Intro to One-way Hash Functions

- Common Hash Function Families
- Hash Function Construction
- Introduce Linux Hash Commands

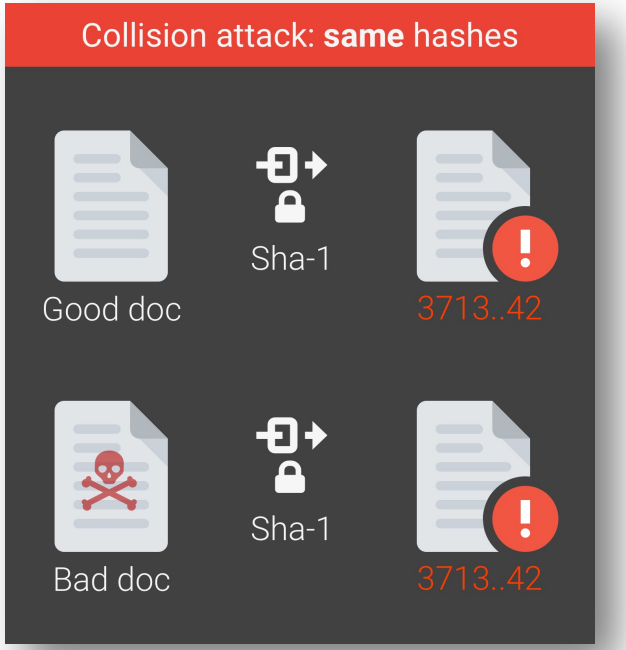
The MD One-Way Hash Functions

- Message Digest
  - Developed by Ron Rivest
  - Produces 128-bit hashes
  - Includes MD2, MD4, MD5, and MD6

- Status of Algorithms:
  - MD2, MD4 - severely broken (obsolete)
  - MD5 - collision resistance property broken; one-way property not broken
    - Often used for file integrity checking
    - No longer recommended for use!
  - MD6 - developed in response to proposal by NIST
    - Not widely used…

The SHA One-Way Hash Functions

- Secure Hash Algorithm
  - Published by NIST
  - Includes SHA-0, SHA-1, SHA-2, and SHA-3

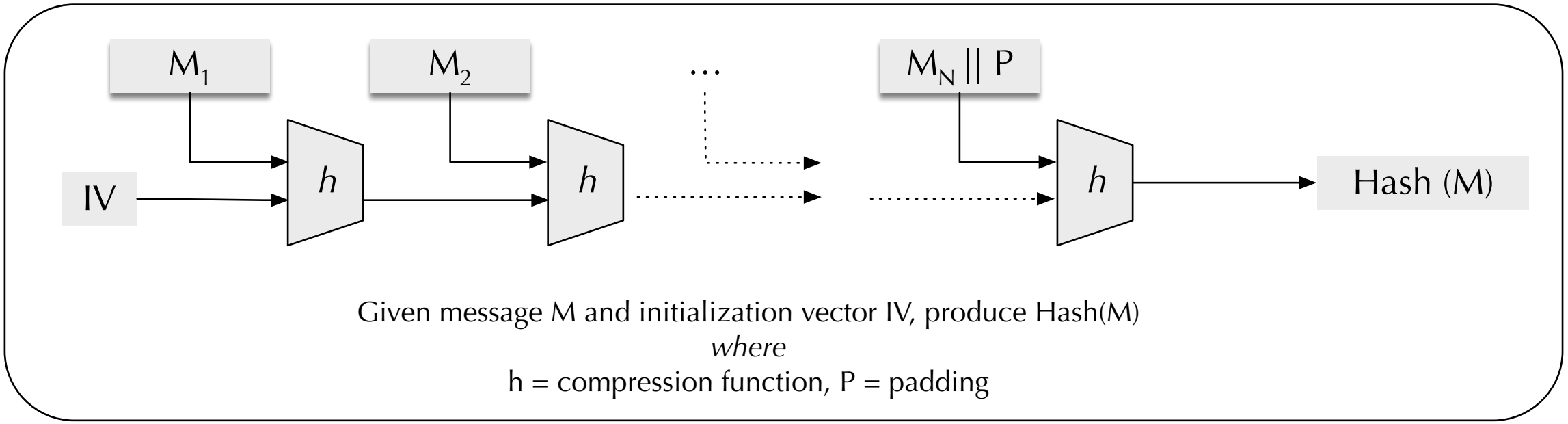


https://shattered.it

- Status of Algorithms:
  - SHA-0: withdrawn due to flaw
  - SHA-1: Designed by NSA Collision attack found in 2017
  - SHA-2: Designed by NSA
    - Includes SHA-256 and SHA-512 + other truncated versions;
    - No significant attack found yet…
  - SHA-3: Not Designed by NSA
    - Released in 2015; not a replacement to SHA-2, but meant to be a genuine alternative
    - Has different construction structure ("Sponge Function") as compared to SHA-1 and SHA-2

How (Most) One-Way Hash Algorithms Work

Most hash algorithms (e.g., MD5, SHA-1, SHA-2)
use a **Merkle-Damgard** construction:



Davies-Meyer compression function uses a block cipher to construct a compression function

(e.g., SHA family uses this compression function)

Others are possible too…

One-Way Hash Commands

Linux utility programs: md5sum, sha256sum, sha512sum, openssl *, etc.

```
$ md5sum print_array.c
aef3a2cac2b4153b9b5a9ff702892e12  print_array.c
$ sha256sum print_array.c
d7653b35b8c37423c6a70852dc373a3e3b2873feab6d19d9d8899eb0e2b5fce0  print_array.c

$ openssl dgst -sha256 print_array.c
SHA256(print_array.c)= d7653b35b8c37423c6a70852dc373a3e3b2873feab6d19d9d8899eb0e2b5fce0
$ openssl sha256 print_array.c
SHA256(print_array.c)= d7653b35b8c37423c6a70852dc373a3e3b2873feab6d19d9d8899eb0e2b5fce0

$ openssl dgst -md5 print_array.c
MD5(print_array.c)= aef3a2cac2b4153b9b5a9ff702892e12
$ openssl md5 print_array.c
MD5(print_array.c)= aef3a2cac2b4153b9b5a9ff702892e12
```

There is also support for hashing commands in C (openssl/sha.h), C++, Python, SQL, PHP, etc.

```
$ python -c "import hashlib; print hashlib.md5('hello').hexdigest();"
```