Message Authentication & Public Key Encryption

COMP 435
Fall 2017
Prof. Cynthia Sturton

Message Authentication

Message Authentication

Alice

Bob

msg

msg →

Is *msg* authentic?

Message Digest

Alice

Bob

$H_m := \mathtt{h}(m)$

$m \mid H_m$ →

$H_m \stackrel{?}{=} \mathtt{h}(m)$

Message Digest

- Variable length input
- Fixed length output

Message Digest

- Variable length input
- Fixed length output

Example: Mod 10 arithmetic

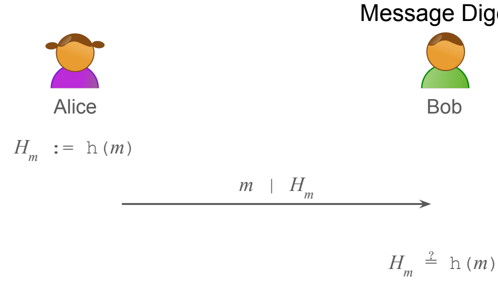
Input: 5
Output: 5

Input: 29882
Output: 2

Message Digest

- Variable length input
- Fixed length output
- Multiple inputs map to one output

Message Digest



Message Digest

A digest demonstrates presence of modification; A digest does not prove the absence of modification.

One Way Hash Function for Message Authentication

Alice

Bob

$H_m := \mathtt{h}(m)$

$D_m := \mathtt{Enc}_{\mathtt{k}}(H_m)$

$m \mid D_m \longrightarrow$

$\mathtt{h}(m) \stackrel{?}{=} \mathtt{Dec}_{\mathtt{k}}(D_m)$

Keyed Hash Message Authentication Code (MAC)

Alice

Bob

$H_m := \mathtt{h}(k \mid m \mid k)$

$m \mid H_m \longrightarrow$

$H_m \stackrel{?}{=} \mathtt{h}(k \mid m \mid k)$

Cryptographically Secure Hash Functions

Cryptographic Hash

1. Function is one way
2. Pre-image resistant
3. Second pre-image resistant
4. Collision resistant

Function is One Way

Given H,
there is no easy algorithm for computing m s.t. h(m) = H.

Collision Resistant

Hard to find m, m' such that

$m \neq m'$ and

$h(m) = h(m')$

Second Pre-image Resistant

Given m, hard to find m' such that

$m \neq m'$ and

$h(m) = h(m')$

Pre-image Resistant

Let H := $\mathtt{h}(m)$.

Given H, hard to find any m' such that

$\mathtt{h}(m') = H$

Cryptographic Hash

1. Pre-image resistant
2. Second pre-image resistant
3. Collision resistant

Pre-image Resistant vs. Collision Resistant and the Birthday Paradox

Pre-image Attack vs. Collision Attack

Pre-image Attack

Given H, find m s.t.

$\mathtt{h}(m) = H$

Collision Attack

Find m, m' where $m \neq m'$ s.t.

$\mathtt{h}(m) = \mathtt{h}(m')$

Birthday Paradox

Prob [you share my birthday] = $\frac{1}{365}$

Birthday Paradox

Prob [anyone in the class shares my birthday] = $\frac{125}{365}$

Birthday Paradox

Prob [any two people in the class share a birthday] = ??

Birthday Paradox

Prob [any two people in the class share a birthday] = ??

Consider all the possibilities

- All the ways there could be one match in the classroom
- All the ways there could be two matches
- …

Birthday Paradox

Prob [any two people in the class share a birthday] =

1 - Prob [no two people share a birthday]

Birthday Paradox

Prob [no two people share a birthday] =

$$\overbrace{\left[\frac{365}{365} \cdot \frac{364}{365} \cdot \frac{363}{365} \cdots \frac{241}{365}\right]}^{\text{125 people}}$$

1st person can safely have any birthday

2nd person can safely have any of the remaining 364 birthdays

Birthday Paradox

Prob [no two people share a birthday] =

$$\overbrace{\left[\frac{365 \cdot 364 \cdot 363 \cdots (365 - n + 1)}{365^n}\right]}^{\text{n people}}$$

Birthday Paradox

Prob [any two people in the class share a birthday] =

$$1 - \left[\frac{{}_{365}P_n}{365^n}\right]$$

Number of people	P(Any two people share a birthday)
1	0%
5	2.7%
10	11.7%
20	41.1%
23	50.7%
30	70.6%
40	89.1%
50	97.0%
60	99.4%

Birthday problem, https://en.wikipedia.org/w/index.php?title=Birthday_problem&oldid=740077911 (last visited Sept. 19, 2016).

Back to Message Authentication

Message Authentication Code (MAC)


Alice


Bob

$MAC_m := f(k, m)$

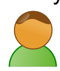
$m \mid MAC_m$ →

$MAC_m \stackrel{?}{=} f(k, m)$

Public Key Encryption

Public Key Encryption

Alice



Bob

$C = \mathtt{Enc}_{\mathtt{B\text{-}pub}}(m)$

C →

$m = \mathtt{Dec}_{\mathtt{B\text{-}priv}}(C)$

Random Numbers

Random Numbers

"Chosen uniformly at random"

Random Numbers

"Chosen uniformly at **random**"

Random Numbers

"Chosen **uniformly** at random"

Large Numbers

An exercise

Key length: 56 bits

Number of possible keys:

Large Numbers

An exercise

Key length: 56 bits

Number of possible keys: 2^56

In decimal notation: