Chapter 9
Machine Learning Techniques to Predict the Inputs in Symmetric Encryption Algorithm

M. Sivasakthi
https://orcid.org/0000-0001-9828-8046
SRM Institute of Science and Technology, India

A. Meenakshi
SRM Institute of Science and Technology, India

ABSTRACT

Applying machine learning algorithms for encryption problems is reasonable in today's research connecting with cryptography. Using an encryption standard such as DES can give insight into how machine learning can help in breaking the encryption standards. The inspiration for this chapter is to use machine learning to reverse engineer hash functions. Hash functions are supposed to be tough to reverse one-way functions. The hash function will be learned by machine learning algorithm with a probability of more than 50%, which means the can develop their guesstimate of the reverse. This is concluded by executing the DES symmetric encryption function to generate N numerous values of DES with a set key and the machine learning algorithm is trained on a neural network to identify the first bit of the input based on the value of the function's output. Testing has ended through a new table, which was created similarly but with different inputs. The SVM runs on the new table, and it compares to the other table, and a confusion matrix is used to measure the excellence of the guesstimates.

INTRODUCTION

Our daily lives are now infinitely more accessible due to the widespread use of numerous electronic devices in the "information age." Because cryptographic algorithms can provide important insights into how cryptographic systems function internally, there has been a concern to device security (Ouladj & Guilley, 2021). Side-channel analysis is a valuable technique for identifying and resolving potential problems with improving safe cryptography systems (Cui et al., 2023).

DOI: 10.4018/979-8-3693-1642-9.ch009

A process known as encryption involves securing the document's or data's validity by employing an algorithm to jumble its contents and render them unintelligible to anybody without authorization to access them. Any kind of data, including messages and documents, can be encrypted and transformed into codes or ciphers. This is to stop unauthorized users from accessing any data, documents, or other material. By changing the data into some unintelligible code, it hides the information (Digital Guardian, n.d.). The process that entails reading the "un-readable code" is called decryption. By deciphering the encryption technique, it translates the message for the reader. The process of decrypting cipher text back into plaintext is known as decryption; symmetric encryption is employed for encrypting larger amounts of data (VTSCADA, n.d.). Data is scrambled using an algorithm during encryption to make it unreadable, and the reverse process is used during decryption to restore the data's readable state. Data is scrambled (or encrypted) using an algorithm in encryption, and the information is subsequently unlocked or decrypted using a key (Sectigostore, n.d.). The application layer is where encryption and decryption take place (Tutorialspoint, n.d.).

Encryption methods are an essential part of applications involving cryptography. Encryption provides security and protects communication channels. Encryption and decryption are tools for cybersecurity procedures, especially those related to servers and applications utilized for data or message transit. By verifying keys from the person supplying the message or data through an application or server, encryption protects the data or document being provided by transforming it into unreadable code that no one without a key can comprehend. Information is changed by data encryption so that only those with a secret key—also referred to as a password or decryption key can read it. Data that has been encrypted is called plaintext or ciphertext. You will need the decryption key in order to decrypt an encrypted message, document, or piece of data and return it to a readable format. Encryption is necessary for security-related contacts with law enforcement and the military since the data may still contain sensitive or private information. Similar to the encryption procedure, the decrypted result is the output and the document is the decryption input. It is encrypted text that cannot be deciphered, or ciphertext.

It is impossible to decode the data or determine the message's intention without a means of deciphering the ciphertext. Selecting a safe encryption technique is crucial to preventing easy data decoding. Security issues could be jeopardized in the absence of a reliable and secure encryption technique. When someone receives data or a document from the sender, they can use a private key to decrypt it and decode it. One instance would be sending a PDF document with a passcode along with an email message. To open the document, the recipient or the email message must know the passcode. Since the recipient's email address is public knowledge and should only be shared with the sender and recipient of the message, the passcode serves as an example of a private key. One frequently asked question is what the distinction is between public and private keys, as well as the kind of encryption technique to use. Both the sender and the recipient of encrypted data share a private key that is used to encrypt and decode the data. The public key is exchanged and is always kept private, while the private key is kept hidden.

Adding an additional layer of encryption using an attacker's key is the most popular method of hacking encrypted data. The private key that is used to encrypt a communication is required in order to decrypt it (Open.edu, n.d.). Numerous encryption techniques exist, each with its own unique style. The difference between symmetric and asymmetric encryption is one illustration. Asymmetric encryption employs a public key for encryption and a private key for decryption, whereas symmetric encryption uses a single key for both operations (Dataoverhaulers, n.d.).

Hashing, symmetric, and asymmetric encryption are all possible methods for protecting our data. To encrypt and decrypt data, the symmetric encryption method employs a single key. Triple Data Encryp-