

# Hashword - Cryptographic Password Manager & Generator

---

Project By: Cieara Pfeifer, Jayden Stearns, & Jarrett Woo

CS-47206: Data Security and Privacy

November 15, 2021

# Passwords - A Brief Background

---

# Password History (Past & Present)

- Passwords were invented in the 1960's
  - Originally used to meter time on shared mainframe computers
- Most common passwords are variants of '123456'
- 91% of people say they know not to reuse passwords, but 66% say they do anyway
- The average person has 191 passwords

# Password Security (Past & Present)

- For login verification, services must store passwords in some way .
  - Storing in plain-text is simple, but very unsafe
- The main method to secure passwords is 'hashing'
  - Using a one-way encryption algorithm
  - In 1979, security was improved by adding 'salt' to the hashes
- Users must trust that the service will:
  - hash the password at all
  - use a secure encryption algorithm

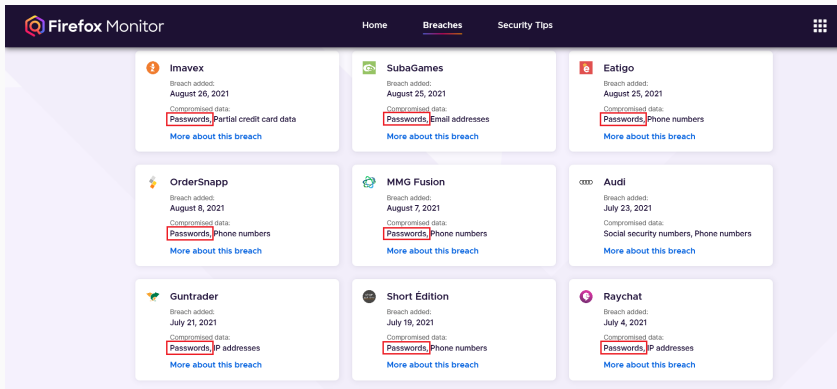
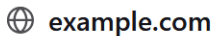


Figure 1: Firefox Monitor Report of Recent Database Breaches

# Password Managers

Password Managers can solve many issues with password security, but may also introduce new issues:

- Many simple password managers store passwords locally in plain-text
  - Single-system access to breach many services at once
- Password 'generators' create very strong passwords, but with little relationship to the user
  - Difficulty synchronizing passwords across platforms



Website address


<https://www.example.com>

Username

ExampleUsername

Copy

Password

ExamplePassword 

Copy

**Figure 2:** In-browser Password Manager - One-click Visibility

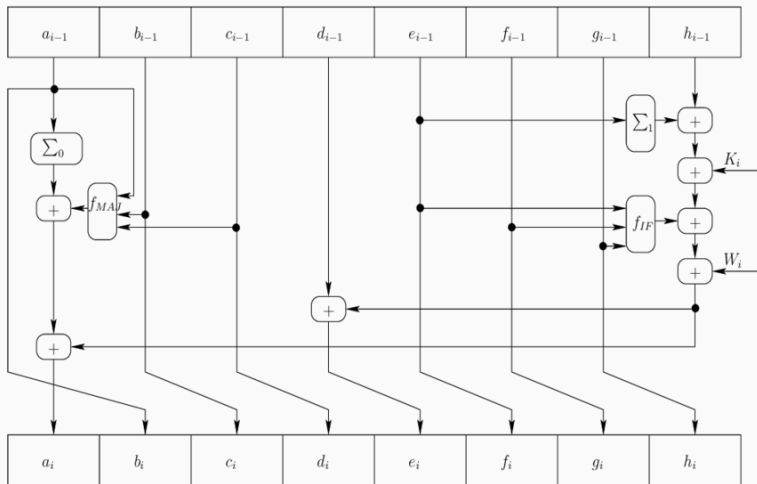
# Hashing - Overview

---



# Hashing - Fundamental Features

- One-way transformation
  - Neither 'Symmetric' nor 'Asymmetric' encryption
  - Non-reversible
- Same input always results in the same output
- Minor change in input = major change in output
- Large enough 'key space' for algorithm security



**Figure 3:** One Round of the SHA-256 algorithm.  
Note basic operations of Addition, XOR, Bitwise Shift, etc.

# Hashing - Differences from Other Encryption

- Designed to *not* recover the original information
- Only input given is the data to hash
  - No 'key' is needed
- Input of any length gives output of a fixed length
  - Ex: SHA-256 always outputs 256 bits

## Our Solution - Hashword

---

# Hashword Overview

- No plain-text password data ever stored
  - Only necessary service information is saved
- User's choice from many secure cryptographic hash functions
  - Ex: SHA-256, BLAKE2, SHA3-512, etc.
- A focus on secure memory management
- The resultant service passwords themselves are cryptographic hashes

# Hashword Implementation

- GitHub
- Python 3
  - hashlib
  - getpass
  - pyperclip

# Service Information File

The little information that is stored uses a 'ServiceData.dat' file:

- Uses a simplified, JSON-like format
- New services can be 'registered' to the file easily through the program
  - Information stored: service name and the maximum password length
- No information within can determine individual service passwords
  - Can be stored in plain-text without issue

```
1 hash:sha256
2 master:ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
3 Zoom:32
4 Gmail:64
5 Amazon:40
6 GitHub:96
7
```

**Figure 4:** Example of a Service Information File



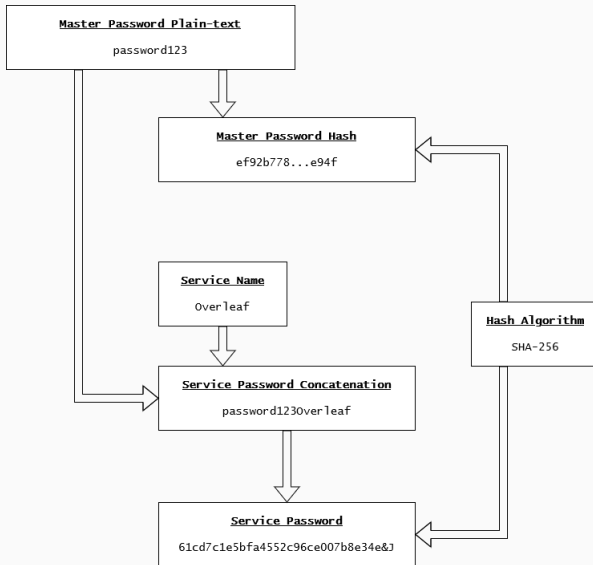


Figure 5: Outline of Data Flow and Hash Construction

# Future Improvements

- Further security improvement by 'salting' the hashes
- Implement System Administrator controls
  - i.e. for easier incorporation into a company's data security policy
- Improve password strength by using custom hash output translation
- Add more types of information to store about services

# References

1. Paar, C., & Pelzl, J. (2010). Hash functions. In *Understanding cryptography: A textbook for students and practitioners* (pp. 293-314). Springer. DOI 10.1007/978-3-642-04101-3
2. Web Desk. (2021, May 18). *The history and future of passwords (and what's next)*. Digital Information World.  
<https://www.digitalinformationworld.com/2020/05/what-comes-after-passwords-infographic.html>

Any Questions ?