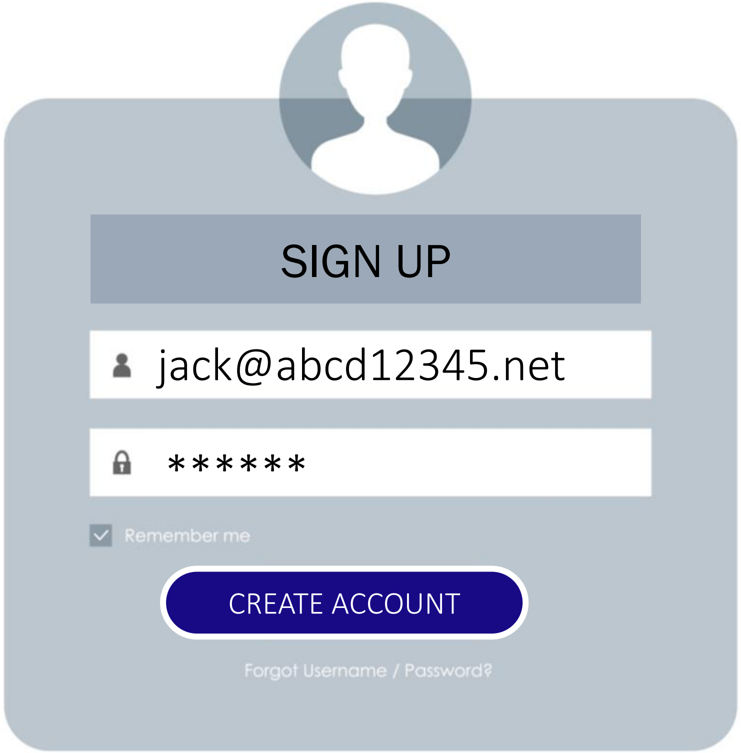
Web & Mobile Security: Test Drive

CRYPTOGRAPHIC HASH FUNCTIONS

An example **use case** to establish a **context**



SIGN UP

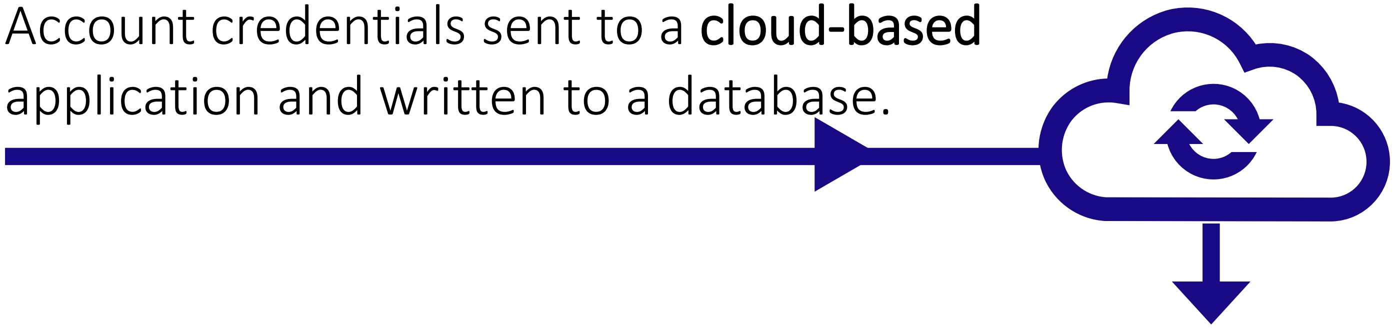
jack@abcd12345.net

******

☑ Remember me

CREATE ACCOUNT

Forgot Username / Password?



Account credentials sent to a **cloud-based** application and written to a database.

CHECK DATABASE RECORD

UserID	jack@abcd12345.net
Password	5c4bf758b3e4a924c49c4cd683cc638b

The password is NOT stored in plaintext.
It is stored as a **cryptographic hash** of the plaintext

HASH: 5c4bf758b3e4a924c49c4cd683cc638b

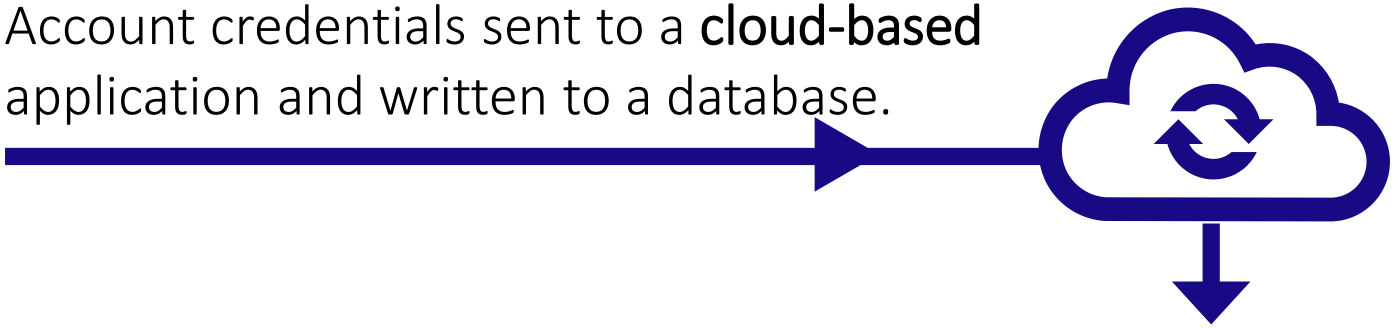
An example **use case** to establish a **context**

QUESTION?

Why is the password stored as a **hash** and not as **plaintext**?

ANSWER...Confidentiality

If the database is compromised, a malicious adversary would need to reverse the hash in order to find the original password.



Account credentials sent to a **cloud-based** application and written to a database.

CHECK DATABASE RECORD

UserID	jack@abcd12345.net
Password	5c4bf758b3e4a924c49c4cd683cc638b

The password is NOT stored in plaintext.
It is stored as a **cryptographic hash** of the plaintext

HASH: 5c4bf758b3e4a924c49c4cd683cc638b

What is a Cryptographic Hash Function

- ✓ A **mathematical algorithm**

- ✓ Takes **data** of any **size as an input**

  (e.g., text, file, document, image, video, music etc.)

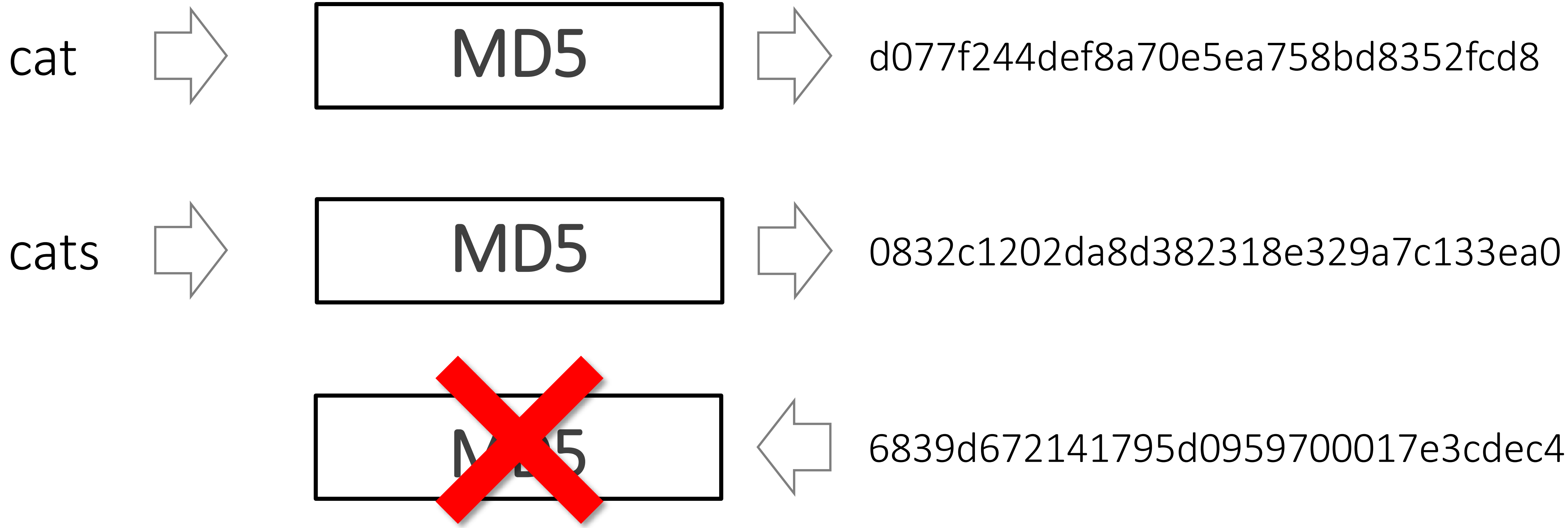
- ✓ **Maps** it to a **fixed size** hexadecimal **output**...a **hash**.

What is a Cryptographic Hash Function

INPUT based on text example

HASH FUNCTION ALGORITHM
(One Way & Deterministic)

OUTPUT is called a HASH
Has a fixed length: (e.g. MD5: 16 bytes=32 hex values=128 bits)



cat → MD5 → d077f244def8a70e5ea758bd8352fcd8

cats → MD5 → 0832c1202da8d382318e329a7c133ea0

~~MD5~~ ← 6839d672141795d0959700017e3cdec4

What is a Cryptographic Hash Function

INPUT based on text example

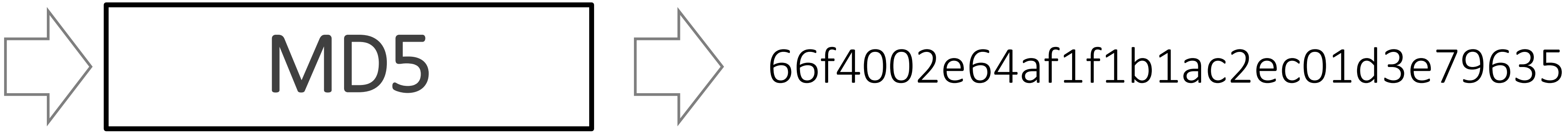
HASH FUNCTION ALGORITHM

OUTPUT is called a HASH
Has a fixed length: (32 bytes = 64 hex values = 256 bits)

Yesterday, upon the stair,
I met a man who wasn't there!
He wasn't there again today,
Oh how I wish he'd go away!

When I came home last night
at three
The man was waiting there for
me
But when I looked around the
hall,
I couldn't see him there at all!
Go away, go away, don't you
come back any more!
Go away, go away, and please
don't slam the door...

Last night I saw upon the stair,
A little man who wasn't there,
He wasn't there again today
Oh, how I wish he'd go
away....



MD5

66f4002e64af1f1b1ac2ec01d3e79635

Source:
https://en.wikipedia.org/
wiki/Antigonish_(poem)

What are the essential characteristics of a Cryptographic Hash Function

1. It is **one-way**. It is computationally impractical to reverse the hash back to the original input.

2. It is **deterministic**. The same input always results in the same hash

3. It **performs efficiently** (typically milliseconds). However, bigger the input…slower the process.

What are the essential characteristics of a Cryptographic Hash Function

4

A **unique input** should always result in a **unique hash**. Therefore, two separate inputs should never result in the same hash result.

5

A **a small change** to an input should result in a **non-deterministic hash as an output**. For example, the hash for “cat” and “cats” should vary, such that they appear to be random.

What are Cryptographic Hash Functions used for

- ✓ Protecting passwords
- ✓ Validating integrity (i.e. that data has not been modified)
- ✓ Blockchain technologies (foundation of cryptocurrencies)
- ✓ Digital signatures, as cryptographic keys and much more!

There are many cryptographic hash function algorithms

- Haval
- MD5
- RipeMD128
- RipeMD160
- SHA-1
- SHA-256
- SHA-384
- SHA-512
- Snefru
- Tiger
- Whirlpool-0
- Whirlpool-T

See examples at https://www.fileformat.info/tool/hash.htm

Road test a cryptographic hash function for yourself…

1) Visit one of the following links:

   https://passwordsgenerator.net/md5-hash-generator/

   https://codebeautify.org/md5-hash-generator

2) Type in: Roehampton

   What is the hash that was returned?

Road test a cryptographic hash function for yourself...

1) Visit one of the following links:

   https://passwordsgenerator.net/md5-hash-generator/

   https://codebeautify.org/md5-hash-generator

2) Type in: roehampton (lowercase r)

   What is the hash that was returned?

An example use case for rainbow table attacks

SIGN UP

jack@abcd12345.net

******

☑ Remember me

CREATE ACCOUNT
Forgot Username / Password?

Account credentials sent to a **cloud-based** application and written to a database.

CHECK DATABASE RECORD

UserID	jack@abcd12345.net
Password	5c4bf758b3e4a924c49c4cd683cc638b

The original plaintext is only **6 characters** and is likely to be a weak password. Therefore this hash is vulnerable to a **rainbow table attack**.

Road test a rainbow table attack for yourself…

1) Visit https://www.whatsmyip.org/hash-lookup/

2) Copy and paste the following hash:
   5c4bf758b3e4a924c49c4cd683cc638b
   Recall that this is the **hash of the password** submitted by our user jack@abcd12345.net

3) Click the "**Reverse Hash**" button.
   What is the plaintext that Jack used as a password?
   Paste your answer in the chat window

Some information about rainbow tables

ℹ Rainbow tables are collated by enthusiasts who are motivated to match a **hash to original plaintext input**.

ℹ Attackers use rainbow tables to **discover weak passwords**, even if they have been cryptographically hashed.

ℹ A rainbow table attack can be mitigated if a **password** is of a **sufficient complexity**.

A summary of this Web & Mobile Security preview session

In this session we have:

- **Previewed** a Web & Mobile Security module
- **Contextualised** a use case for a cryptographic hash function
- **Defined** what a **cryptographic hash function** is and its **essential characteristics**.
- **Road tested SHA-256** hash functions
- **Utilised a Rainbow Table** to identify a weak password.