CIS 3362 11/8/22 (Stallings Cht 11)

Hash Functions + Msg Authentication
Birthday Paradox

Msg Authentication - verifying msg hasn't been altered.

A simple method to achieve

Alice → Bob

assume RSA

(a) no one else read
(b) bob proof msg was unaltered
(c) came from alice.

1. M

2. $E_{\text{Bob-Public}}(M)$, encrypt msg w/ Bob-Public key
only Bob can read it.

3. $C = E_{\text{Alice-Private}}(E_{\text{Bob-Public}}(m)) \rightarrow$ send to Bob

When Bob receives → 4. $D_{\text{Alice-Public}}(C)$

5. $D_{\text{Bob-Private}}(D_{\text{Alice-Public}}(C)) \rightarrow M$

If this all works + you get a meaningful msg, then it must have been Alice who sent the msg.

* THIS IS SLOW !!!

Two Different Goals

1) Message Authentication - verifying msg has not be altered since it was sent

2) Digital Signature - Proof of who authored a msg.

Hash Functions

1. Input - any size bitstring
2. Output - fixed size output typically either $\boxed{n \text{ bits}}$ OR value $[0, MAX-1]$.

3. It's possible that $x \neq y$ but $H(x) = H(y)$. This is called a collision.

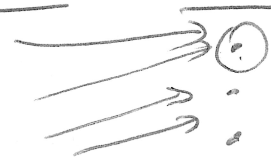
Properties of a Good Hash Func

1) Given an output value y, it should computationally infeasible to find a value x, s.t. $H(x) = y$.

Weak Collision Resistance
2) Given an input x, it should be computationally infeasible to find some x', with $x' \neq x$ but $H(x') = H(x)$.

Strong Collision Resistance
3) Hard to find <u>ANY</u> pair x, x', with $x \neq x'$ such that $H(x) = H(x')$.

Inputs   Outputs



.261 adam   257 jordan
.223 gaya   252 lucas
.374 dean   232 jack
.245 kevin   201 tresly
.255 jorge

If I pick a number in range $[1,n]$, then have k people also pick a rnd number $[1,n]$ with $k < n$ probability one of their numbers matches mine $< \frac{k}{n}$.

$k+1$ people all pick a rnd number $[1,n]$ what's the probability that some 2 people pick the same number?

What's prob all #s are different?

$$\underbrace{\frac{n}{n}}_{1^{st}\text{ person}} \times \underbrace{\frac{n-1}{n}}_{2^{nd}\text{ per}} \times \frac{n-2}{n} \times \frac{n-3}{n} \times \cdots \frac{n-k}{n}$$

birthday paradox $n=365$, $k = 2\cancel{3}2$ for the formula the ~~proba~~ probability is $< \frac{1}{2}$ all are different!

4 Modes of Use

a) $E(K, [M \,||\, H(m)])$

encrypt everything. Receiver gets msg, they decrypt to reveal M' and $H(m')$. Now to verify the message wasn't altered calculate $H(m')$ and make sure it's equal to $H(m)$.

b) $M \,||\, E(K, H(m))$

everyone can read but receiver can verify that it's not altered.

c) $M \,||\, H(M \,||\, S)$, S = secret value

Only receiver knows S, so they can calculate $\underline{\underline{M'}} \,||\, S$

received msg.

Calc $H(M' \,||\, S)$ to see if it matches $H(M \,||\, S)$.

Alice Private

d) $E(\underline{\underline{K}}, [M \,||\, \underline{E(PR_a, H(m))}])$

shared private key

Proves Alice sent it but w/o using slow public key on the whole msg.