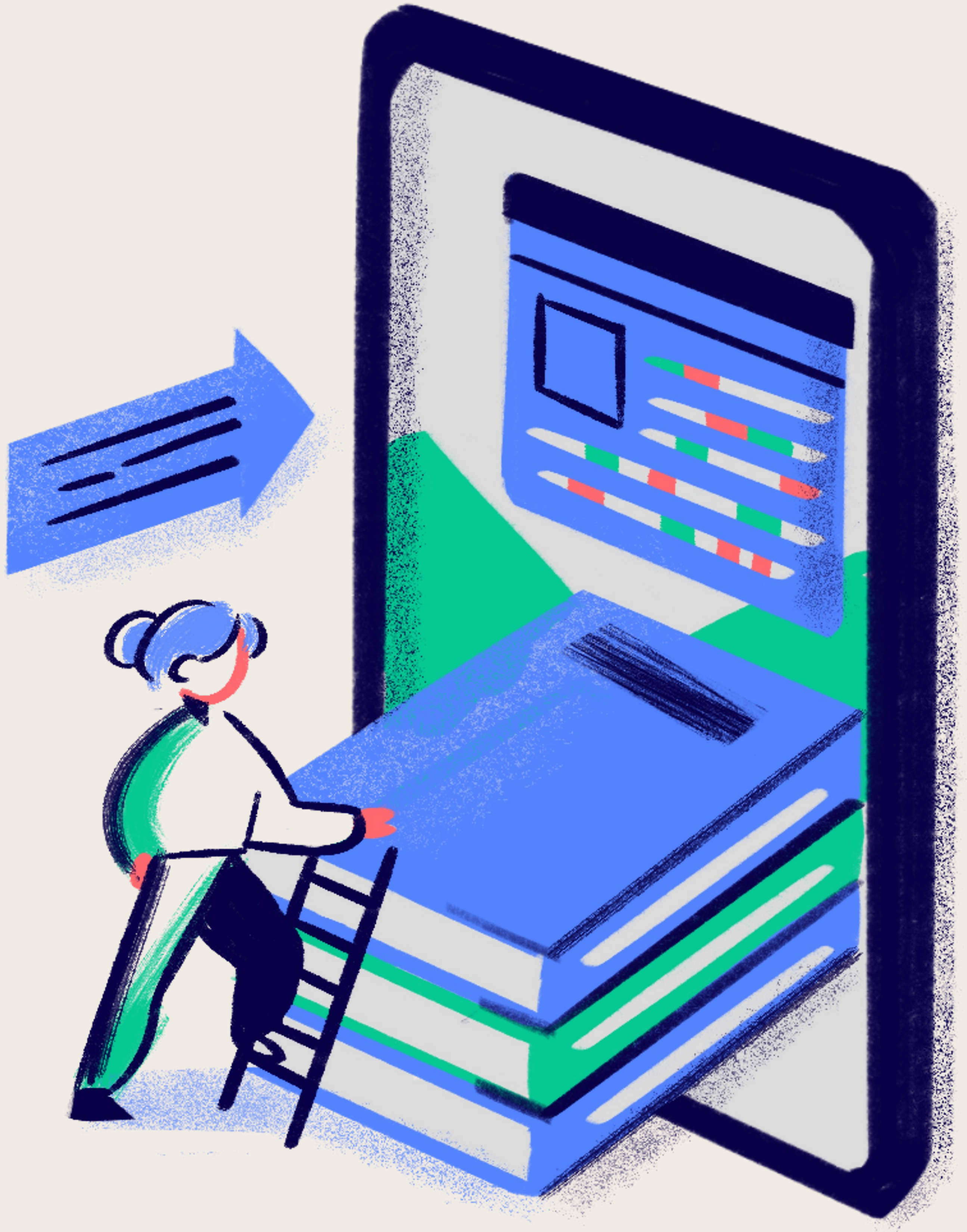
Local Secure: A Secure File Management System

CMSC 334 Computer Security Final Project

Presented by Sophie Zhao & Maggie Song



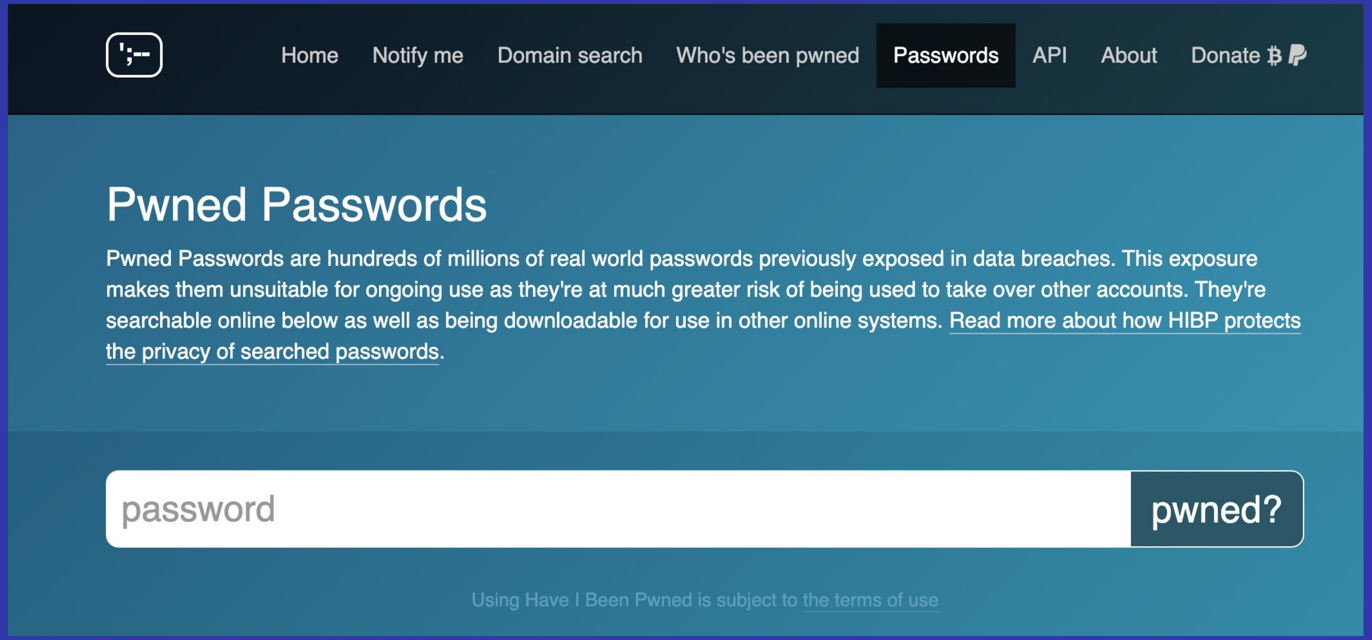
Problem to Address

- Individuals and organizations are **increasingly vulnerable to data breaches and unauthorized access**
  - According to a report published by the **Identity Theft Resource Center (ITRC),** a record number **of 1862 data breaches** occurred in 2021 in the US; this number broke the previous record of 1506 set in 2017 and represented **a 68% increase** compared to the 1108 breaches in 2020
  - The **average cost** of a data breach for organizations globally is **$3.86 million**, according to the IBM Cost of a Data Breach Report 2020

- We want to help users secure their files by encrypting and decrypting a diverse range of file types
  - If someone steals your computer or gains access to your encrypted files without the correct passwords, **they will be unable to decipher the encrypted data!**

Strong Password

A common password repository with the top 100,000 passwords from the Have I Been Pwned dataset to verify against any common passwords



Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

Using Have I Been Pwned is subject to the terms of use

and

Same Key Enforced

Users must use the same password to encrypt and decrypt

Different File Types to Handle

We categorize files into the following categories with different encryption and decryption strategies

01. Text Document:
Salt + AES & CBC

02. PDF Document:
Salt + PyPDF2

03. Multimedia (Image, Audio, and Video):
Salt + Fernet

Main Encryption Approaches

Salt

An additional input to the encryption process

AES & CBC

An AES cipher in CBC mode with the provided key

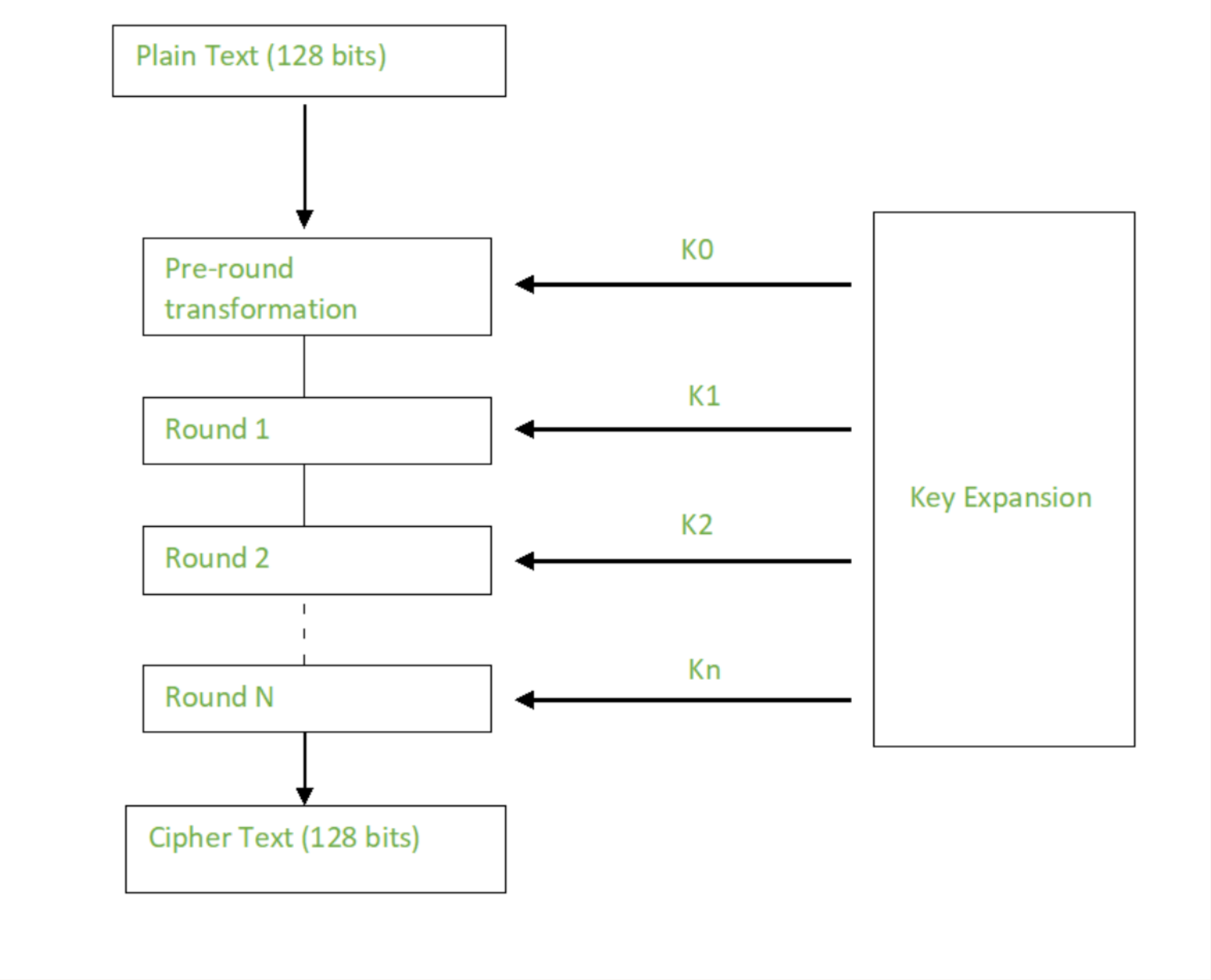
PyPDF2

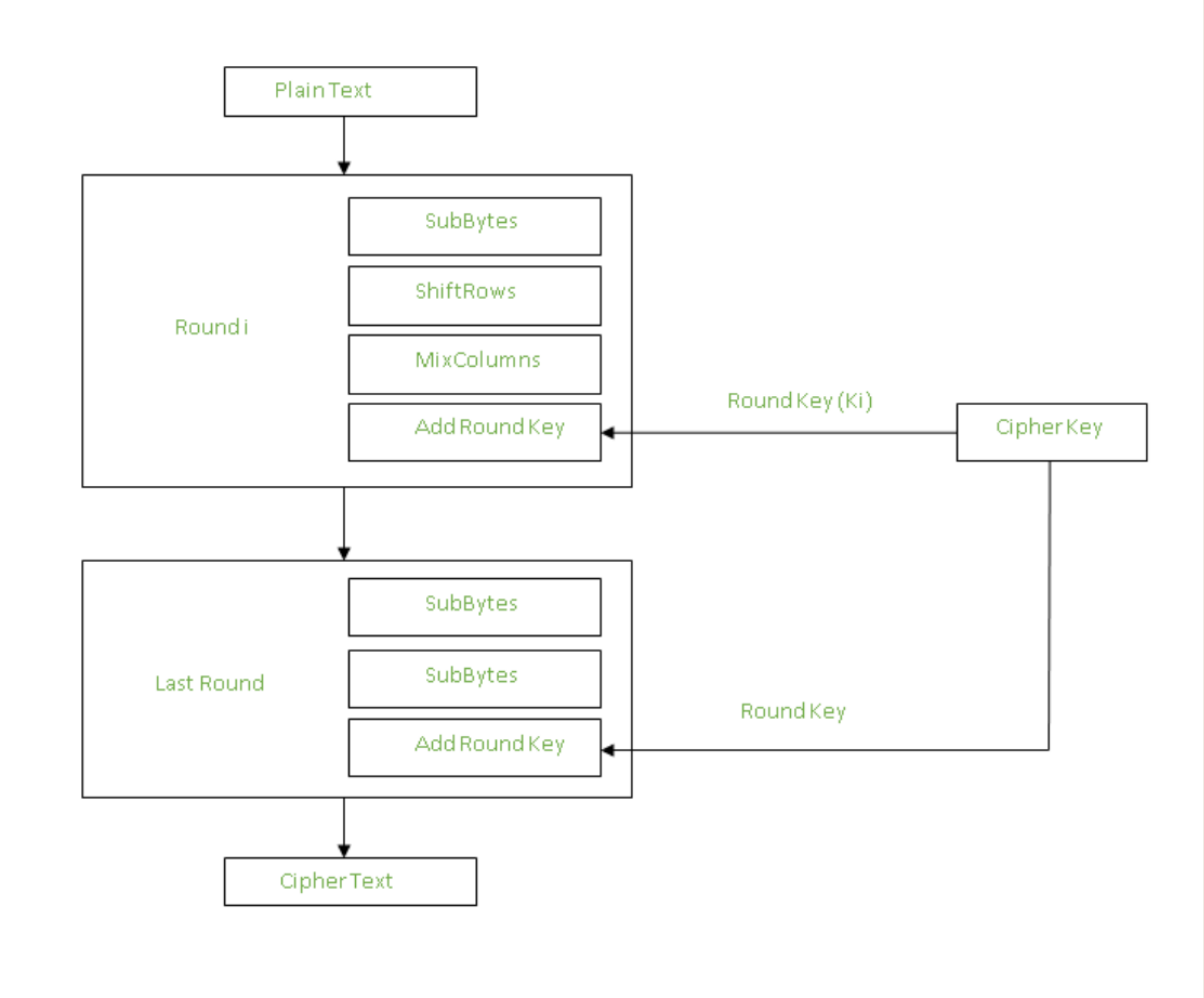
A Python library for working with PDF files, using RC4 algorithm

Fernet

A symmetric encryption algorithm introduced in the cryptography library in Python

AES


Plain Text (128 bits)
Pre-round transformation
Round 1
Round 2
Round N
Cipher Text (128 bits)
K0
K1
K2
Kn
Key Expansion


Plain Text
Round i
SubBytes
ShiftRows
MixColumns
Add Round Key
Round Key (Ki)
Cipher Key
Last Round
SubBytes
SubBytes
Add Round Key
Round Key
Cipher Text

DEMO!

Thank You Very Much!

Presented by Sophie Zhao & Maggie Song