# Letscrypt 2.0 Protocol Intro Spec

## Smart Contract Layer (LENS.sol)

The LENS.sol smart contract acts as the backbone of the Lenscrypt protocol, enabling decentralized and secure transactions on the Rootstock TestNet.

## User Data Module (UDM)

The UDM module contains ENCRYPTED SCORE and ENCRYPTED REPORT data structures, which store the encrypted credit scores and reports of users on the blockchain.

## Encryption Techniques

512 bit RSA encryption is the first component of a double-encryption process that prioritizes security, speed, and storage efficiency on the blockchain.

There is also a symmetric encryption layer given to vendors, using AES-256-CBC encryption, which allows vendors to access user data with a unique access key.

## Decryption Techniques

When data is requested by an approved vendor or user, the Lenscrypt Protocol uses a two-step decryption process. First, the users private and public keys and used to perform the asymmetric decryption of the data. Then, the vendor's access token is used to perform the second symmetric decryption of the data.

# Security

Based on the double-encryption process, Lenscrypt performs a unique method of holding encrypted data and history on the blockchain. Thus, the information is immutable, verifiable, and does not depend on a centralized authority.

In conclusion, the Lenscrypt Protocol is a secure, decentralized, and efficient method of storing and accessing user data on the blockchain. It is a significant advancement in the field of decentralized finance and data security, and it has the potential to revolutionize the way we think about data privacy and security and trust.