CIS 3362 11/30/22

Hash Functions - Today
Final Exam Rev - Fri
Check off Quizzes - Fri, outside of HEC 125 after class

Hash Function

1) Variable length input
2) Fixed length output
3) It's possible that $x \neq y$ but $H(x) = H(y)$. (collision)
4) Fast to compute.

Uses

1) Message Authentication
   - Proving message hasn't been altered since it was sent.
2) Digital Signature
   - Proof of who composed/wrote message.

4 Modes of use

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

↑ concatenate

everything encrypted. If modification, recipient should be able to take recoved M', calculate $H(m')$ and see it doesn't match $H(m)$.

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

everyone can see m, but again if M is modified to m', it's hard Eve to adjust $E(K, H(m))$ accordingly.

c) $M \,||\, \overset{H}{\equiv}(M \,||\, S)$, S = secret value

d) $E(K, [M \,||\, E(PR_a, H(M))])$

This proves Alice sent it.

Passwords

Bob	12121 9 Hello
Alice	woohoo!
Eve	christmas1225
⋮	⋮

BAD!

If stolen, every person's account accessible.

Better

	H(password)
Bob	1101011100 0...
Alice	0101101011 0...
Eve	1111001010001...

If Bob's pswd is x and I guess $y \neq x$ but $H(y) = H(x)$, then I set in as Bob...

drawback. BUT most hash func have a very low prob of collision

Weakness - Rainbow Table

Make a list of 10^6 possible common passwords.

for each x, calculate H(x). "woohoo!" → 0101101011 0...

Improvement: Add Salt

	SALT	H(password ⊕ ‖ SALT)
Bob	010110...	0110110101110...
Alice	101101...	1110101010...
Eves	010110..	100101101...

Slows down by search O(n), n = # users

Good Hash Function Requirements

1) Given an output value y, it should be computationally infeasible to find some x such that $H(x) = y$. Pre-image collision resistance

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

3) Hard to find any pair x, x' such that $H(x) = H(x')$.
Collision Resistance

→ Difference btw these is known as the Birthday Paradox.

1 − prob all birthdays diff, k people in room $k < 365$

$$1 - \frac{365}{365} \times \frac{364}{365} \times \frac{363}{365} \times \frac{362}{365} \times \cdots \frac{(365-k+1)}{365}$$