UNIVERSITY OF TWENTE.

Cryptographic hash functions

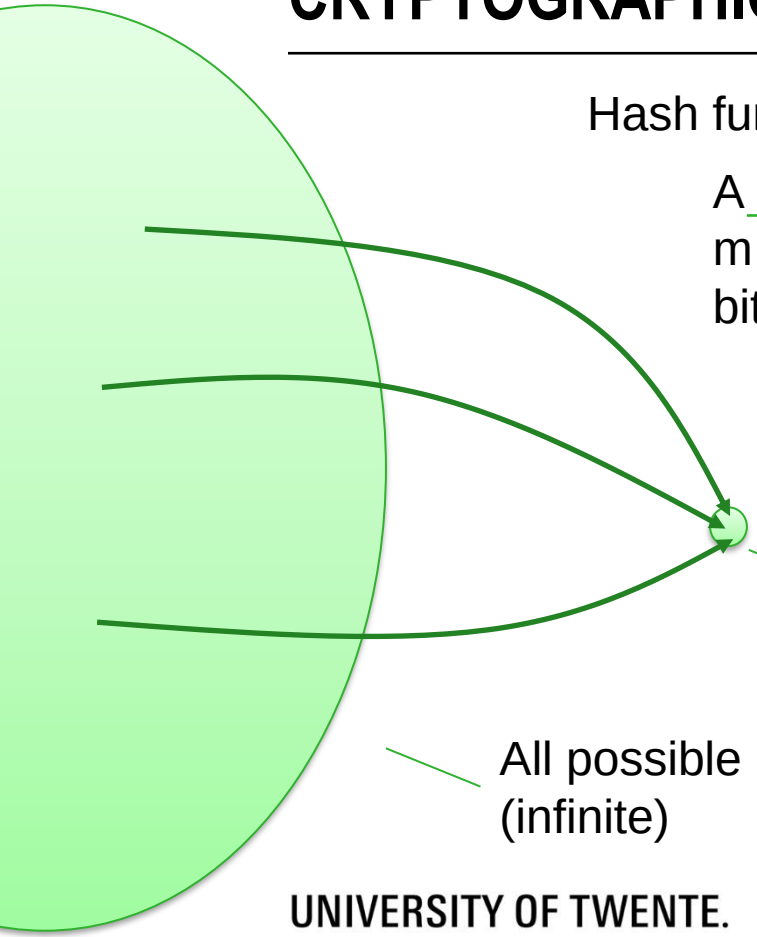
Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts

CRYPTOGRAPHIC HASH FUNCTIONS

Hash function:

A (one-way) function that takes a message m (of arbitrary length) and outputs a bitstring of fixed length.



All possible outputs (finite)

All possible inputs (infinite)

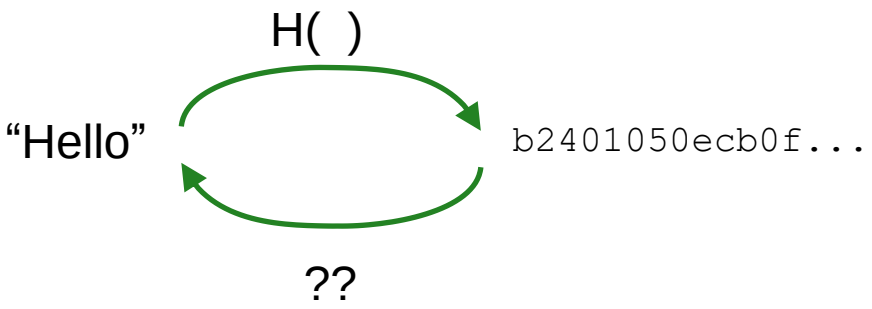
HASH FUNCTION PROPERTIES

A “good” hash has the following properties:

1. One-way
2. Second preimage resistant
3. Collision resistant

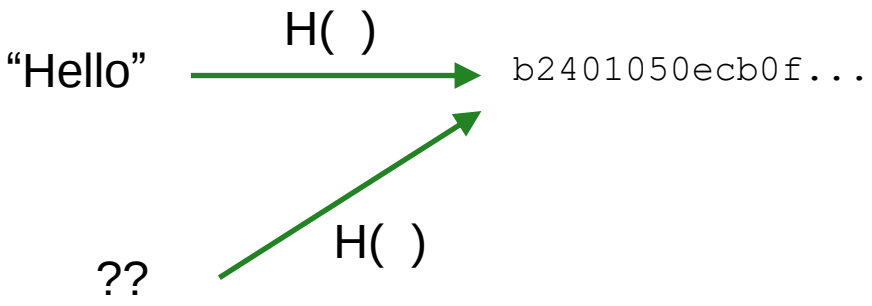
1: ONE-WAY

It is difficult (computationally infeasible) to *invert the hash function.*



2: SECOND PREIMAGE RESISTANT

It is difficult (computationally infeasible) to
find a second input that hashes a given value.



3: COLLISION RESISTANT

It is difficult (computationally infeasible) to
find two inputs with the same hash value.

$$?? \xrightarrow{H(\ )} == \xleftarrow{H(\ )} ??$$

HASH FUNCTION EXAMPLES

SHA1(“Security in Module 2”) ⇨ `bee1d949794fbc27dffec42e20b666ae03eefd65`

hexadecimal representation of the output (message digest)

SHA1(“Security in Module 3”) ⇨ `78e93bc6fc500b0c2a0adba2ba3429503652b6cf`

small change (a few bits)

very different output!

SHA1(“Security in Module 3 and Module 4”)

⇨ `ef2a19599a9b8e8a8715f345ba437c8b268c8202`

length remains the same

HASH FUNCTIONS

MD5	⇨	Broken DO NOT USE! (collisions found)
SHA-1	⇨	Theoretical attacks & more (avoid if possible, will soon be deprecated)
SHA-2 family (e.g., SHA-256)	⇨	Still safe (for now), your best bet
SHA-3	⇨	Recent standard, somewhat ‘unproven’

USES OF HASH FUNCTIONS

Digital signatures — See module 1

HMAC — Coming up

Integrity checks

Content Addressable Storage — Version control, e.g., git

Magnet links:

magnet:?xt=urn:sha1:YNCKHTQCWBTRNJIV4WNAE52SJUQCZO5C

Storing passwords — See assignments P-6.24-30

Commitments — Let's play with that!

HASH FUNCTIONS IN JAVA

```
byte[] inputData = "The data to hash".getBytes();
MessageDigest md = null;
md = MessageDigest.getInstance("SHA-256");
md.update(inputData);
byte[] digest = md.digest();
```

UNIVERSITY OF TWENTE.

Cryptographic hash functions

Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts