SHA-256 in Practice: Zoom Meetings

Zoom URLs

https://duke.zoom.us/j/9192718156?pwd=WG8wamRsdlpPVDlEdUxIajlVTllpdz09

- Vanity URL
- Meeting ID
- Password Hash
  - Zoom’s hashing algorithm for creating the password is kept secret for security purposes
  - Generated from a password and other static parameters

SHA-256 in Practice: Creating a Meeting

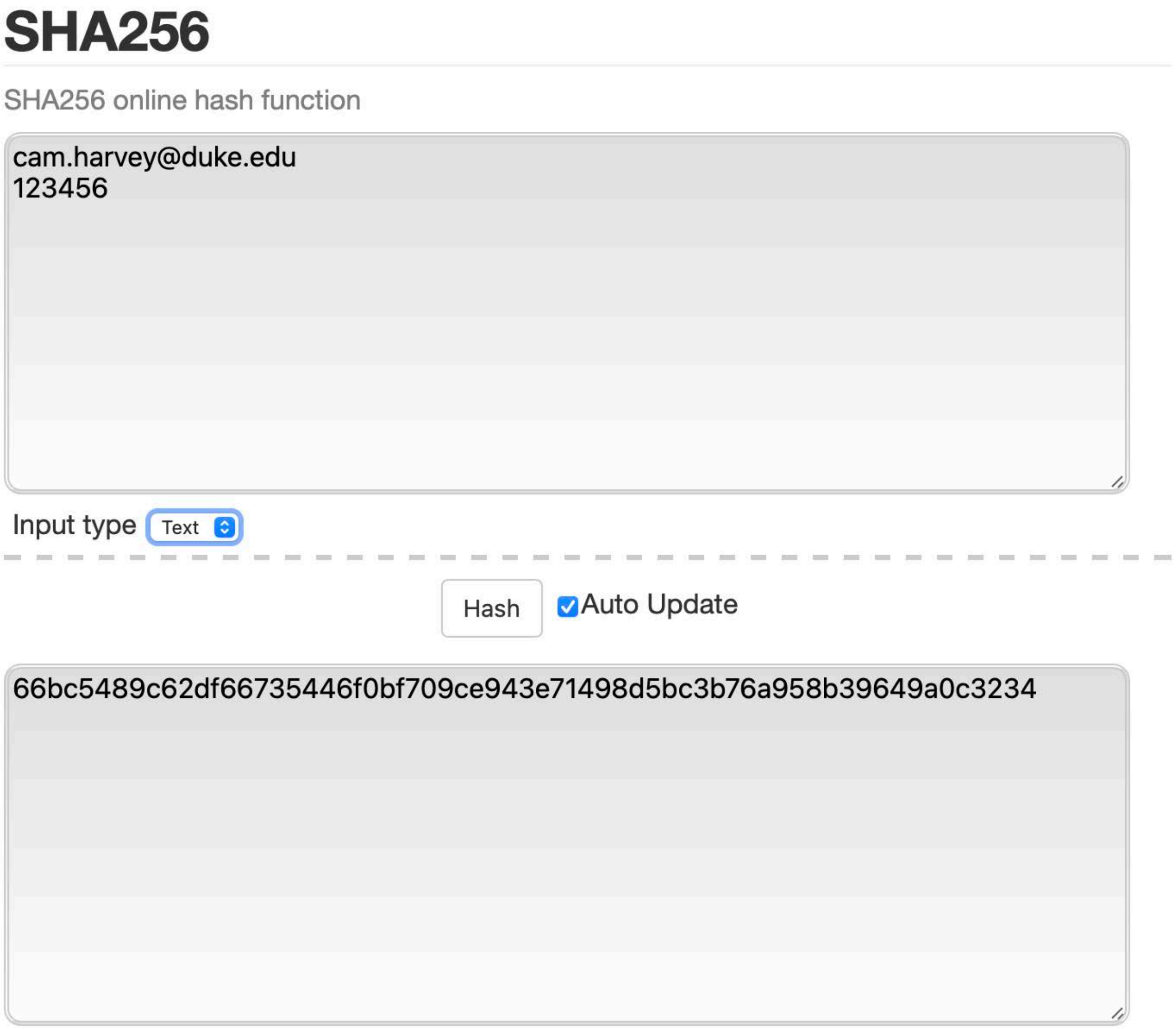
Parameters

- Creating a password hash for a recurring meeting requires static parameters
- For purposes of our example, we will use my username (cam.harvey@duke.edu) and a passcode (123456)

SHA-256 in Practice: Creating a Meeting

Hashed Parameters

- The hashed username and password can be easily duplicated
  - 10^6 tries needed to create the same Hash
- We will append a random “salt” to provide an extra layer of security



SHA256

SHA256 online hash function

```
cam.harvey@duke.edu
123456
```

Input type: Text

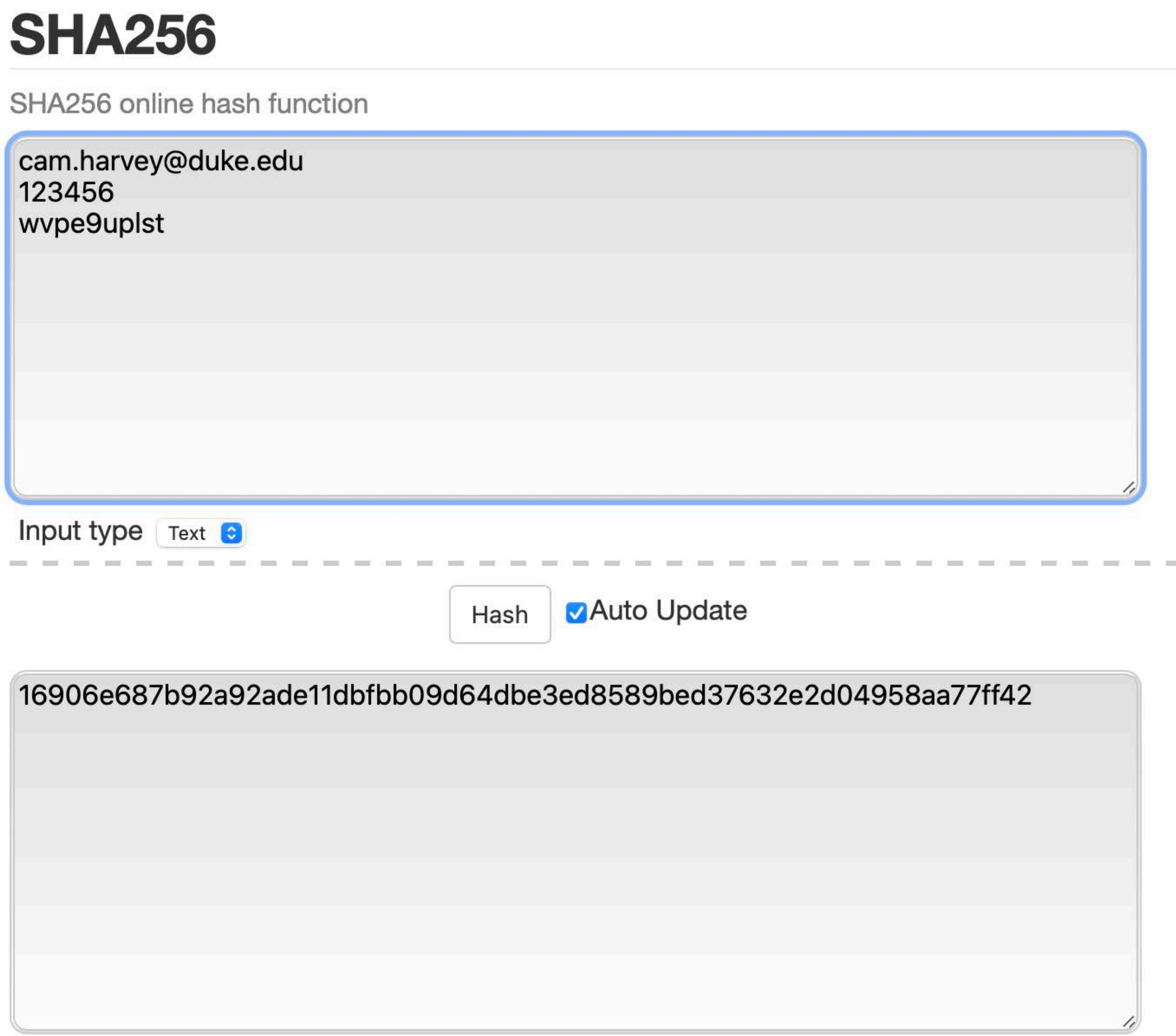
```
66bc5489c62df66735446f0bf709ce943e71498d5bc3b76a958b39649a0c3234
```

https://emn178.github.io/online-tools/sha256.html

SHA-256 in Practice: Creating a Meeting

Base64 Encoding

- We will now Base64 encode our hash
  - Base64 is an encoding scheme that represents data in an ASCII string
  - Consists of upper and lower case letters, 0-9, and 2 additional characters. We use "-" and "_" because they are URL safe
  - Base64 is a more efficient way to represent our hash
    - Base64 uses 6 bits for one character whereas Hex uses 4 bits for one character



SHA256

SHA256 online hash function

```
cam.harvey@duke.edu
123456
wvpe9uplst
```

Input type: Text

```
16906e687b92a92ade11dbfbb09d64dbe3ed8589bed37632e2d04958aa77ff42
```

https://emn178.github.io/online-tools/sha256.html

SHA-256 in Practice: Creating a Meeting

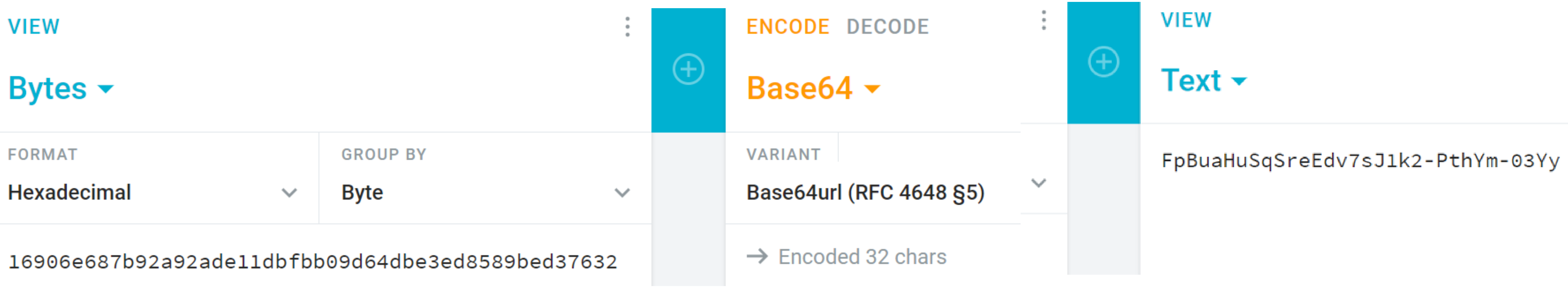
Truncating

- Before we Base64 encode, we will truncate our Hex representation of the hash to 48 characters:
- Truncated hash:

16906e687b92a92ade11dbfbb09d64dbe3ed8589bed37632~~e2d04958aa77ff42~~

- Truncated hash is 192 bits: (=48x4)
- There are 6 bits in every Base64 character. Hence, the encoding is 32 Base64 characters (=192/6)

SHA-256 in Practice: Creating a Meeting



VIEW

Bytes

FORMAT: Hexadecimal

GROUP BY: Byte

16906e687b92a92ade11dbfbb09d64dbe3ed8589bed37632

ENCODE DECODE

Base64

VARIANT: Base64url (RFC 4648 §5)

→ Encoded 32 chars

VIEW

Text

FpBuaHuSqSreEdv7sJ1k2-PthYm-03Yy

- Our meeting is now:
  https://duke.zoom.us/j/9192718156?pwd=FpBuaHuSqSreEdv7sJ1k2-PthYm-03Yy

Campbell R. Harvey 2021

https://cryptii.com/pipes/hex-to-base64

SHA-256 in Practice: Creating a Meeting

- Verification:
  1. Decode Base64 to Hex
  2. Check to see if matches first 48 characters of the SHA-256 of email, passcode plus salt
  3. If yes, meeting opens

https://cryptii.com/pipes/hex-to-base64

Contact: Follow me on LinkedIn

http://linkedin.com/in/camharvey

cam.harvey@duke.edu

@camharvey

SSRN: http://ssrn.com/author=16198

PGP: E004 4F24 1FBC 6A4A CF31 D520 0F43 AE4D D2B8 4EF4