Cryptographic Hash Functions

-MD5 & SHA  
Hash Function Uses  
Functions & Passwords  
Message digests/digital signatures  
Proof of work

Deterministic Function  
-Always produces the same output for the ame input  
-Input is an arbitrary length string  
-Output is a fixed-length string

Output seems to be random, but is not actually random at all but deterministic. Same input will always yield the same output

Any change in input (however small) produces a large change in output (Avalanche property)

Collision resistance:  
-Computationally infeasibly to find x,y (x!=y) such that h(x)=h(y)  
Pre-image resistance:  
-Given x it should be computationally infeasible to find x such that h(x)=x’  
Speed:  
-Fast, but not too fast

Pre-image attack:  
Given x’, find x such that h(x)=x’  
-Can be done using brute force  
-Average 2L attempts where L = digest size(bits).

Practical image attacks:  
-Internet search (for published hashes)  
-More specialised methods (rainbow tables)

Common hash Algorithms  
-MD5 (128 bit digest)  
-Developed by Ronald Rivest in 1991  
-Weaknesses discovered from 1996 onwards  
  
-SHA-1 (160 bit digest)  
-SHA-3 (224+)  
-Released in 2015

Uses of Hash Functions  
-Checksum  
-Passwords  
-Digital Signatures  
-Proof of Work

Message digests and Digital Signatures  
-If read by a machine or if message is very long, use hash functions

Proof of Work  
-Sometimes helpful to make a user o an internet service “pay” for it by performing “work”  
-Examples: Bitcoin miners must perform work to add transaction records to the block chain and claim rewards. Users logging into a system might be made to work to submit their password (to prevent them doing a “brute force” attack)