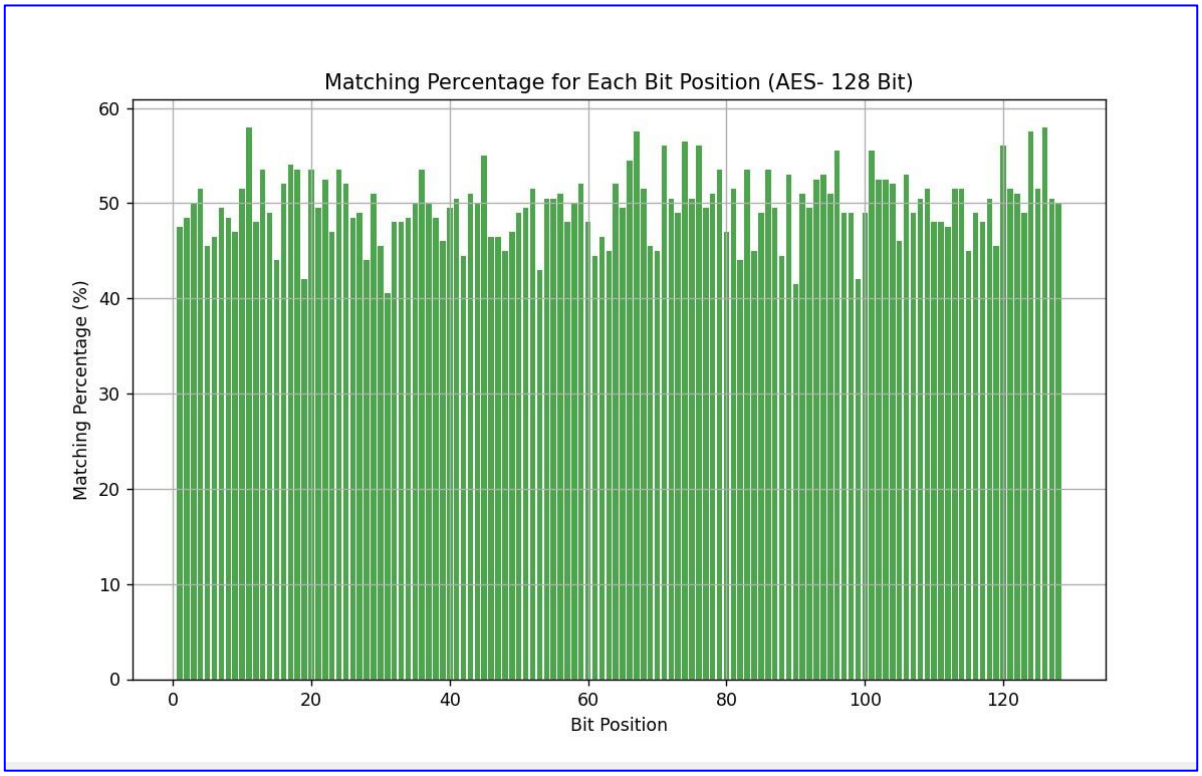
Analysis of AES & PRESENT Cipher KSA

In this research paper, we focus on enhancing the security analysis of the Advanced Encryption Standard (AES) and PRESENT cipher by using the power of Deep Learning, specifically Sequential Neural Networks (SNN). AES and PRESENT is mostly considered as most secure encryption algorithms, but they may not be immune to any deep learning based attacks. One area of vulnerability may lie in the key scheduling process, which generates round keys from the initial secret key. We propose using SNN to analyse and potentially strengthen this crucial component . We trained our model using 10,000 samples of AES and PRESENT Initial Round key and last Round key and after then we tested our Deep Learning trained model using 200 Initial Round Keys which tries to predict corresponding final round keys from Initial Keys. Following are Steps our Deep Learning Implementation:

1. Input Layer contains 128 neurons for AES and 80 for PRESENT Cipher
2. There are 5 hidden layers of 64, 32 , 16 , 8, 4 bits of neurons
3. Output layers activated using sigmoid function and it is of 128 bit neurons for 128 bit final Round key of AES and 80 bit neurons for 80 bit final round key of PESENT.

By using above steps we tested our model and gain insights about the AES KSA and PRESENT KSA security and Vulnerabilities.

Following is Bar chart representation of the gained output which shows bit position to X axis and Matching percentage to Y Axis.

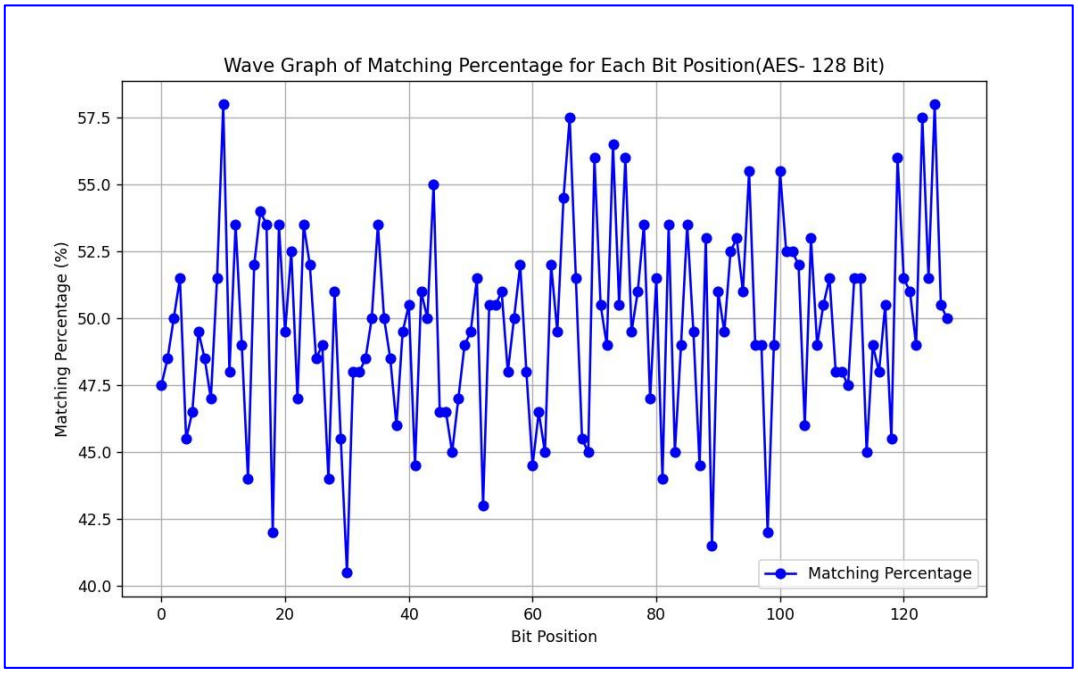


Results Table of AES

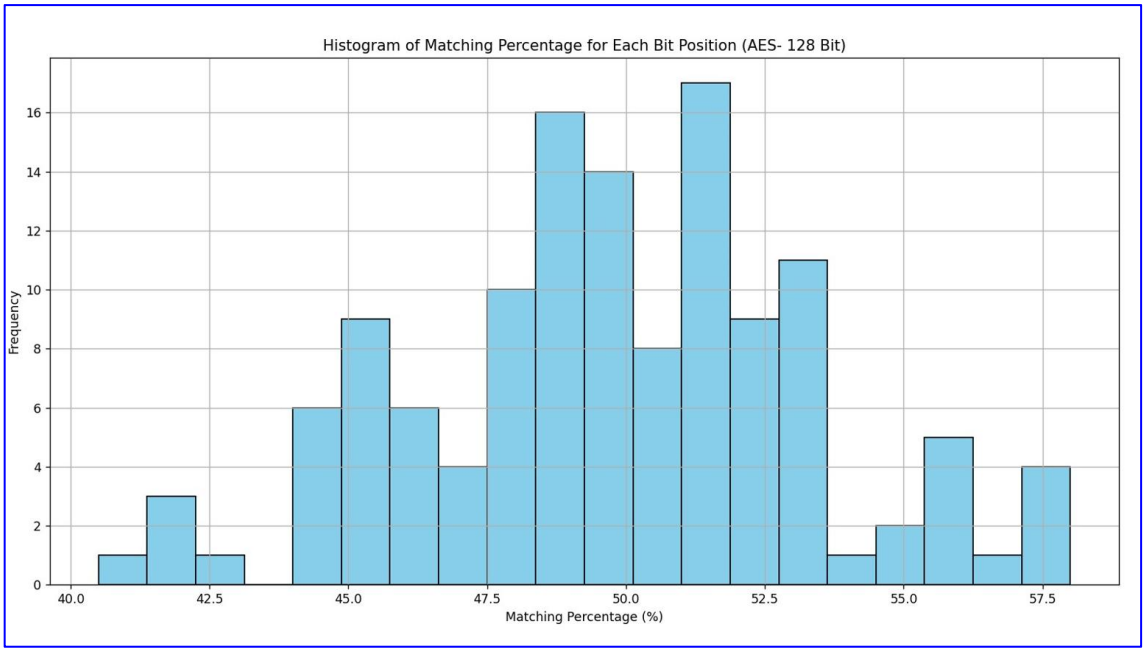
Deep Learning based Analysis of Key Scheduling Algorithm : AES Cipher							
Bit Position (1-32)	Matching % (1-32)	Bit Position (33-64)	Matching % (33-64)	Bit Position (65-96)	Matching % (65-96)	Bit Position (97-128)	Matching % (97-128)
1	47.5	33	48	65	49.5	97	49
2	48.5	34	48.5	66	54.5	98	49
3	50	35	50	67	57.5	99	42
4	51.5	36	53.5	68	51.5	100	49
5	45.5	37	50	69	45.5	101	55.5
6	46.5	38	48.5	70	45	102	52.5
7	49.5	39	46	71	56	103	52.5
8	48.5	40	49.5	72	50.5	104	52
9	47	41	50.5	73	49	105	46
10	51.5	42	44.5	74	56.5	106	53
11	58	43	51	75	50.5	107	49
12	48	44	50	76	56	108	50.5
13	53.5	45	55	77	49.5	109	51.5
14	49	46	46.5	78	51	110	48
15	44	47	46.5	79	53.5	111	48
16	52	48	45	80	47	112	47.5
17	54	49	47	81	51.5	113	51.5
18	53.5	50	49	82	44	114	51.5
19	42	51	49.5	83	53.5	115	45
20	53.5	52	51.5	84	45	116	49
21	49.5	53	43	85	49	117	48
22	52.5	54	50.5	86	53.5	118	50.5
23	47	55	50.5	87	49.5	119	45.5
24	53.5	56	51	88	44.5	120	56
25	52	57	48	89	53	121	51.5
26	48.5	58	50	90	41.5	122	51
27	49	59	52	91	51	123	49
28	44	60	48	92	49.5	124	57.5
29	51	61	44.5	93	52.5	125	51.5
30	45.5	62	46.5	94	53	126	58
31	40.5	63	45	95	51	127	50.5
32	48	64	52	96	55.5	128	50

The above accuracy table shows about how much percentage of bits we are able to predict correctly using our trained model. In the result table we can see some bits have more than 50 percent accuracy and some have less than 50 precent , In the overall result we can say it have approximate 50 percent accuracy which is 1/2 accurate predictability of the 10th round key in the form of 128 bits 0s and 1s. In the other words 1 and 0 bit also have 1/2 predictability means in any place there will be either 0 or either 1 . So by analyzing our results we can say the AES Key scheduling algorithm is secure and effective in order to face deep learning cryptanalysis by applying our used method. In further we can also used some more advance technique to test AES KSA Vulnerabilities.

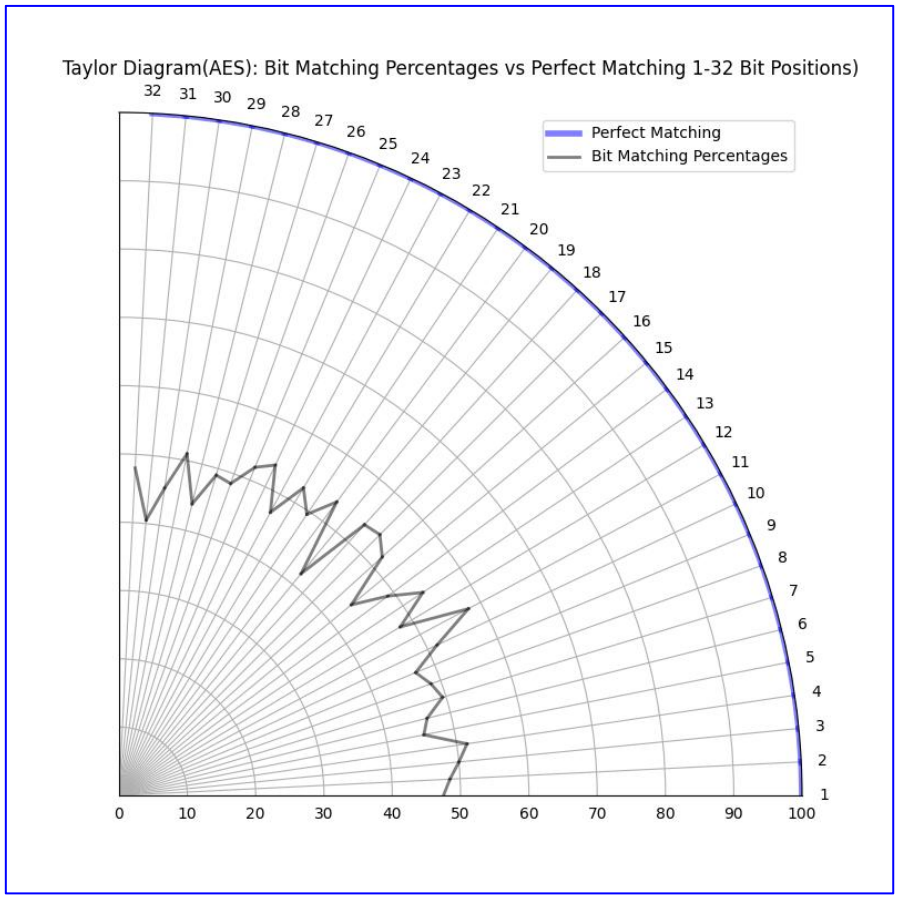
Following is Wave graph visualization of our gained output of AES Cipher.

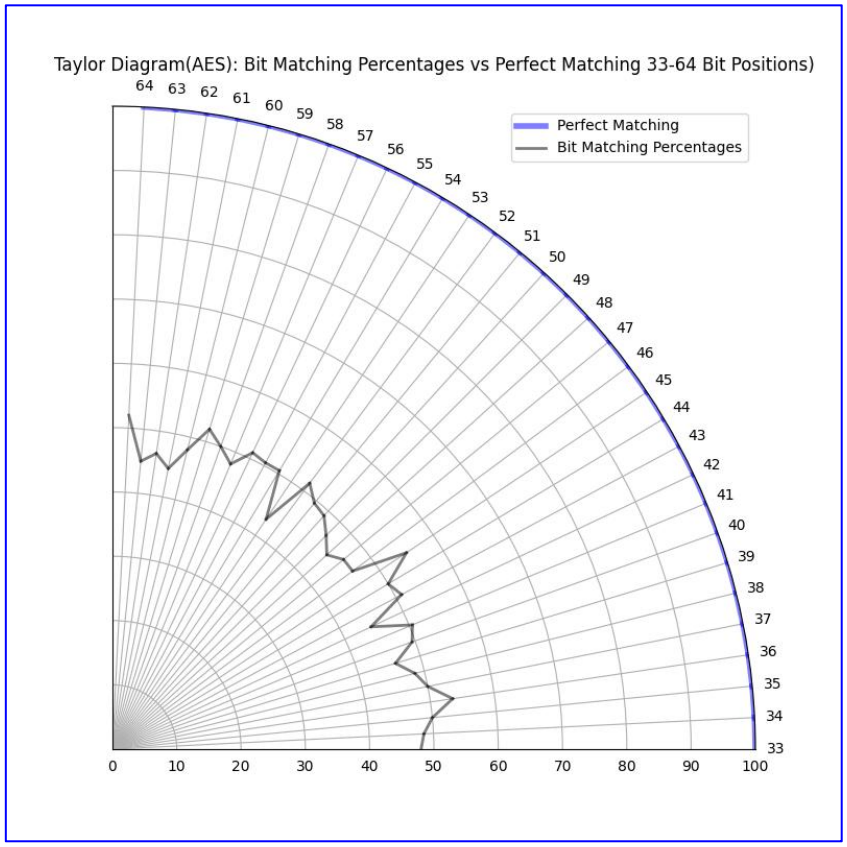


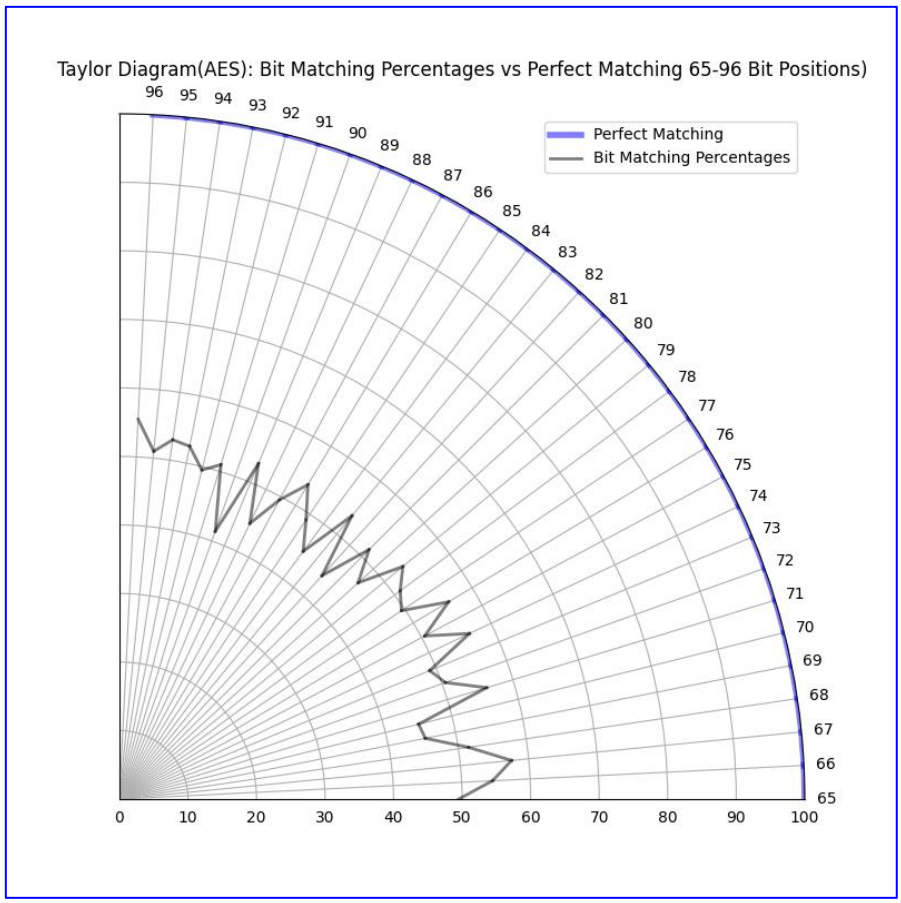
Following is histogram of our gained output of AES cipher.

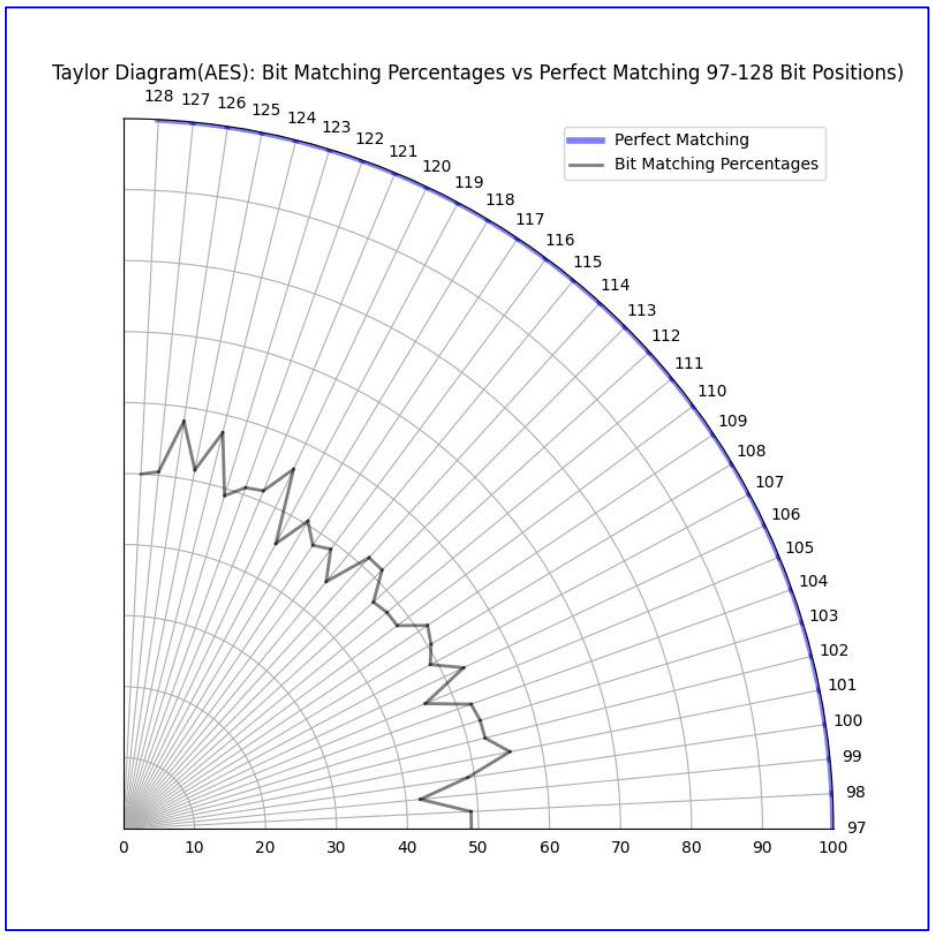


Following figures shows Taylor diagram of our gained output of 128 bit AES Cipher






Taylor Diagram(AES): Bit Matching Percentages vs Perfect Matching 65-96 Bit Positions)
Perfect Matching
Bit Matching Percentages
96 95 94 93 92 91 90 89 88 87 86 85 84 83 82 81 80 79 78 77 76 75 74 73 72 71 70 69 68 67 66 65
0 10 20 30 40 50 60 70 80 90 100

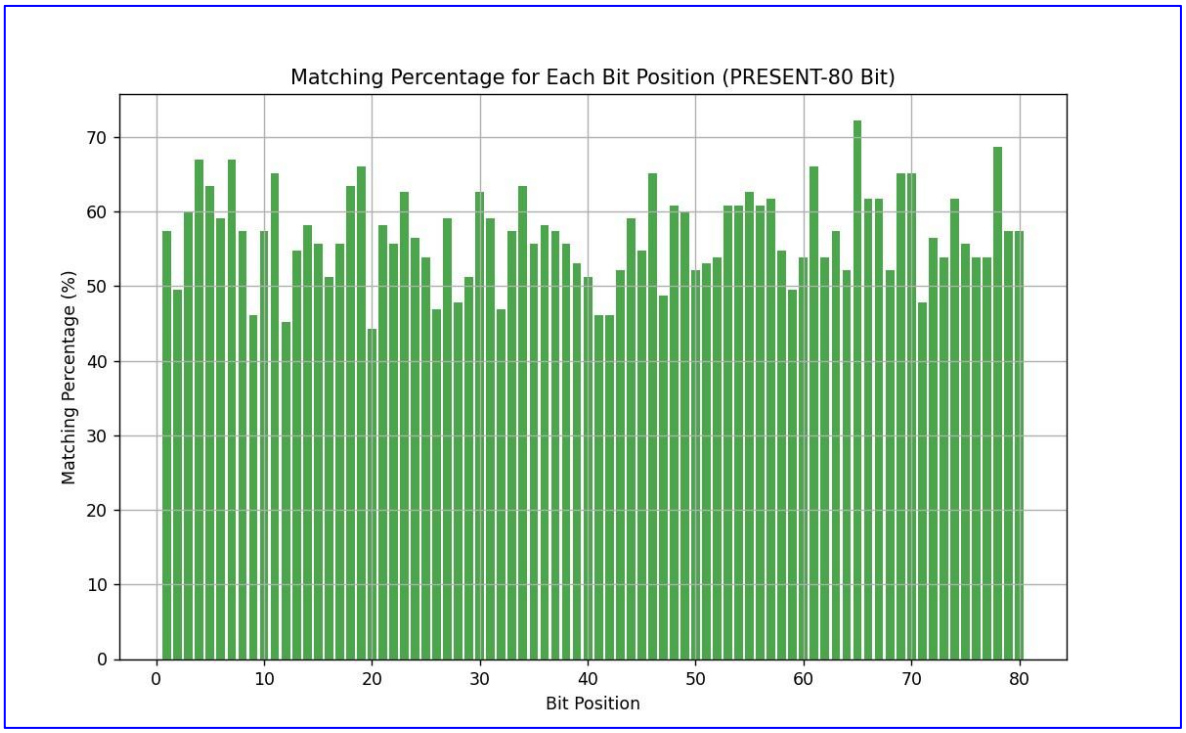

Taylor Diagram(AES): Bit Matching Percentages vs Perfect Matching 97-128 Bit Positions)
Perfect Matching
Bit Matching Percentages
128 127 126 125 124 123 122 121 120 119 118 117 116 115 114 113 112 111 110 109 108 107 106 105 104 103 102 101 100 99 98 97
0 10 20 30 40 50 60 70 80 90 100

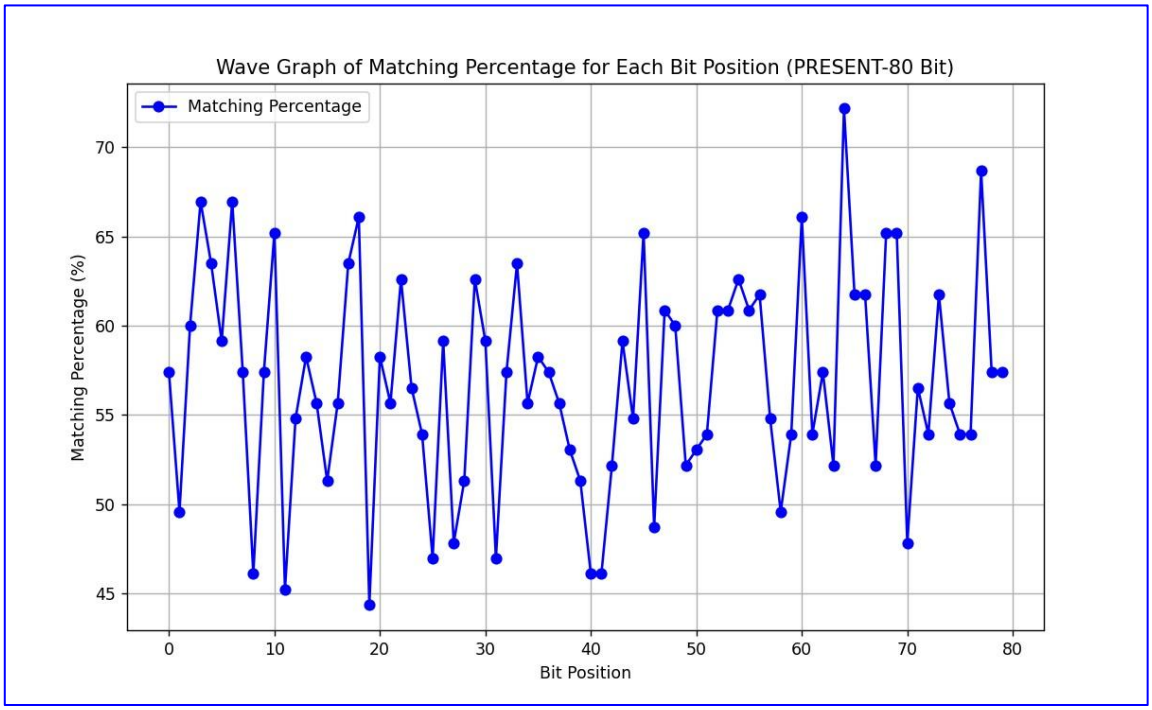
Results Table of PRESENT

Deep Learning Based Analysis of Key Scheduling Algorithm : PRESENT Cipher							
Bit Position (1-20)	Matching % (1-20)	Bit Position (21-40)	Matching % (21-40)	Bit Position (41-60)	Matching % (41-60)	Bit Position (61-80)	Matching % (61-80)
1	57.39	21	58.26	41	46.09	61	66.09
2	49.57	22	55.65	42	46.09	62	53.91
3	60	23	62.61	43	52.17	63	57.39
4	66.96	24	56.52	44	59.13	64	52.17
5	63.48	25	53.91	45	54.78	65	72.17
6	59.13	26	46.96	46	65.22	66	61.74
7	66.96	27	59.13	47	48.7	67	61.74
8	57.39	28	47.83	48	60.87	68	52.17
9	46.09	29	51.3	49	60	69	65.22
10	57.39	30	62.61	50	52.17	70	65.22
11	65.22	31	59.13	51	53.04	71	47.83
12	45.22	32	46.96	52	53.91	72	56.52
13	54.78	33	57.39	53	60.87	73	53.91
14	58.26	34	63.48	54	60.87	74	61.74
15	55.65	35	55.65	55	62.61	75	55.65
16	51.3	36	58.26	56	60.87	76	53.91
17	55.65	37	57.39	57	61.74	77	53.91
18	63.48	38	55.65	58	54.78	78	68.7
19	66.09	39	53.04	59	49.57	79	57.39
20	44.35	40	51.3	60	53.91	80	57.39

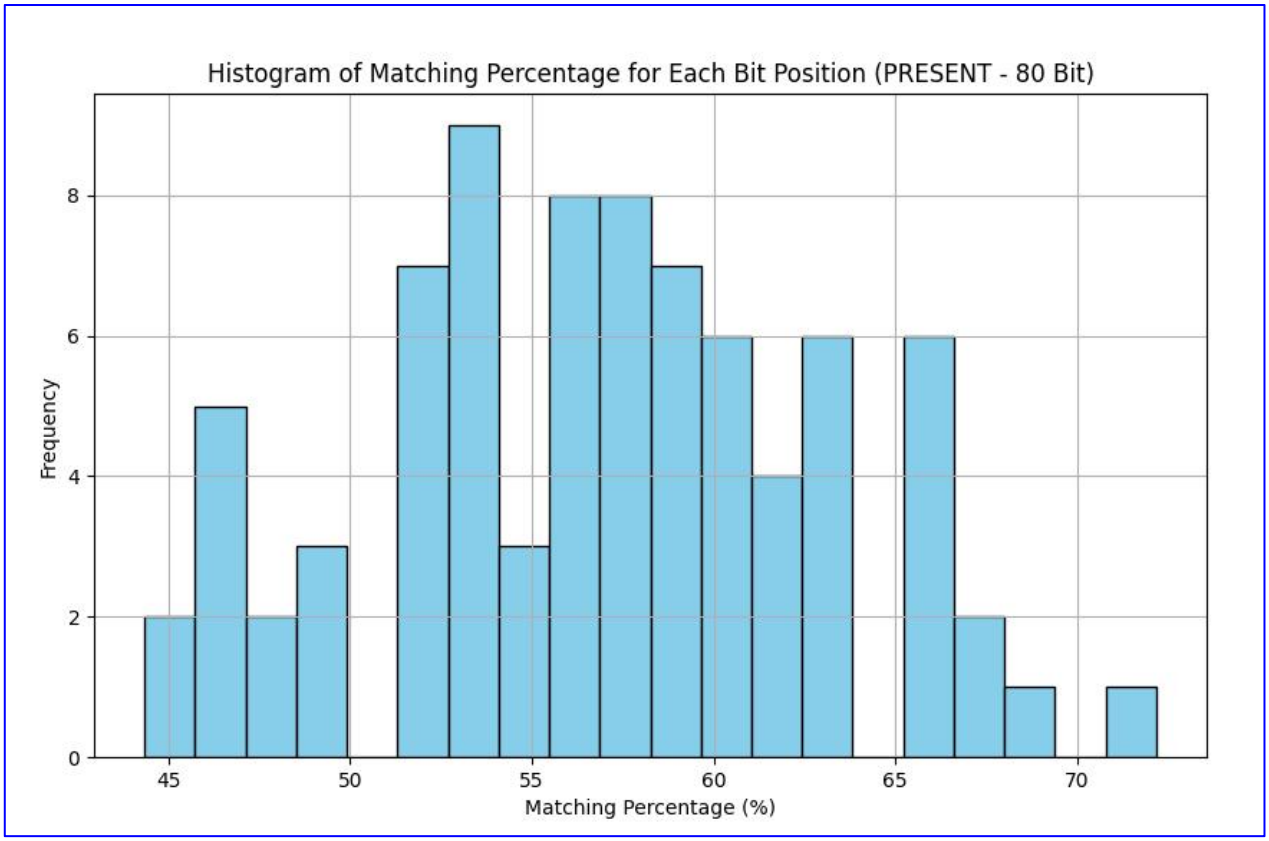
By applying same method as AES The above accuracy table shows about how much percentage of bits we are able to predict correctly using our trained model of PRESENT Cipher. We can see it is approximate 50% Accuracy and 1s and 0s predictability is also 50% separately .We can say that by using our model and method PRESENT Have resistance to face deep learning based Cryptography Analysis attack.

Following are bar chart and wave graph of our Analyzed results of PRESENT Cipher Key Scheduling Algorithm,

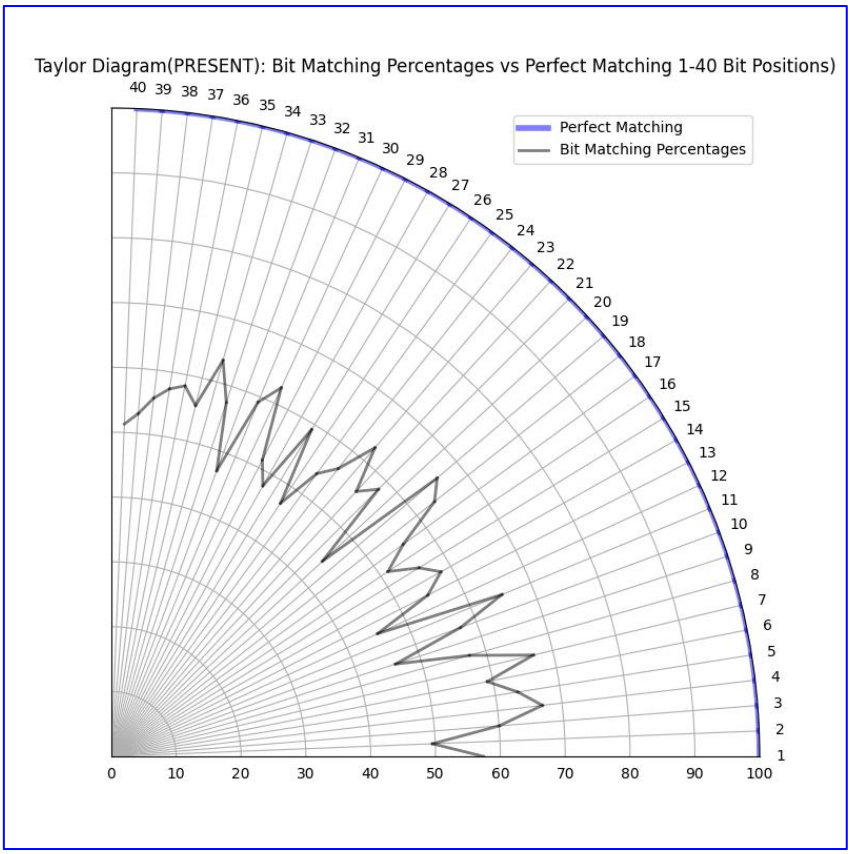


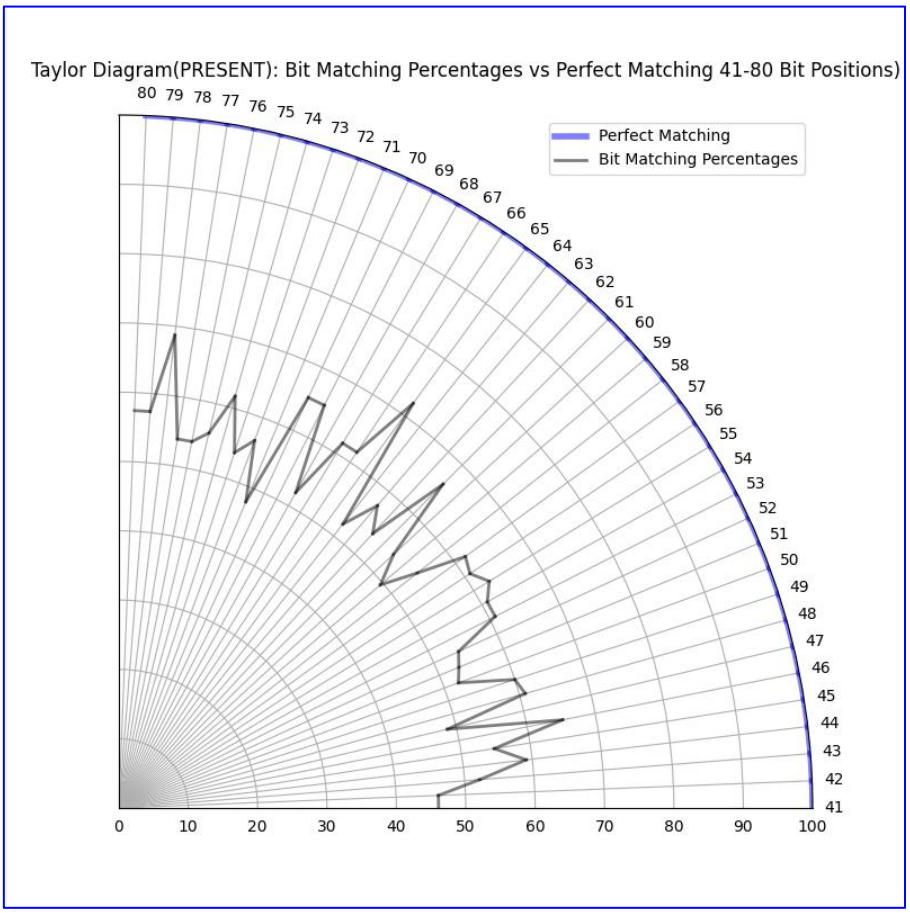


Following is Histogram Representation of our gained result of PRESNT Cipher



Following are Taylor Diagram Representation of our gained results.





Conclusion

In summary, we can say our paper focused on testing and ensuring that the Advanced Encryption Standard (AES) and PRESENT Cipher is secure by using a smart computer method which is also known as Deep Learning. We looked closely at a part of AES and PRESENT called the Key Scheduling Algorithm (KSA) and found that, despite being it strong, there are some areas where it could be safer. Using our Deep Learning model, we tried to find patterns and weaknesses in these KSA. The results, shown in the accuracy table, describes that we could predict about half of the final round key bits accurately. This means that the these KSA is quite good at resisting certain types of Deep learning analysis. Essentially, our study emphasizes that PRESENT and AES is secure and it provides ideas on how to make our cryptographic systems stronger against any AI based possible threats. It is also contributing to the ongoing improvement of data security and privacy issues.

References

[1] Chong, Bang & Salam, Iftekhar. (2021). Investigating Deep Learning Approaches on the Security Analysis of Cryptographic Algorithms. Cryptography. 5. 30.10.3390/cryptography5040030.

[2] Pareek, M., Mishra, G., & Kohli, V. (2020). Deep Learning based analysis of Key Scheduling Algorithm of PRESENT cipher. Cryptology ePrint Archive, Paper 2020/981.

[3] Bogdanov, A. *et al.* (2007). PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74735-2_31.

[4] So, Jaewoo. (2020). Deep Learning-Based Cryptanalysis of Lightweight Block Ciphers. Security and Communication Networks. 2020. 1-11. 10.1155/2020/3701067.

[5] Anees, Amir & Hussain, Iqtadar & Mujahid, Umar & Ahmed, Fawad & Shaukat,Sajjad. (2022). Machine Learning and Applied Cryptography. Security and Communication Networks. 2022. 1-3. 10.1155/2022/9797604.

[6] Abhishek Kumar Sinha , Jayaraj N, 2015, Performance Analysis of AES Cryptographic Algorithm, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCRTS –2015 (Volume 3 – Issue 27)

[7] Abdullah, Ako. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.

[8] Meraouche, Ishak & DUTTA, Sabyasachi & Tan, Haowen & Sakurai, Kouichi. (2021). Neural Networks Based Cryptography: A Survey. IEEE Access. PP. 1-1.10.1109/ACCESS.2021.3109635.ers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

[9] Nitaj A, Rachidi T. Applications of Neural NetworkBased AI in Cryptography.Cryptography.2023;7(3):39.https://doi.org/10.3390/cryptography7030039

[10] Rivest, R.L. (1991). Cryptography and Machine Learning. International Conference on the Theory and Application of Cryptology and Information Security.

[11] Taye MM. Theoretical Understanding of Convolutional Neural Network: Concepts, Architectures, Applications, Future Directions. Computation. 2023; 11(3):52. https://doi.org/10.3390/computation11030052.

[12] O'Shea, Keiron & Nash, Ryan. (2015). An Introduction to Convolutional Neural Networks. ArXiv eprints.

[13] S. Albawi, T. A. Mohammed and S. Al-Zawi, "Understanding of a convolutional neural network," 2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, 2017, pp. 1-6, doi: 10.1109/ICEngTechnol.2017.8308186.

[14] Grossi, Enzo & Buscema, Massimo. (2008). Introduction to artificial neural networks. European journal of gastroenterology & hepatology. 19. 1046-54. 10.1097/MEG.0b013e3282f198a0.