

# A Study on Cryptography

Rishab V<sup>1</sup>, Sachin<sup>2</sup>, Sagar S Yadrami<sup>3</sup>, Shamjetshabam Noren Singh<sup>4</sup>, Partha Sarathi Pati<sup>5</sup>

Students, Department of Computer Science and Engineering<sup>1,2,3,4</sup>

Sr. Assistant Professor, Department of Computer Science and Engineering<sup>5</sup>

Alva's Institute of Engineering and Technology, Mangalore, India

**Abstract:** *With the internet having reached a level that merges with our lives, growing explosively during the last several decades, data security has become a main concern for anyone connected to the web. Data security will ensure that our data is only accessible by the intended receiver and prevents any modification or alteration of data. In order to achieve this level of security, various algorithms and methods have been developed. High-assurance cryptography leverages methods from program verification and cryptography engineering to deliver efficient cryptographic software with machine-checked proofs of memory safety, functional correctness, provable security, and absence of timing leaks. Traditionally, these guarantees are established under a sequential execution semantics. However, this semantics is not aligned with the behavior of modern processors that make use of speculative execution to improve performance. This mismatch, combined with the high-profile Spectre-style attacks that exploit speculative execution, naturally casts doubts on the robustness of high-assurance cryptography guarantees. Cryptography can be defined as techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender.*

**Keywords:** Cryptography.

## REFERENCES

- [1] FIPS 197, Advanced Encryption Standard, National Institute of Standards and Technology, US Department of Commerce, WashingtonD. C.,2001
- [2] Research on Various Cryptography Techniques Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi
- [3] Review and Analysis of Cryptography Techniques Nitin Jirwan, Ajay Singh, Dr. Sandip Vijay
- [4] Chandra M. Kota et al., "Implementation of the RSA algorithm and its cryptanalysis," In proceedings of the 2002 ASEE Gulf-Southwest Annual Conference, March 20 – 22, 2002
- [5] R. GENNARO, "IEEE Security & Privacy," IEEE Security & Privacy, vol. 4, no. 2, pp. 64 - 67, 2006
- [6] Cryptographic Hash Functions: A Review Rajeev Sobti 1, G.Geetha2 1 School of Computer Science, Lovely Professional University Phagwara, Punjab 144806, India 2 School of Computer Applications, Lovely Professional University Phagwara, Punjab 144806, India.