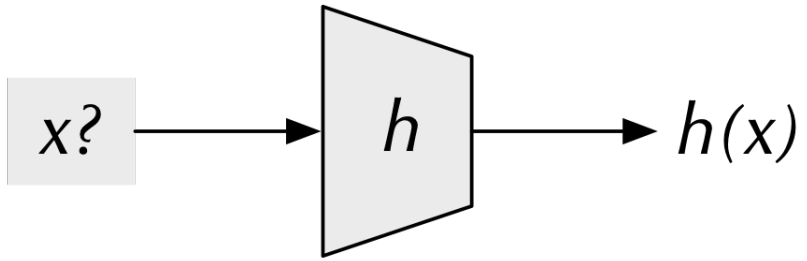
Applications of One-Way Hash Functions

- Integrity Verification — Detecting when data has been altered
- **Commitments** — Committing a secret without telling it
- Password Verification — Verifying a password without storing the plaintext

Commitments — Committing a Secret Without Telling It

- One-way property
  - Disclosing the hash does not disclose the original message
  - Useful to commit secret without disclosing the secret itself



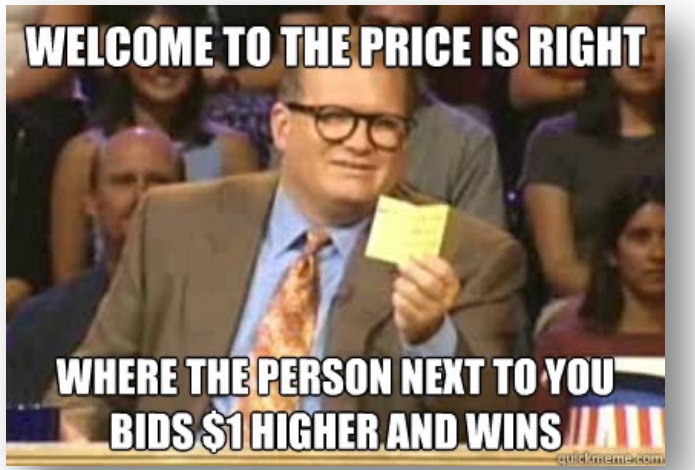
Given $\mathrm{h}(x) = z$, hard to find x

*(or **any** input that hashes to z for that matter)*

Commitments — Committing a Secret Without Telling It

- One-way property
  - Disclosing the hash does not disclose the original message
  - Useful to commit secret without disclosing the secret itself

- Example: Fair Games



Commitments — Committing a Secret Without Telling It

- One-way property
  - Disclosing the hash does not disclose the original message
  - Useful to commit secret without disclosing the secret itself

- Example: Fair Games