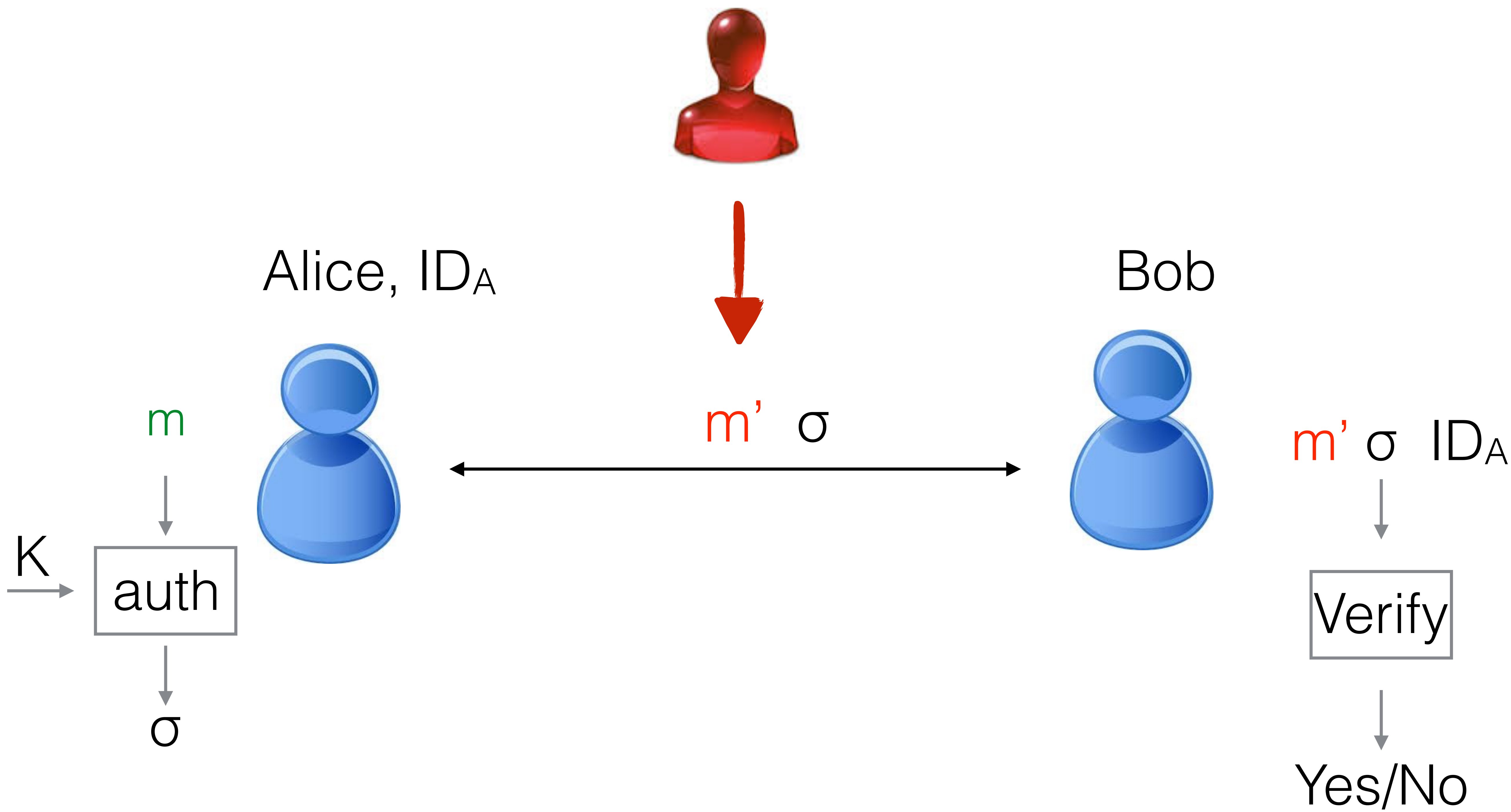
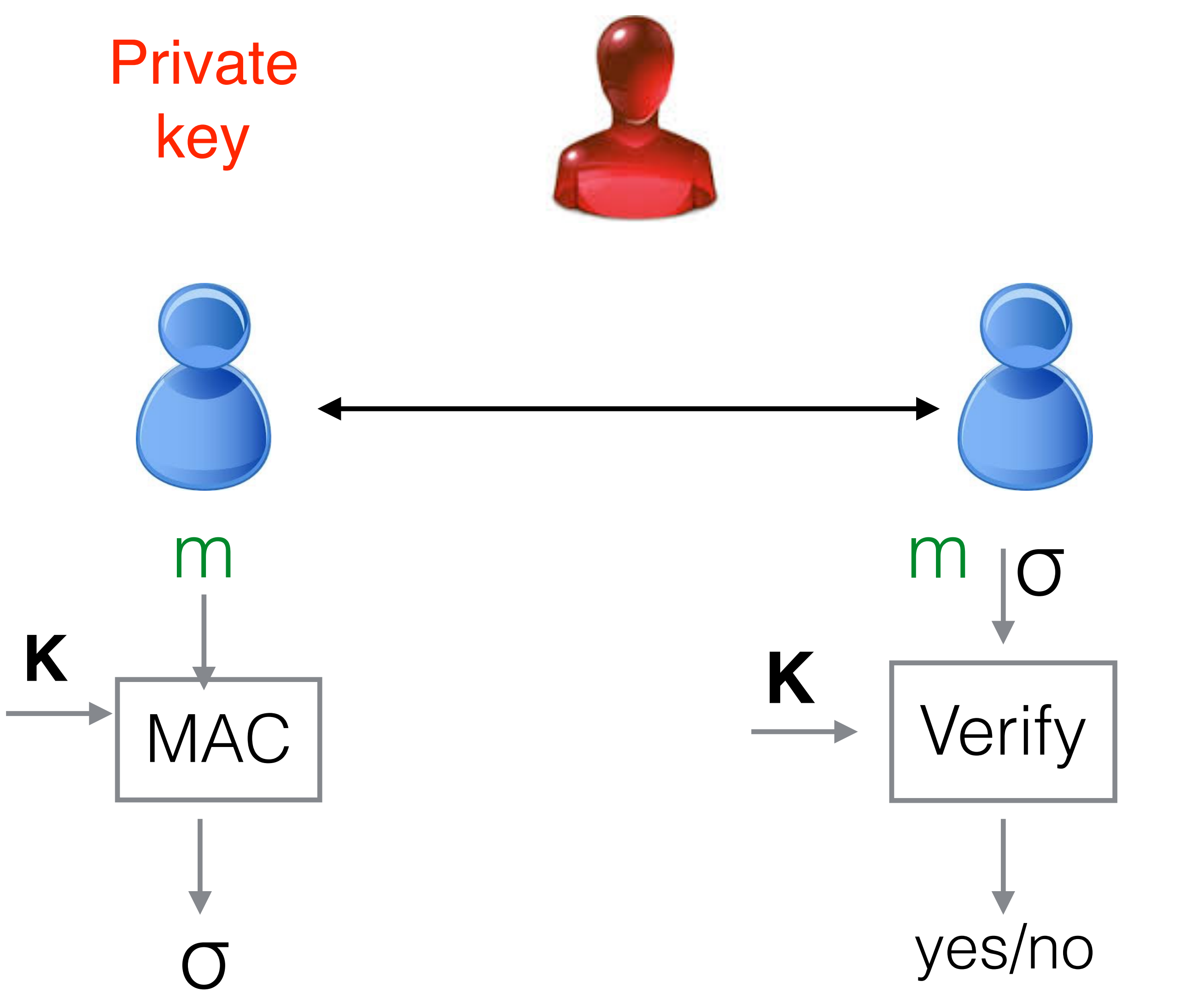
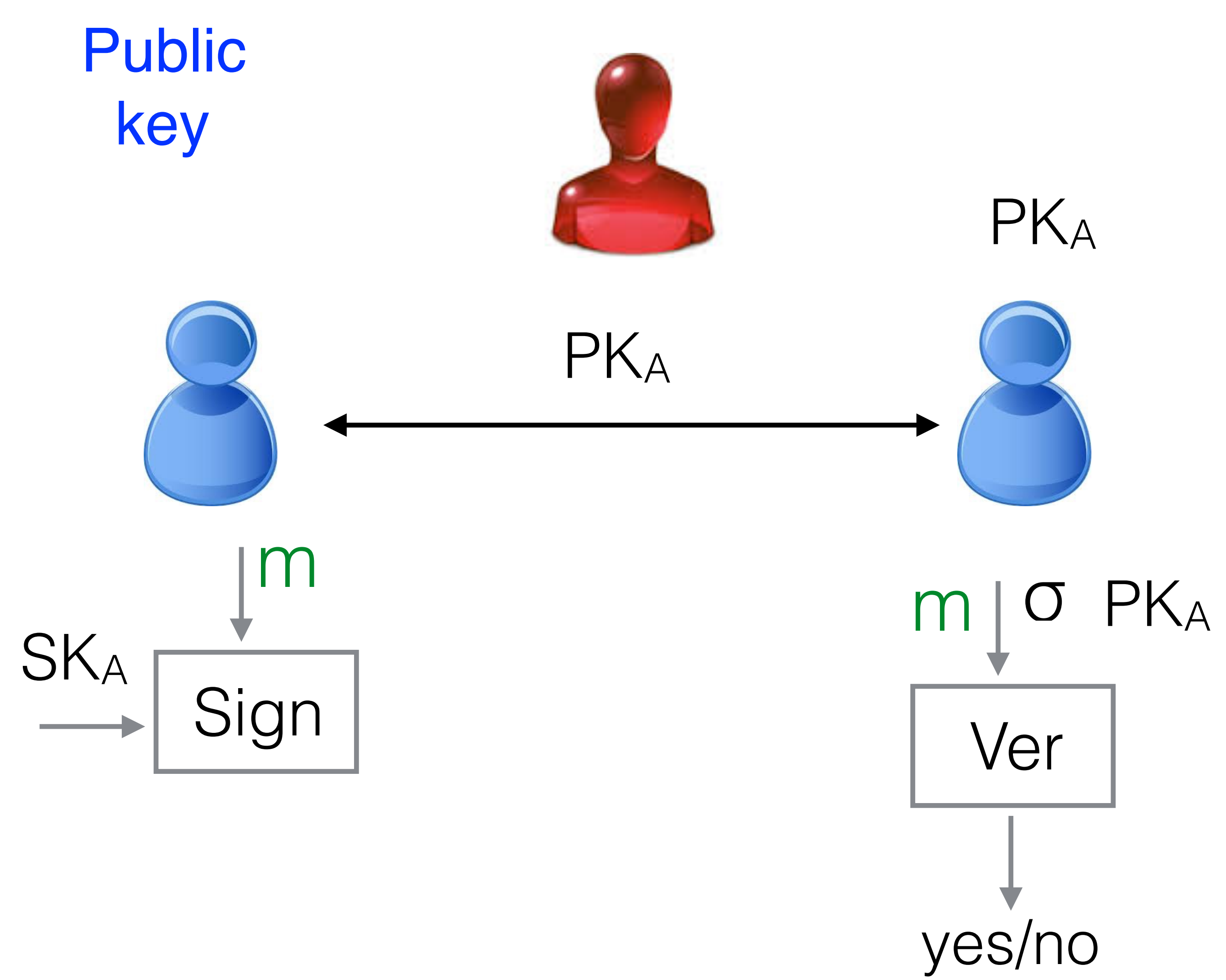
Authentication / Integrity



Message Authentication Code



Signature



Hash Functions

Hash Functions

Definition

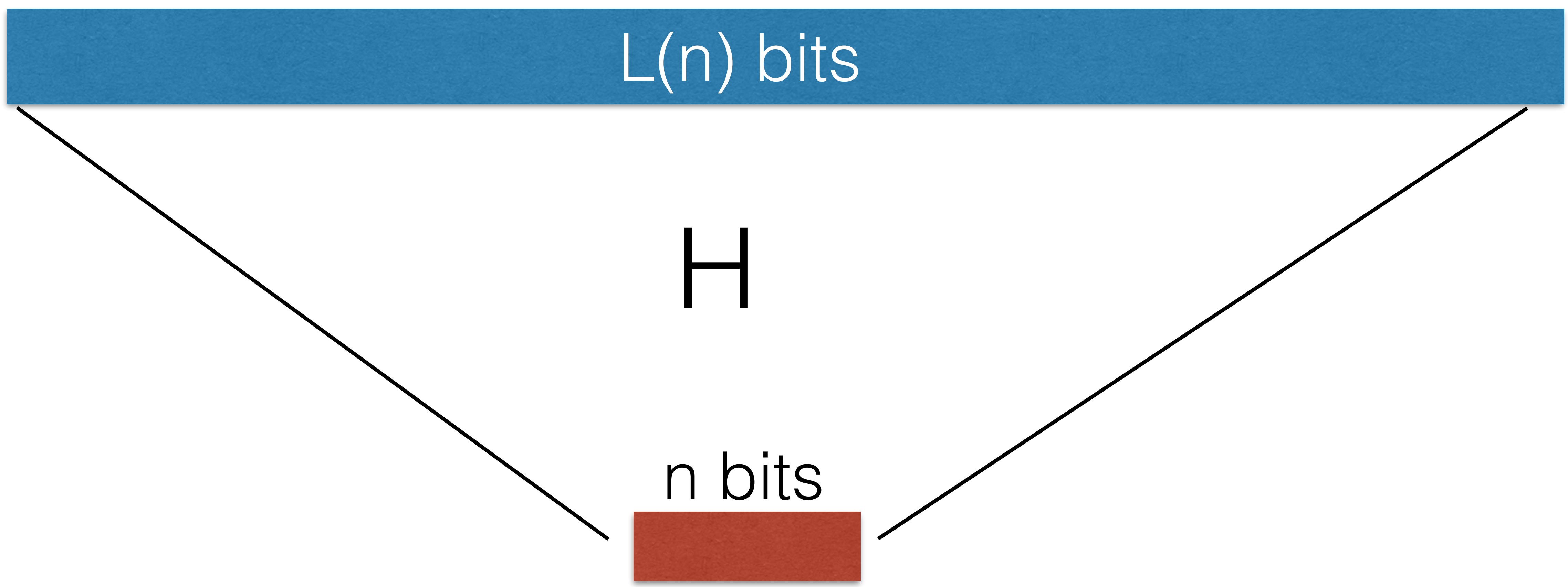
- Collision Resistance

  (Birthday Attack)

Construction

- Merkle - Damgård Transformation
- Construction of a 2n —> n hash function

Hash Function

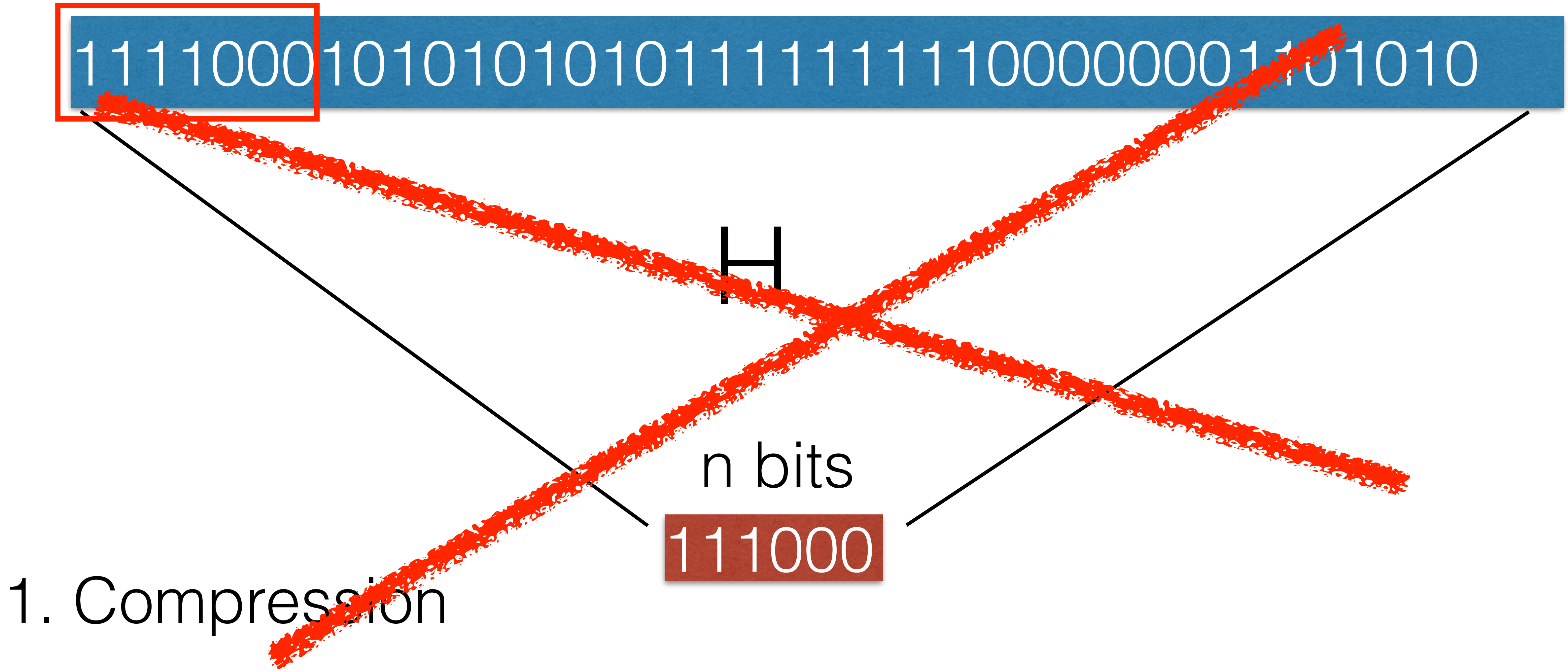


1. Compression

2. **Hard to find** collision (collision-resistance)

Collision: a pair of inputs x_1, x_2
s.t. $H(x_1) = H(x_2)$

Example: Bad Hash Function



easy to find collision!

Building up intuition on Collisions…

- In class exercise

MyH : $\{0,1\}^{3n} \rightarrow \{0,1\}^{n}$

MyH(M)

parse M = $m_1 | m_2 | m_3$

output h = $m_1 \oplus m_2 \oplus m_3$

Find a collision in MyH

a pair of inputs A, B
s.t. MyH(A)= MyH(B)

Why Collision Resistance is crucial?

- ....
- ....
- ....

Definition Collision-Resistance Hash function

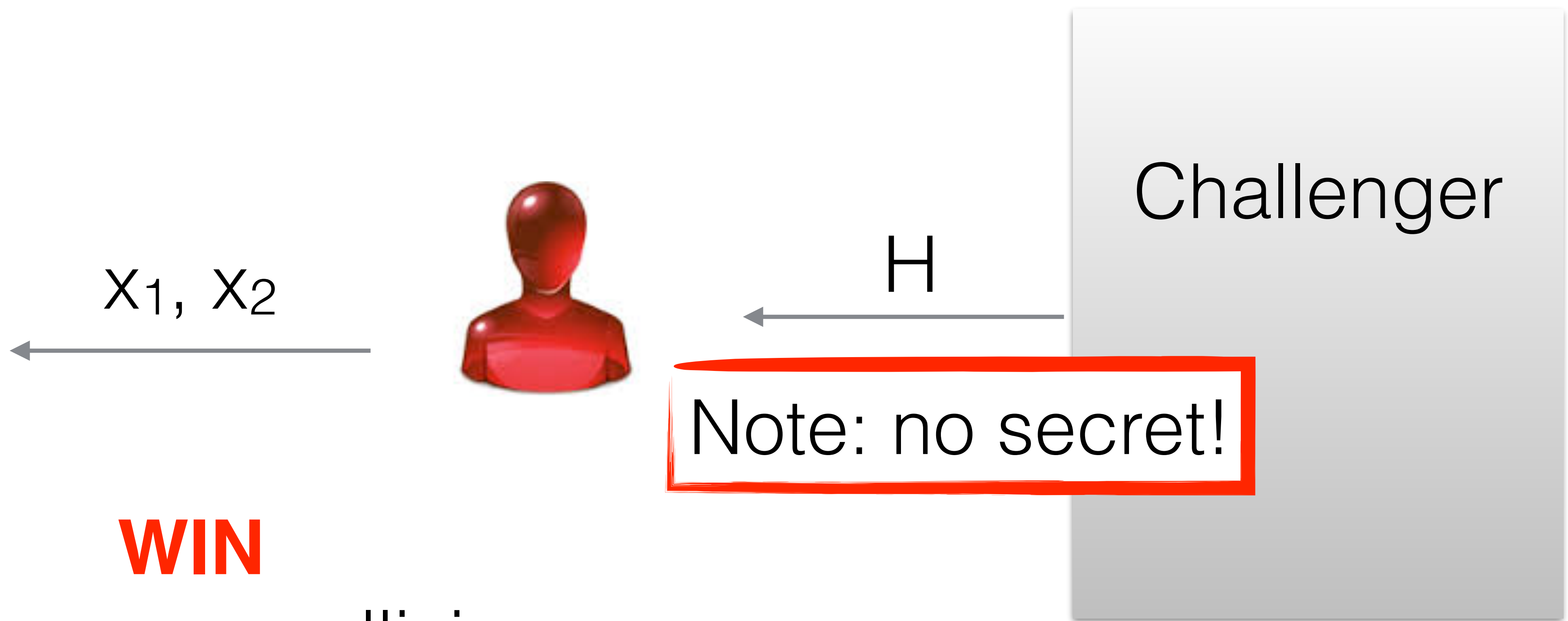
A function $H:\{0,1\}^* \longrightarrow \{0,1\}^n$ is collision resistance if

- **Compressing**. |input| < |output|
- **Collision Resistance**. Finding a collision is hard.

For any PPT Adversary, probability that adversary finds two inputs **x, x’** , such that

H(x) = H(x’) is negligible.

Hash-Collision Game



WIN

if x_1,x_2 are a collision

$H(x_1) = H(x_2)$

H is collision-resistance if

Pr[A finds a collision] = negl(n)

Definition from Introduction to Modern Cryptography

The collision-finding experiment $\mathsf{Hash\text{-}coll}_{\mathcal{A},\Pi}(n)$**:**

1. *A key s is generated by running* $\mathsf{Gen}(1^n)$.
2. *The adversary $\mathcal{A}$ is given s and outputs x, x'. (If Π is a fixed-length hash function for inputs of length $\ell'(n)$ then we require $x, x' \in \{0,1\}^{\ell'(n)}$.)*
3. *The output of the experiment is defined to be 1 if and only if $x \neq x'$ and $H^s(x) = H^s(x')$. In such a case we say that $\mathcal{A}$ has found a collision.*

Discussion on Collision-Resistance Hash Functions

- There is no secret!
- The probability of success is negligible **but** ….

How hard is to find a collision?

- Brute Force Attack. $\boxed{\text{Time } N=2^n}$

  1. Pick **N+1** messages $m_1, \ldots, m_{N+1}$

  2. Compute hash $H(m_1), \ldots H(m_N)$

- Birthday Attack $\boxed{\text{Time } \sqrt{N} = 2^{n/2}}$

Why “Birthday” Paradox

$N = 365$

$q = \sqrt{365} = 23$

Discussion on Collision-Resistance Hash functions

- Even the perfect hash function, can be broken in $2^{n/2}$

- If we want security of **k** bits, then the security parameter must be n=…?

Construction

Hash Functions

Definition

- Collision Resistance

(Birthday Paradox)

Construction

- Merkle - Damgård Transformation
- Construction of a 2n —> n hash function

How to build an arbitrary length hash function

1. Merkle-Damgård transform.

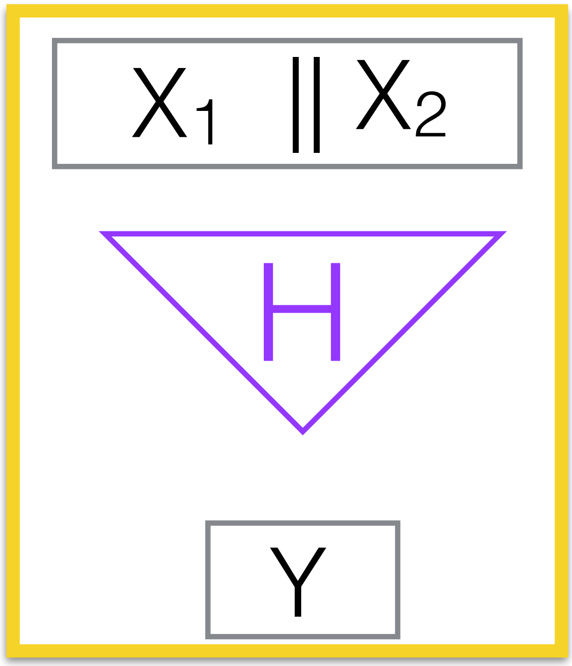
   Assume we can compress from 2n —> n,
   then we can compress any length

2. Hash function 2n —> n

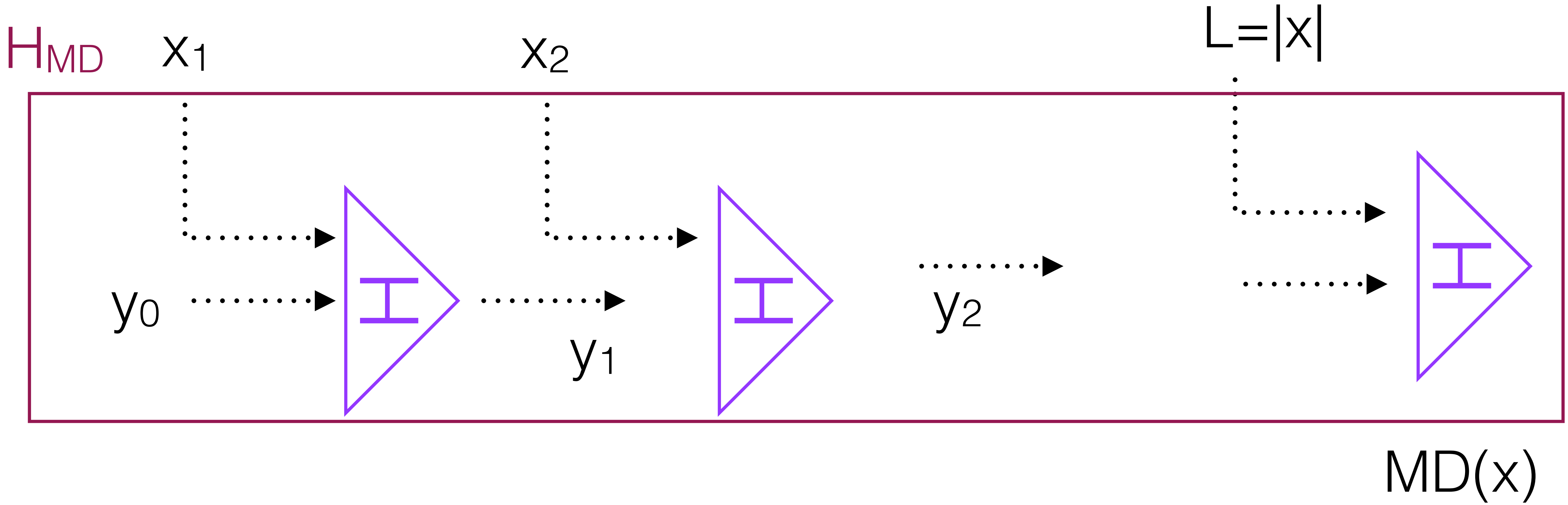
1

Merkle-Damgård transformation

assume



$x = x_1 \| x_2 \| \ldots\ldots.$



CONSTRUCTION 4.13

Let (Gen, h) be a fixed-length collision-resistant hash function for inputs of length $2\ell(n)$ and with output length $\ell(n)$. Construct a variable-length hash function (Gen, H) as follows:

- Gen: remains unchanged.
- H: on input a key s and a string $x \in \{0,1\}^*$ of length $L < 2^{\ell(n)}$, do the following (set $\ell = \ell(n)$ in what follows):

  1. Set $B := \lceil \frac{L}{\ell} \rceil$ (i.e., the number of blocks in x). Pad x with zeroes so its length is a multiple of ℓ. Parse the padded result as the sequence of ℓ-bit blocks $x_1, \ldots, x_B$. Set $x_{B+1} := L$, where L is encoded using exactly ℓ bits.
  2. Set $z_0 := 0^\ell$.
  3. For $i = 1, \ldots, B+1$, compute $z_i := h^s(z_{i-1} \| x_i)$.
  4. Output z_{B+1}.

Theorem.

If H is a collision-resistant hash function with compression factor 2

then MD is a collision-resistant hash function for arbitrary input string

Proof.

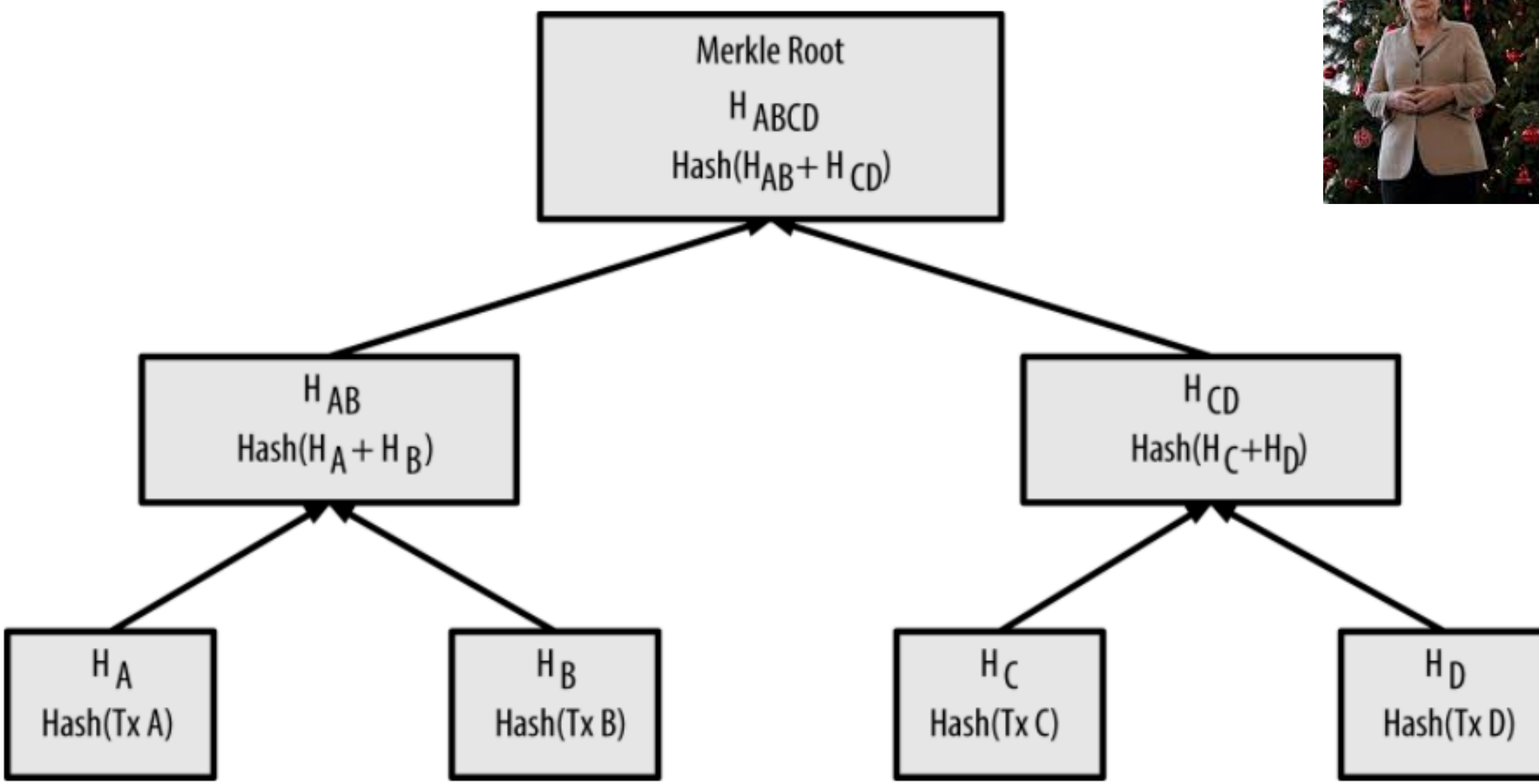
By contradiction

Merkle Damgård transformation

Merkle

Damgård

Merkle Tree



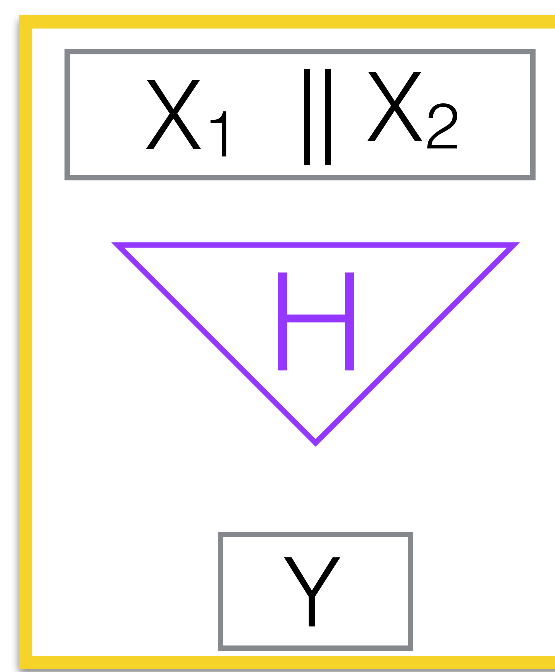
Merkle Root
H_{ABCD}
$Hash(H_{AB} + H_{CD})$
H_{AB}
$Hash(H_A + H_B)$
H_{CD}
$Hash(H_C + H_D)$
H_A
Hash(Tx A)
H_B
Hash(Tx B)
H_C
Hash(Tx C)
H_D
Hash(Tx D)

How to build an arbitrary length hash function

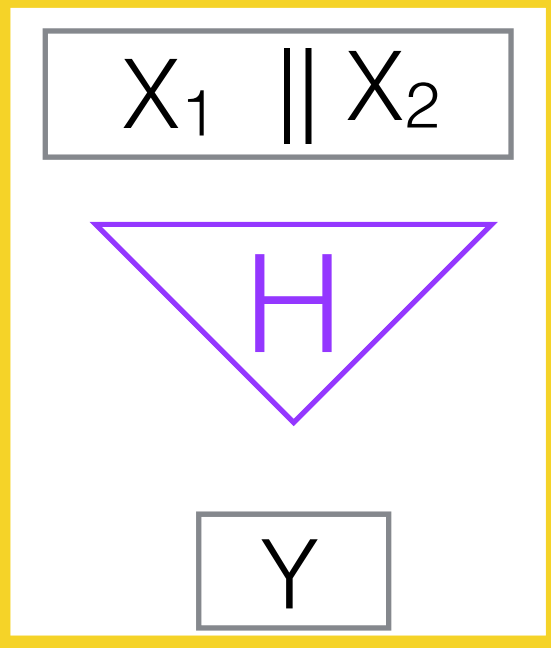
1. Merkle-Damgard transform.

   Assume we can compress from 2n —> n,
   then we can compress any length

2. Hash function 2n —> n



How to construct a Hash Function

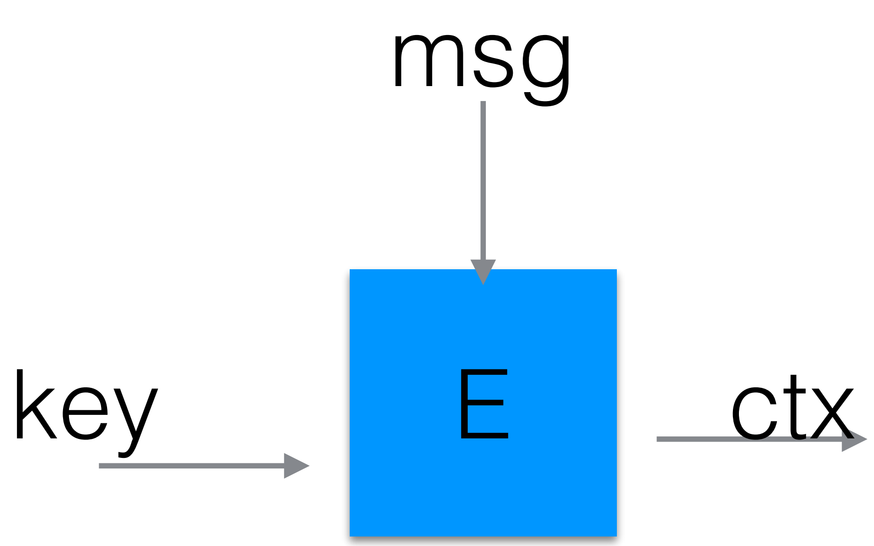


- From Block-ciphers (Davies-Mayer)
- From Number Theoretic Construction

How to construct a Hash Function

(Ideal Permutation) Block-Cipher

$$E: \{0,1\}^k \times \{0,1\}^m \longrightarrow \{0,1\}^m$$



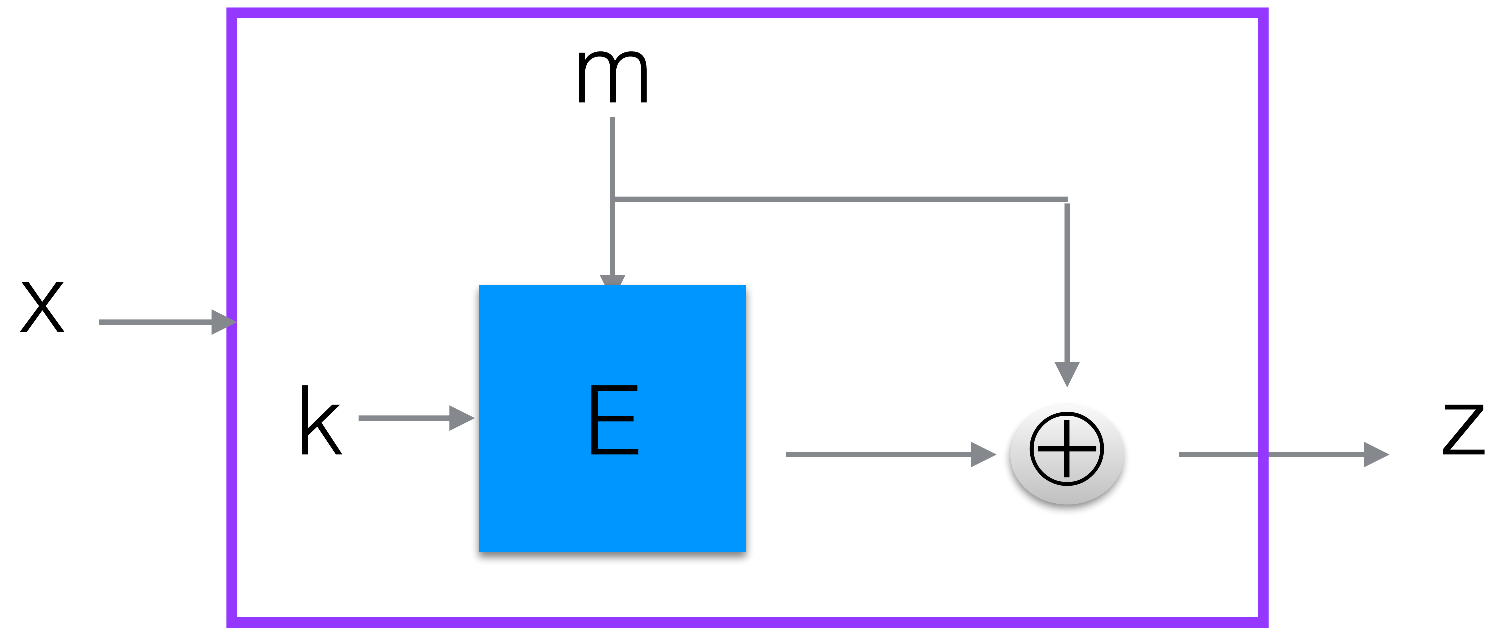
How to construct a Hash Function

Davies-Mayer $H : \{0,1\}^{k+n} \rightarrow \{0,1\}^n$

H(x)

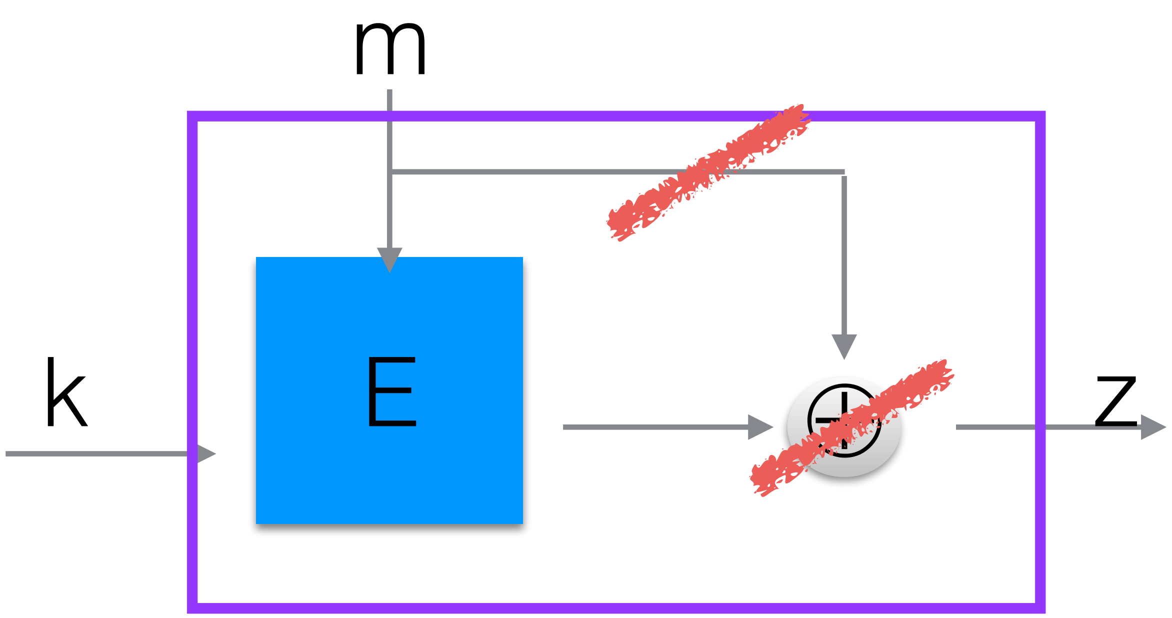
Parse x as k|m

z= $E_k(m) \oplus m$



In class exercise

MY Davies-Mayer***



H(x)

Parse x as k|m

$\boxed{z = E_k(m)}$

can you find a collision?

$E: \{0,1\}^k \times \{0,1\}^m \quad \{0,1\}^m$ HINT: we can decrypt

Many variants for constructing Hash functions from block-cipher

12 variants

$$z = E(k_0, m_0) \oplus k_0 \oplus m_0$$

$$z = E(k_0 \oplus m_0, m_0) \oplus m_0$$

……..

……..

Putting things together

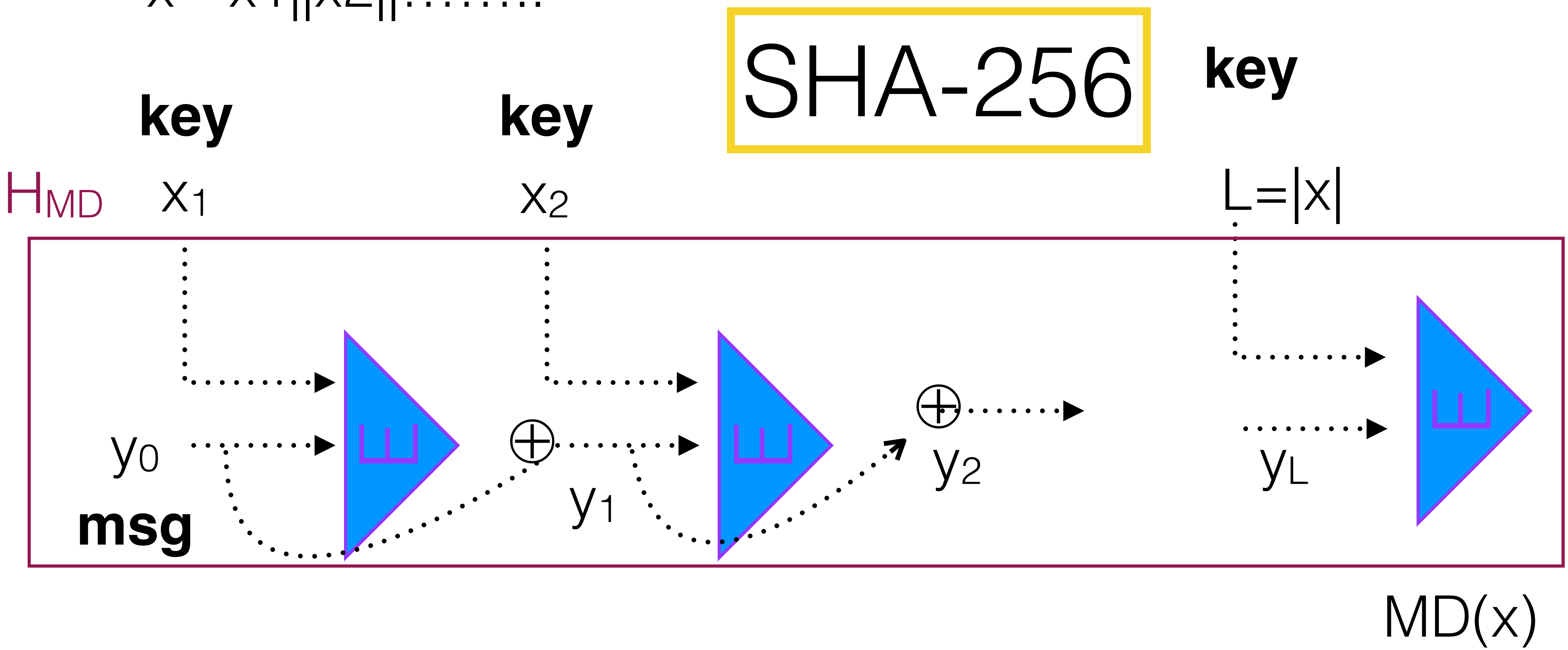
Merkle-Damgård transform

Davie Mayers with block cipher

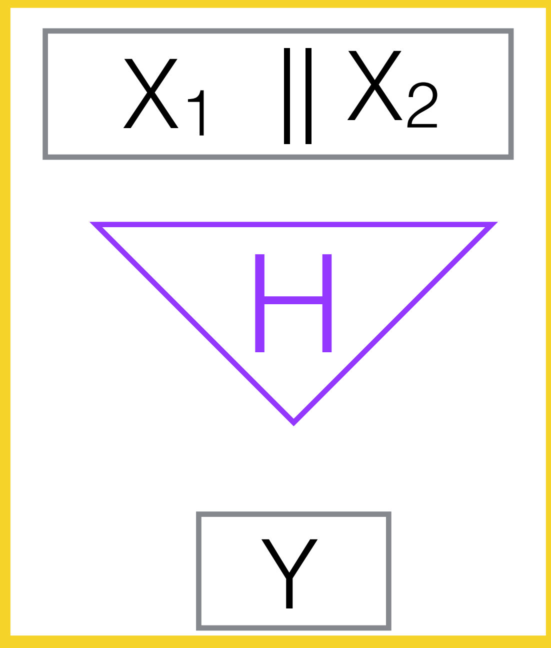
Putting things together

Merkle-Damgård transformation + Davies-Mayer

x= x1||x2||........

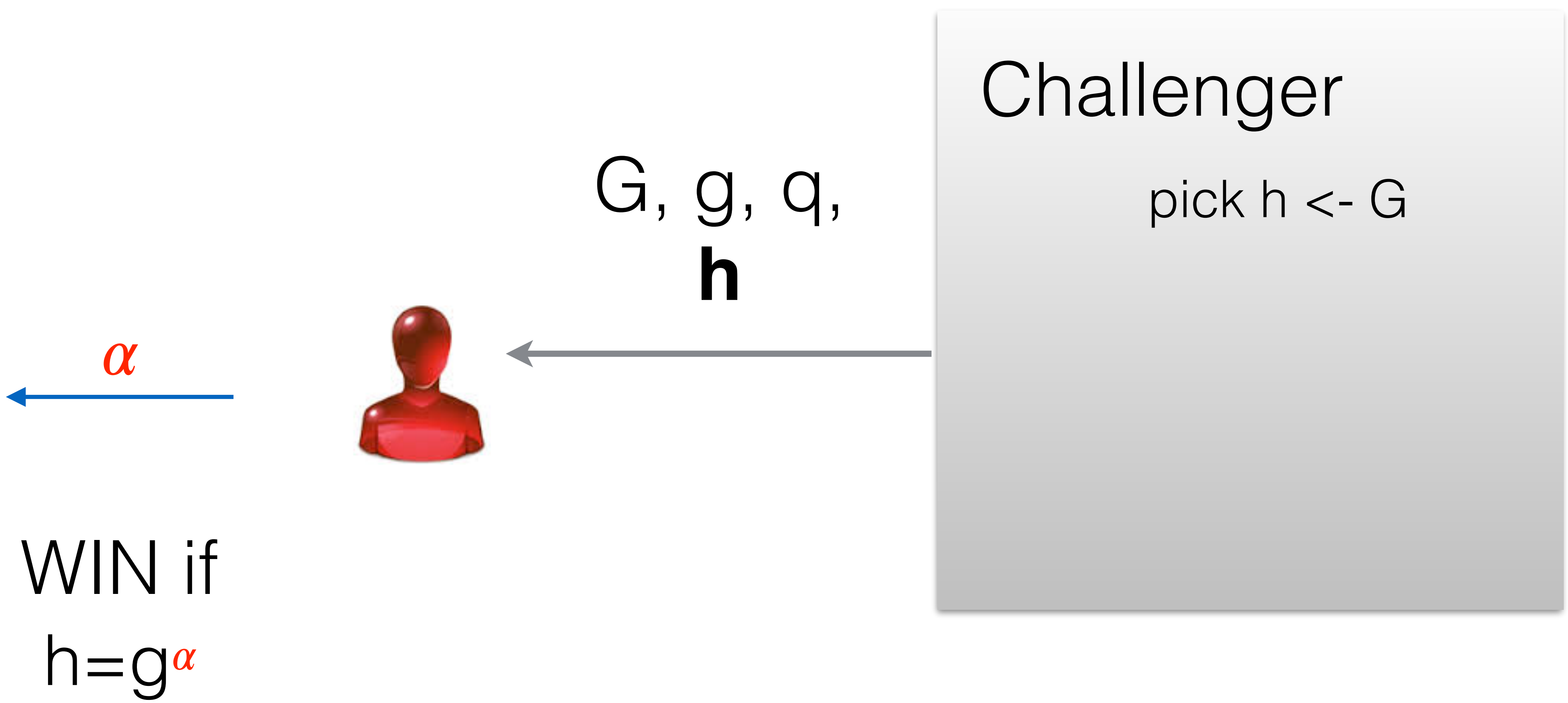


How to construct a Hash Function



- From Block-ciphers (Davies-Mayer)
- From Number Theoretic Construction

Discrete Log Assumption



1. Number Theoretic Construction

Assume G is a cyclic group where the DL assumption is believed to hold

Gen(G, g, q)

pick a **random h** in G

Output h

H(X,m)

parse $m = m_1 | m_2$

Output $y = g^{m1} h^{m2}$

1. Number Theoretic Construction

Theorem.

Assume that the discrete logarithm problem is hard in G

Then (Gen, H) is a collision-resistant hash function

Proof.

By contradiction
[on board in class]