CIS 3362 - 11/19/21

(1) No class Wed 11/24. Will adjust syllabus.

(2) Hash Functions - Today, Monday

Hash Function

1) Variable Length Input
2) Fixed bit output.
3) It's possible for 2 different inputs x, y $H(x) = H(y)$. But this shouldn't occur "easily".
4) Should be fast to compute.

Uses

1) Message Authentication
   - Proof message hasn't been changed since it left the sender
2) Digital Signature
   - Proof of who ~~sent~~ sent the message.

4 Methods to use a hash function for message authentication

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

$\|$ → concatenate

$E(K, \text{something})$: encrypt something using the symmetric key K.

I receive $E(K, [M \| H(M)])$, I decrypt, get $M \| H(M)$ → run through hash func to double check that this matches.

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

I receive ↑. Decrypt to get $H(M)$. Then calculate $H(M)$ and see if they match.

(c) $M \| H(M \| S)$, S = Secret Value.

I receive this, I know S. Calculate $M \| S$. Then I calc $H(M \| S)$ and see if it matches

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

both digital sign AND msg auth AND confidential

I receive + decrypt ⇒ $M \| E(PR_a, H(M))$.

I calculate $H(M)$.

Use PU_a to decrypt this part to reveal $H(M)$, see if they match.

Storing Passwords (hashing is used)

System

Bob abc123
Alice fifi123
⋮

Stealing a file with plaintext passwords is very bad!

Instead this better:

Name	H(pswd)
Bob	110100...
Alice	01011...

Just because I know y it's hard to calc x s.t. $H(x) = y$.

Problem: Rainbow Table

Generate few million "common" passwords.
for each, calculate $H(x)$.
Then look for matches in this
if ANY of the 1000 users has abc123,
we'll figure who it is...

Improvement: SALT

Name	Salt	H(pswd ‖ Salt)
Bob	110101... (rnd bit string	01....
Alice	011011...	

Multiplies work by # of users.

Now if I add Bob's salt to all million pswd, I can only break Bob's IF he had one I guessed.

Requirements for a good hash function

1. Variable Input Size
2. Fixed Output Size
3. Fast to Compute

] HASH

4. Given output value y, it should be computationally infeasible to find any x such that $H(x) = y$.
   [PRE-IMAGE RESISTANCE]
5. Given an input x, it's computationally infeasible to find y, $y \neq x$, such that $H(x) = H(y)$.
   [SECOND IMAGE RESISTANCE]
6. Hard to find <u>ANY</u> x, y such that $H(x) = H(y)$
   [COLLISION RESISTANCE]

→ BIRTHDAY PARADOX!

#4, #5 $\quad prob = \frac{1}{2^{bits}}$

30 room — What's prob all birthdays are different?

$$1 \times \frac{364}{365} \times \frac{363}{365} \times \frac{362}{365} \times \cdots \frac{336}{365}$$

$p(\text{some 2 people}) = 1 -$