Hash functions

H: input (arbitrary length) $\longrightarrow$ output b bits (fixed length)

applications

- error-checking
- tamper-protection
- password storage
- digital signatures
- block chains

$A \xrightarrow[H(m)]{m} B$ $\quad$ $A \xrightarrow{m} B$ $\quad$ $A \xrightarrow{H(m)} B$

H one-way if, given y, infeasible to compute m with $H(m) = y$

H (strongly) collision-resistant if infeasible to find m, m' with $H(m) = H(m')$

popular hash functions

	published	output bits	
CRC32	1975	32	only for checksums!
MD5	1992	128	broken!
SHA-1	1995	160	collision found 2017
SHA-2	2001	256/512	
SHA-3	2015	arbitrary	

"workable"

- hash to PRG: $x_0 = \text{seed}$ $\quad x_n = H(x_{n-1})$
  $y_n = x_n \pmod 2$
  output: $y_1 y_2 y_3 \cdots$

- block-cipher to hash: $\tilde{H}(x, k) := E_k(x) \oplus x$ (AES-256; k: 256, x: 128; $\tilde{H}$: 128+256; output: 128; $\tilde{H}$: compression function)