Chapter 1
Introduction to Modern Cryptography and Machine Learning

Preeti Mariam Mathews
MIT Mahaguru Institute of Technology, India

Anjali Sandeep Gaikwad
Bharati Vidyapeeth, India

Mathu Uthaman
Mahaguru Institute of Technology, India

B. Sreelekshmi
Mahaguru Institute of Technology, India

V. Dankan Gowda
https://orcid.org/0000-0003-0724-0333
BMS Institute of Technology and Management, India

ABSTRACT

Cryptography and machine learning are part of mega-tech today. The whole of this chapter is about digital currencies. This is what will happen in the encryption world. First, the authors show how to use PMBeast-1 for something and then later on with bitcoin cryptography where information privacy is concerned. The objective of cryptography is to make data impossible for a human eye by encryption so that only someone in possession of the secret key can determine their length. Yet cryptography is ancient. But actually, it's only within the last few hundred years that their methods and purpose have completely changed. Later parts of this chapter review some recent advances in areas such as symmetric and asymmetric encryption, public-key infrastructure (PKI), and cryptographic hashes. In this way, information becomes one's tutor—machine-like learning. The only difference is that we want these next-generation machines to understand the process of machine learning so as to enhance encryption systems.

DOI: 10.4018/979-8-3693-1642-9.ch001

1. INTRODUCTION

In an era of technology so advancing by the nano-second that it is known as cutting edge only if you have a single letter hanging off it somewhere--the age itself seems to be mutating into a technical one. But among all this change two fields enjoy ascendancy over everything else; each field wields its power and potential according to its own particularity. The twin foundations that are transforming our digital world, machine learning (a technical subfield of artificial intelligence in which a computer does discoveries and creates new facts) lets the Internet learn from itself; cryptography is an age-old discipline for encrypting information. Their convergence represents a nexus of innovation and transformation, with profound implications for the realm of cybersecurity and beyond. In this chapter, we will explore the vast landscape of machine learning and the complex web of contemporary encryption. Our mission is twofold: to unravel the essential concepts and techniques that underlie these fields and to illuminate the extraordinary synergy that emerges at their intersection.

Cryptography and Cryptanalysis are two subfields of cryptology, the field that studies cryptosystems generally (Figure 1). The art and science of cryptography come together to build cryptosystems, which provide strong protection for sensitive data (M. N. Reza, and M. Islam, 2021). This field revolves around the practical aspect of safeguarding digital data, involving the design and implementation of mechanisms based on mathematical algorithms. These mechanisms serve as the foundation for essential information security services, effectively forming a versatile toolkit for security applications. In parallel, Cryptanalysis serves as the complementary counterpart to Cryptography within the realm of cryptology. While cryptography generates ciphertext for secure transmission or storage, cryptanalysis is concerned with the analysis and potential decryption of these cryptographic systems. Cryptanalysts study cryptographic mechanisms with the aim of breaking them, revealing vulnerabilities, and identifying weaknesses (Kumar, Pullela SVVSR, & Chaturvedi, Abhay, 2023). Additionally, cryptanalysis plays a crucial role in the development of new cryptographic techniques by rigorously testing their security strengths and assessing their resilience against potential attacks. These two branches, cryptography and cryptanalysis, coexist in the ongoing quest for information security and encryption advancements.

Figure 1. Context of cryptology