Last time

- domain extension for hashes
- Hash-and-MAC
- HMAC

Lecture Let 22

Oct 25 2020

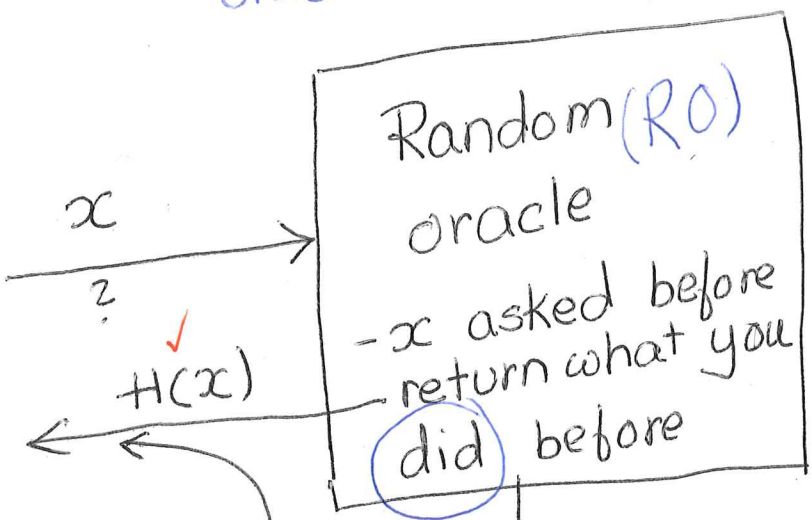
Random Oracle model (RO)

Hash functions are complex (Look at SHA-1, SHA-2, SHA-3, ...) Look at it!

$H: \{0,1\}^* \longrightarrow \{0,1\}^n$

arbitrary size

n-bit, $n=128$



x	H(x)
1011...	✓
11011...	

Intuition
- Model as random function

Fix integer N

Pick q elements $y_1, \dots, y_q$ from $[1 \dots N]$

($q \le \sqrt{2N}$) technical

$$\Pr(\text{coll}(q,N)) \ge 1 - e^{-\frac{q(q-1)}{2N}} \ge \frac{q(q-1)}{4N}$$

($\exists\, y_i = y_j$, $i \ne j$)

collision: two random vals are $= \frac{N-2}{N}$

y_1 y_2 y_3 $\dots$ y_q

1 $(1-\frac{1}{N})$ $(1-\frac{2}{N})$ $(1-\frac{q-1}{N})$

$\frac{N}{N}$ $\frac{N-1}{N}$

no collision (NoColl) — opposite of Coll

$$1\,(1-\tfrac{1}{N})(1-\tfrac{2}{N}) \cdots (1-\tfrac{q-1}{N})$$

$$\le e^{-1/N} \cdot e^{-2/N} \cdots e^{-\frac{(q-1)}{N}} \qquad [1-\tfrac{i}{N} \le e^{-\frac{i}{N}}] = \text{Taylor exp}$$

$$= e^{-\frac{(1+2+\cdots+(q-1))}{N}}$$

$$= e^{-\frac{q(q-1)}{2N}}$$

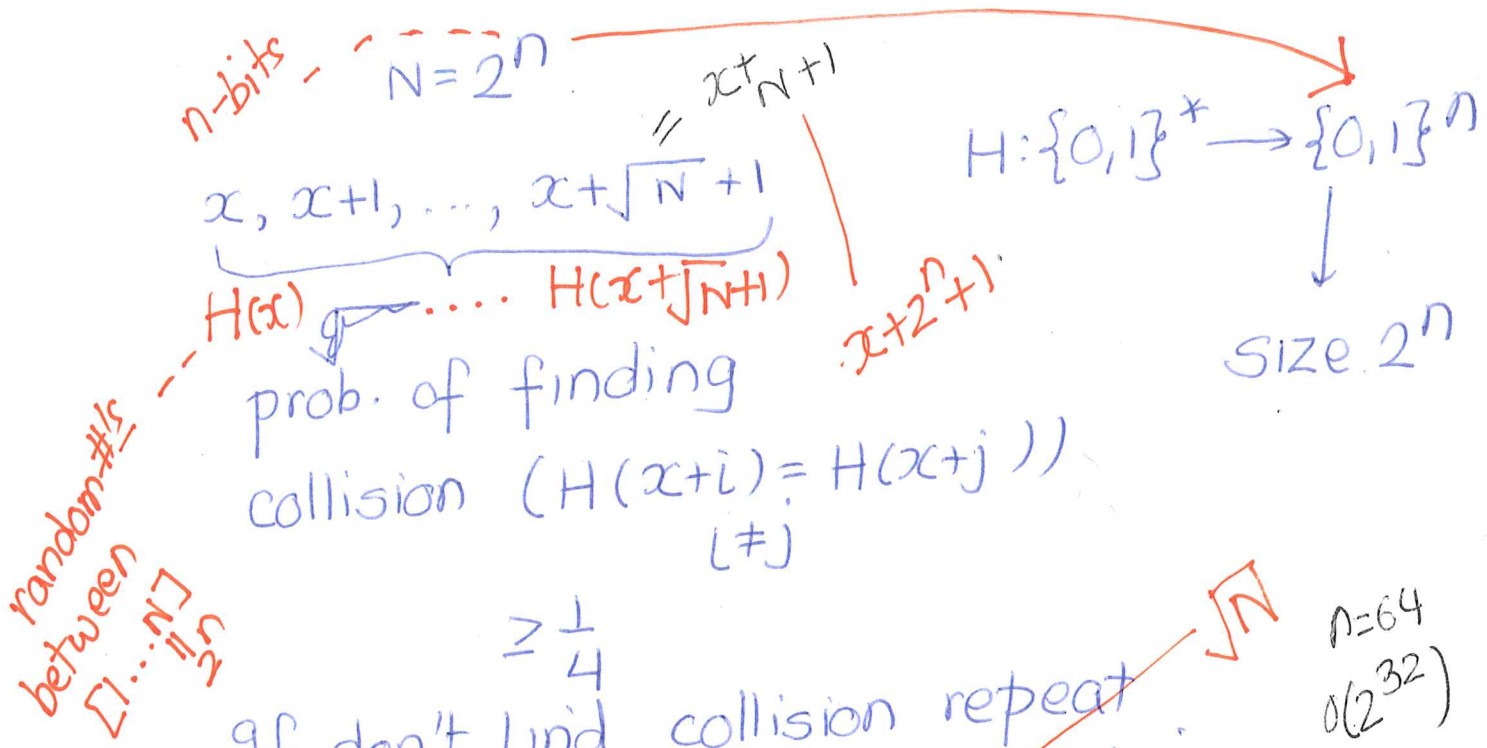
$$\Pr_{(q,N)}[\text{Coll}] = 1 - \Pr_{(q,N)}[\text{NoColl}] \ge 1 - e^{-\frac{q(q-1)}{2N}} \ge \frac{q(q-1)}{4N}$$

$(e^{-x} \le 1 - \frac{x}{2})$ $x<1$

$$q = \sqrt{N} + 1 \le \sqrt{2N}$$

$$\frac{q(q-1)}{4N} = \frac{(\sqrt{N}+1)\sqrt{N}}{4N} \ge \frac{1}{4}$$ ✓

25%



Revisit the birthday problem

$N = 365$ $q = 30$

$1 - e^{\frac{-q(q-1)}{2N}}$ $1 - e^{\frac{-30 \cdot 29}{365 \cdot 2}} = 1 - e^{-2.38} > 50\%$

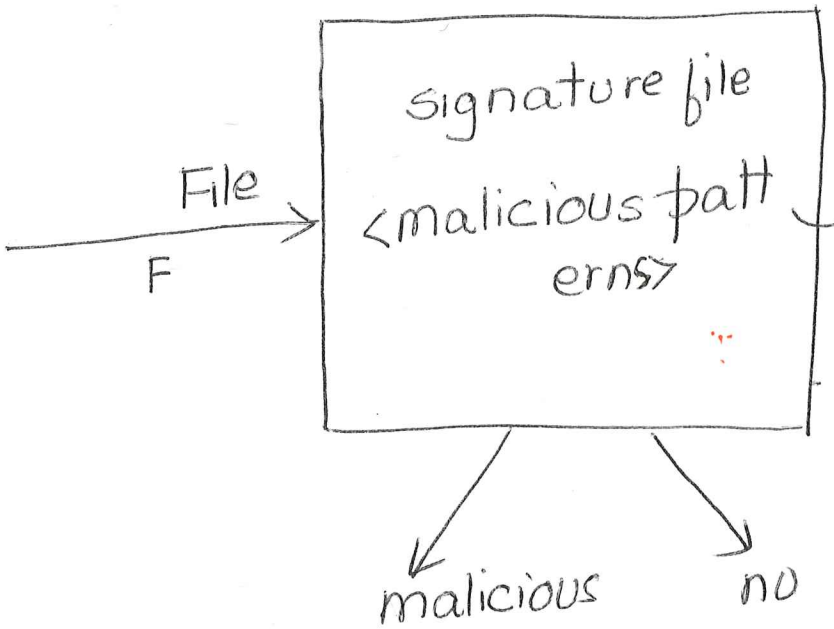
$= 1 - 0.092 = 0.908$

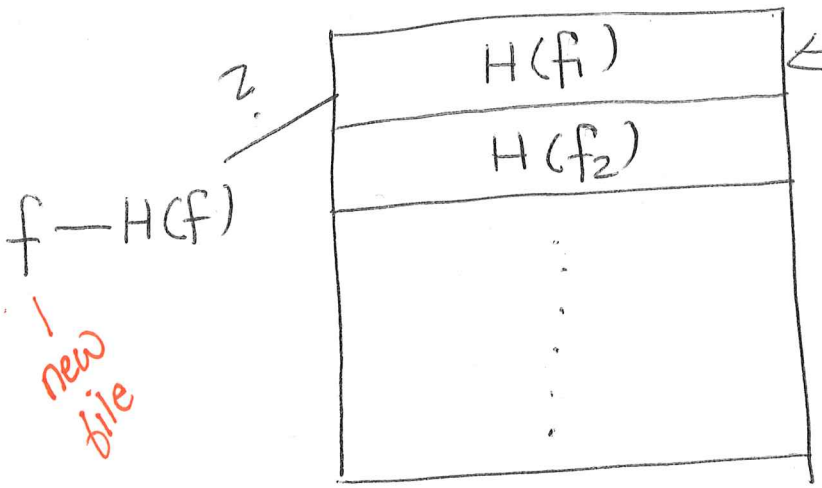
$= 90.8\%$

Several applications of hashing

Virus fingerprinting, Deduplication, P2P file sharing, bitcoin, block chain, ...

Virus fingerprinting





hashes of all malicious files (malware)
VirusTotal

$1 \le i \le n$

check if $H(f) = H(f_i)$
↳ malicous

else
expensive ← check the sig data base.

Oct 27, 2020

Last time

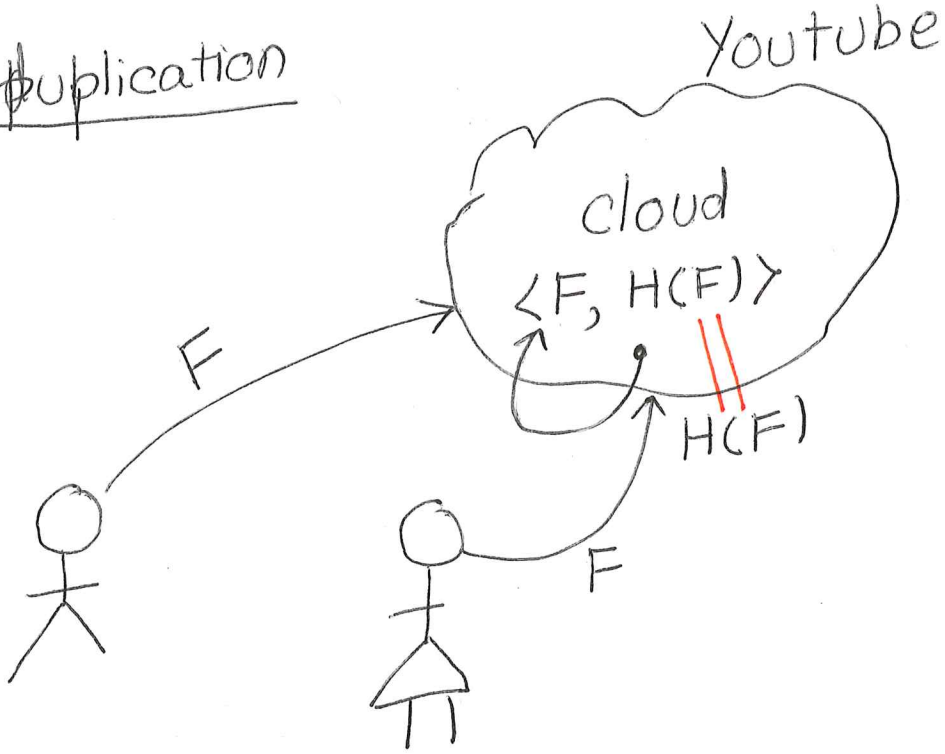
- Improved attack ✓ $\sim O(2^{n/2})$
  - Birthday paradox
- RO-model ✓
- Applications of hash funcs
  - virus scanning, fingerprinting

Logistics

Lecture 23

More applications

Deduplication

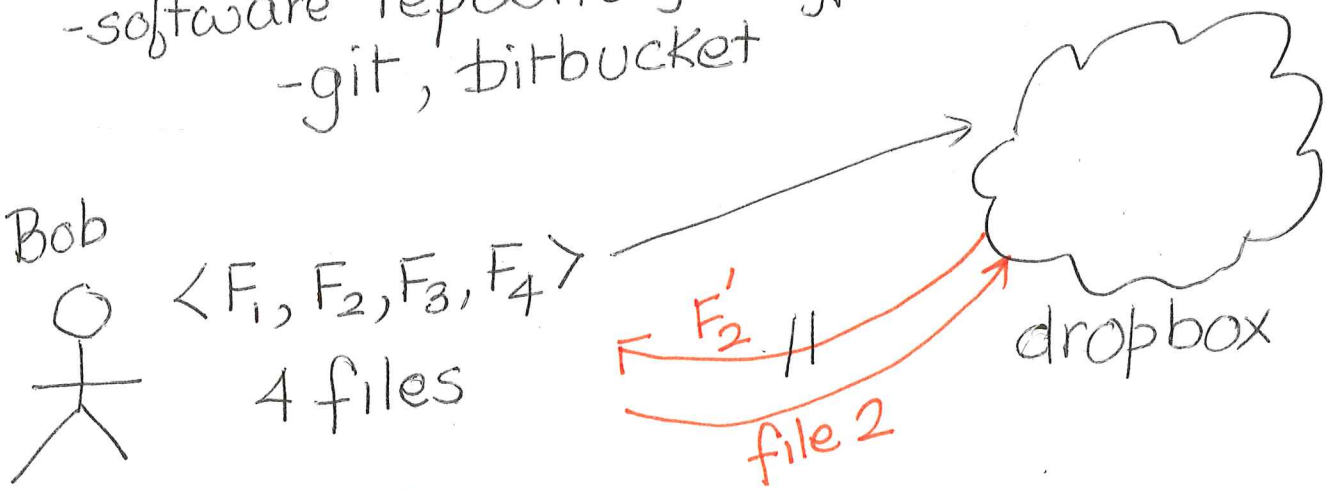


P2P filesharing

servers keep hash functions of files for faster lookup.

Merkle trees

- blockchains
- cryptocurrencies
- software repository
  - git, bitbucket

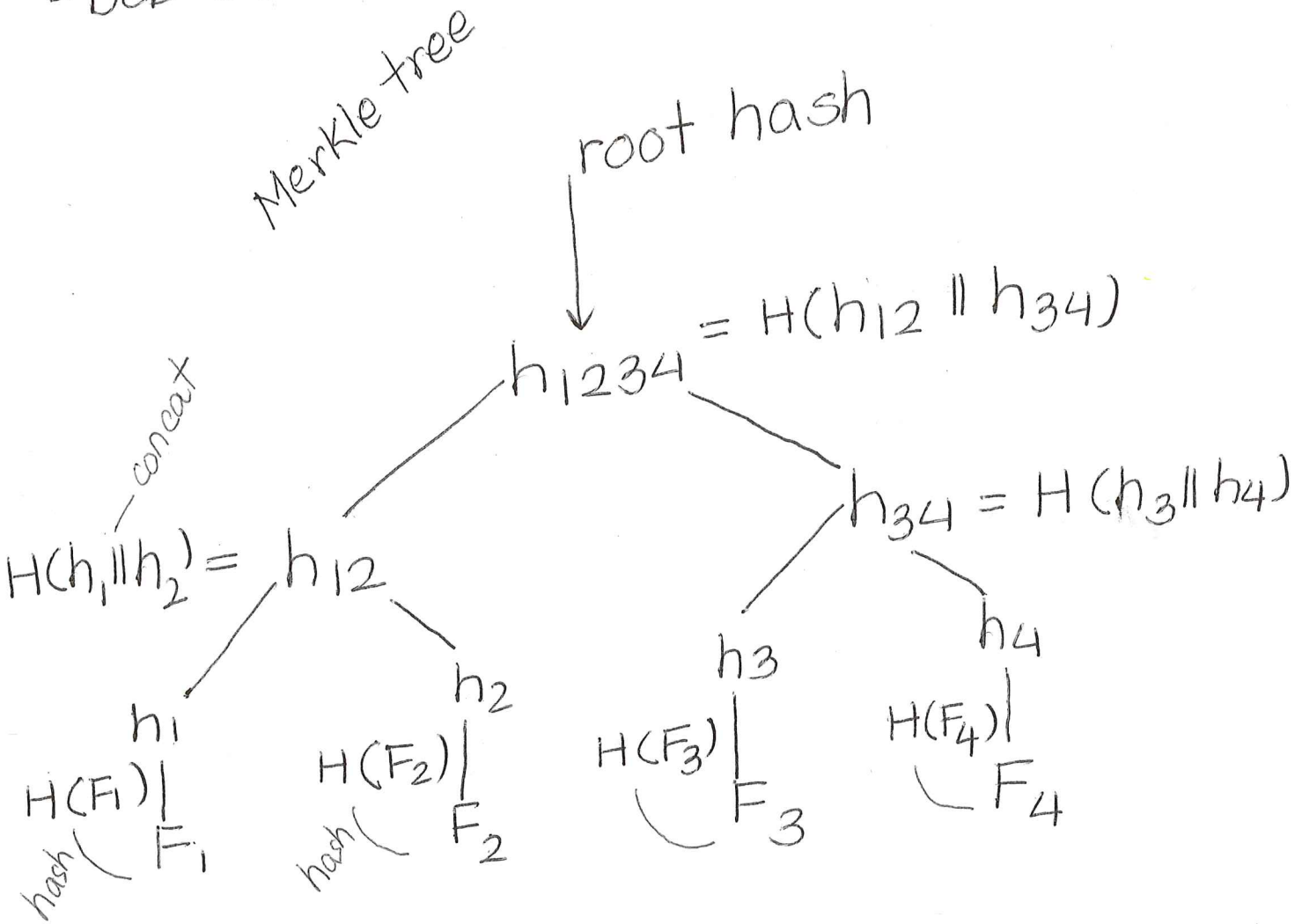


Is $F_2 = F_2'$?

F_1, F_2, F_3, F_4

- Bob doesn't want store files locally

Merkle tree



Bob stores h_{1234} locally F_1, F_2, F_3, F_4

small (256-bits)

Bob asks for File 2

F_2' <file>

h_1', h_{34}'' <proof $F_2 = F_2'$)

$h_2' = H(F_2')$

$h_{12}' = H(h_1' \| h_2')$

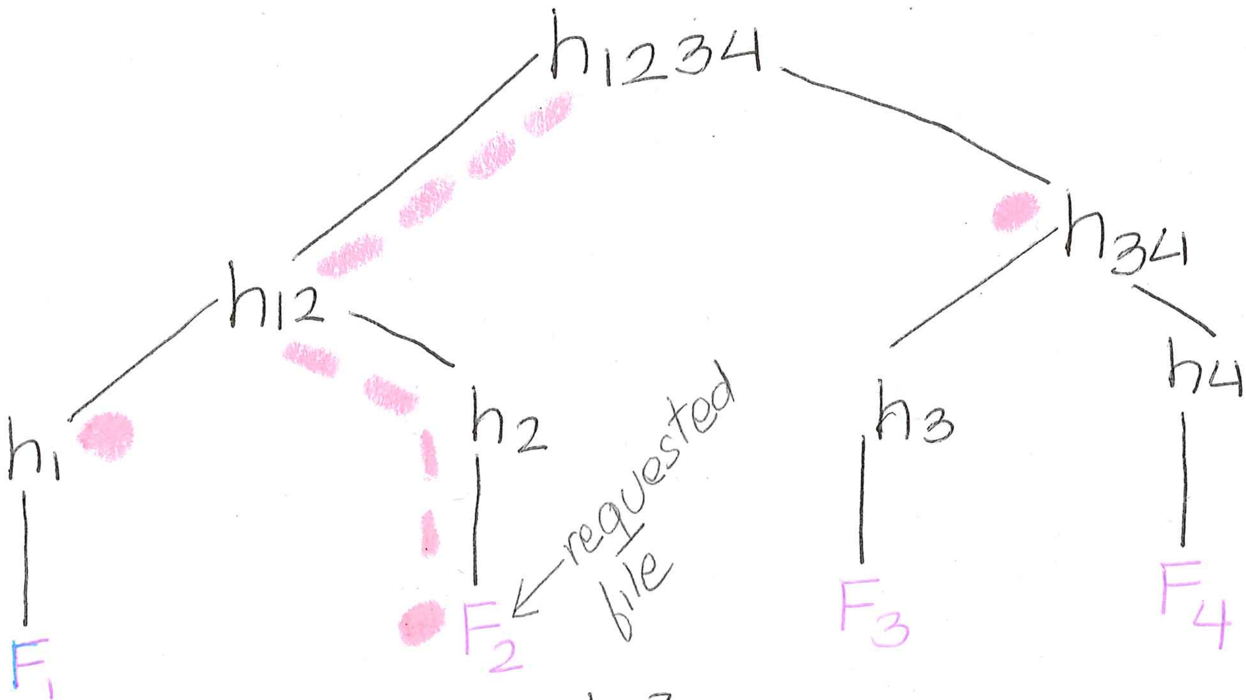
$h_{1234}' = H(h_{12}' \| h_{34}'')$

Is $h_{1234}' = h_{1234}$?

Bob checking the proof

Y → <file is right>

N → F_2 probably $\neq F_2'$



<u>Can server cheat bob?</u>

Bob sent to → $F_2 \neq F_2'$, h_1', h_{34}'

s.t.

$h_2 \neq h_2'$, $h_2 = h_2'$
$H(F_2) = H(F_2')$

$h_2' = H(F_2')$

$h_{12}' = H(h_1' \| h_2')$

$h_{1234}' = H(h_{12}' \| h_{34}')$ — Bob checks

$\|$

$H(h_{12} \| h_{34})$

$h_{1234} = h_{1234}'$

(I) $h_{12}' \neq h_{12}$ or
$h_{34}' \neq h_{34}$ then collision found.

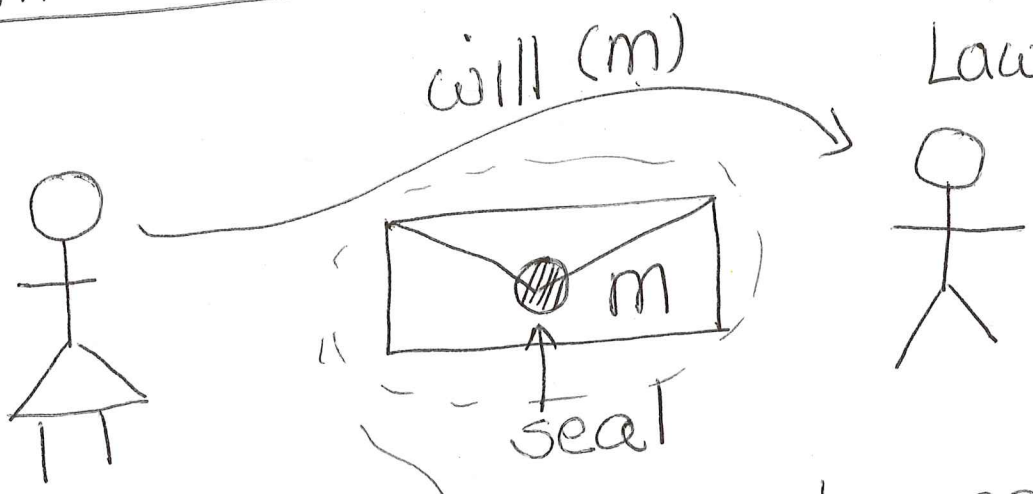
(II) $h_{12} = h_{12}'$ $H(h_1' \| h_2') = H(h_1 \| h_2)$

(III) $h_1' \neq h_1$ or $h_2 \neq h_2'$ $H(h_1' \| h_2') = h_{12}'$
$H(h_1 \| h_2) = h_{12}$
- collision found

(IV) $h_2 = h_2'$ $\neq$
$H(F_2) = H(F_2')$
collision found

Since collision ~~is~~ are hard to find, dropbox can't fool Bob

Commitment Schemes



- Hiding: the commitment reveals nothing about m
- Binding: can't open to another msg m' $(m \neq m')$

Sender (Alice) — Receiver (Lawyer)

$r \leftarrow \{0,1\}^n$ — commitment

$com := H(m \| r)$

$H(m \| r)$ — concat

sealed env.

open

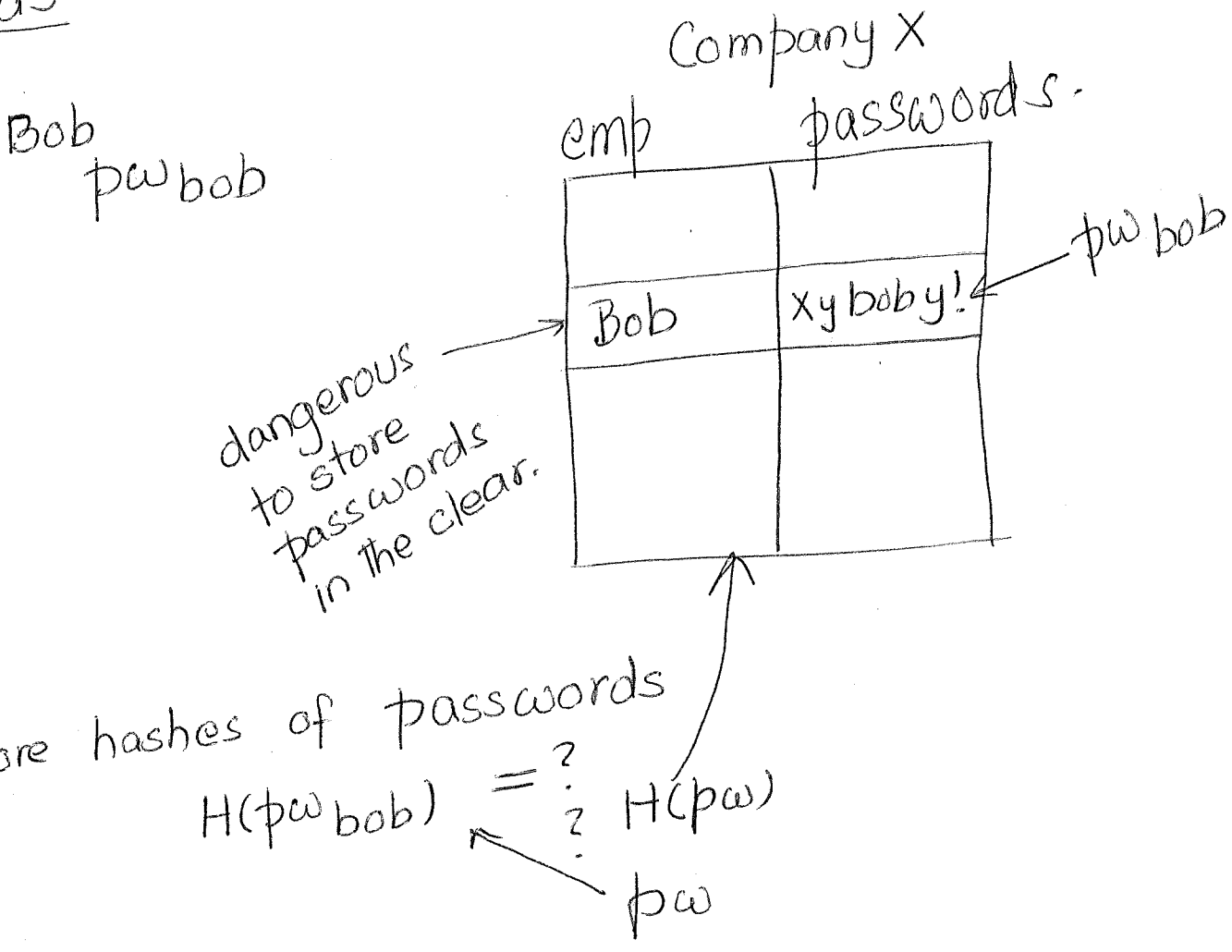
$H(m \| r) = com$?

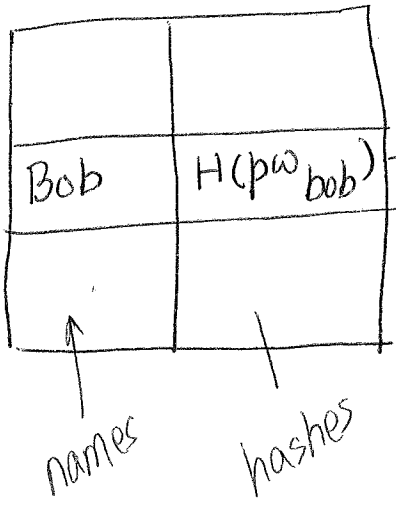
Hiding: $H(m' \| r)$ ← hides m

Binding: $H(m \| r) = H(m' \| r)$ $m \neq m'$

↑ collission

Passwords





exfiltrated → password crackers
- go through dictionary of common passwords once
- Use pre-processing.

- slow down hash

hashing I-times $H^{(I)}(pw)$ (e.g. $H^{1000}(pw)$) $H(\ldots) = H(pw)$

- Slows the attacker down.
- Not too bad for checking $H^{1000}(pw) = H^{1000}(pw')$?

- salting

store: $s, H(s, pw)$ (concat)

s: random salt

pw: password.

diff salts
- Bob: xy^2 ← Company
- Bob: xy^2 ← Bank

- Bob: cs435
- Alice: cs435

different salts

pre-processing doesn't work.

Last time

- Applications of hash functions
  - Merkle trees
  - Passwords

Logistics

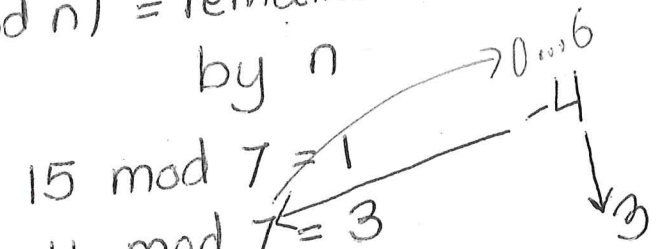
HW 4
Quiz 1 - grades

Oct 28, 2020

LectureLet 24

- Number Theory needed for public-key crypto

$a \pmod n$ = remainder when a is divided by n



$15 \bmod 7 = 1$

$-11 \bmod 7 = 3$

$a \pmod n = b \pmod n$

$a \equiv b \pmod n$

$\gcd(a,b)$: greatest common divisor

$\text{lcm}(a,b)$: least common multible

$\gcd(6, 15) = 3$ check!

$\text{lcm}(6, 15) = 30$

Extended ~~Euclid~~ Algorithm Euler's

$\text{gcd Euler}(x,y) = [c,a,b]$

$c = \gcd(x,y)$

$ax + by = c$

See Fig 1 (note)

Intuition:

same gcd ?

(x, y)
$(y, x \bmod y)$ ← written as $x \% y$

Basis for recursion

$(7, 15)$
↓
$(15, 7) \longrightarrow (7, 1)$
↓
$(1, 0)$ $(7 \bmod 1 = 0)$

$\gcd(1,0) = 1 = \gcd(7, 15)$

Fermat's little theorem (FLT)

p prime
any integer a satisfies $a^p \equiv a \pmod p$
$p \nmid a$, $a^{p-1} \equiv 1 \pmod p$

(e.g $5 \nmid 2$ ($5 = p$) $\quad 2^4 \equiv 1 \pmod 5$)

Groups

Think reals for intuition.

Group

$(G, \bullet)$ — G: non-empty set; $\bullet$: operation

[Ex: $(\mathbb{R}, +)$]

- [order doesn't matter] (I)

$a(bc) = (ab)c$ — associativity

- [every element has identity] (II)

$ae = ea = a$ — e: identity

- [every element has inverse] (III)

$a^{-1}a = aa^{-1} = e$ — a^{-1}: inverse

$Z_n = \{0, 1, 2, \dots, n-1\}$

$Z_7 = \{0, 1, 2, \dots, 6\}$

$(2+5) \bmod 7$

$\| $

0

- $(Z_n, +)$ is a group

$(i+j) \bmod n$

- I ✓, II ✓, III ✓

identity $= 0$

what about $-\{0\}$ ← exclude 0

$2 \cdot 5 = 3$

$(Z_n, \bullet)$

$(i \times j) \bmod n$

$(2 \times 5) \bmod 7$

$\| $

3

I ✓, II ✓, III ✗

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

↓ exclude

n	inverse
1	1
2	×
3	×
4	×
5	5

inverses don't exist

$$Z_n^* = \{ i \mid i \in Z_n \text{ and } \gcd(n, i) = 1 \}$$

n, i relatively prime

$Z_6^* = \{1, 5\}$

$(Z_n^*, \cdot)$ ← $(i * j) \bmod n$ or $(i \times j) \bmod n$

- I ✓
- II ✓ (1 is the identity)
- III $i \in Z_n^*$, $\gcd(n, i) = 1$

$ai + bn = 1$ (Extended Euler)

$ai \equiv 1 \pmod n$

$(a \bmod n)\, i \equiv 1 \pmod n$

↑ inverse

Size of Z_n^* = ?

$Z_6^* = \{1, 5\}$

$\varphi(n) = |Z_n^*|$

$Z_n^* \subseteq Z_n$

$|Z_n^*| \leq n-1$

- p prime

$Z_p = \{0, 1, \cdots, p-1\}$

$Z_p^* = \{1, 2, \cdots, p-1\}$

$\varphi(p) = |Z_p^*| = p-1$

- power of prime p^i $(i > 1)$ Ex: p^2

$Z_{p^i}^* = \{1, 2, \cdots p-1, p+1, \cdots, \{2p-1, \cdots\}$

p ↑ $2p$ ↑

multiples of p missing

$|Z_{p^i}^*| = p^i - p^{i-1} = \Phi(p^i)$ $i \geq 1$

p^{i-1} ↑ multiples of p

we know.

- General

$n = p_1^{i_1} \cdots p_k^{i_k}$

$\Phi(n) = \Phi(p_j^{i_1}) \cdots \Phi(p_k^{i_k})$

Ex:

$n = 3^2 5^3$

$\phi(n) = \phi(3^2) \cdot \phi(5^3)$ check!

$= (3^2 - 3) \cdot (5^3 - 5^2)$

$= 600$

Ex.

$Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$8 \pmod 7$

$2 \longrightarrow 4 \longrightarrow 1$ X

(3) $3 \longrightarrow 2 \longrightarrow 6 \longrightarrow 4 \longrightarrow 5 \longrightarrow 1$

$3^2 \quad 3^3 \quad 3^4 \quad 3^5 \quad 3^6$

$3^6 \equiv 1 \pmod 7$ FLT ✓

$(G, \cdot)$ is cyclic if there exists $g \in G$ s.t

generator $\longrightarrow \{g, g^2, g^3, \dots\} = G$

Z_7^* is cyclic, g is generator

prime

$g = 3$.

$\{3, 3^2, 3^3, 3^4, 3^5, 3^6\} = Z_7^*$

Fact 1: Z_p^*, is cyclic.

Alg. for finding generator. (NOT DONE)

assume + trust

Last time

- Number theory basics
  - Z_n, Z_n^*

Logistics

Lecture Let 25

Nov 1 2020

Chinese Remainder Theorem (CRT)

$m_1, \dots, m_r$ relatively prime — r positive integers, $\gcd(m_i, m_j) = 1$ for $i \neq j$

$M = m_1 \cdots m_r$

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{m_r}$$

x: variable; $a_1, \dots, a_r$: constants

solve for x

$x \equiv 3 \pmod 5$

Ex

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 2 \pmod 5$$

x: var

Uniqueness

two solutions — Alice: v, Bob: v'

"essentially same"

- $v \pmod{m_i} = a_i = v' \pmod{m_i}$ (remainder a_i)
- $v \equiv v' \pmod{m_i}$?
- $m_i \mid v - v'$ $(1 \le i \le r)$

$3 \mid a \Rightarrow 6 \mid a$

$2 \mid a$

$v \equiv v' \pmod M \Leftarrow M \mid v - v'$ $(M = m_1 \cdots m_r)$

Two solutions are congruent modulo M

Existence

$$M_1 = \frac{M}{m_1}, \quad M_2 = \frac{M}{m_2}, \quad \dots, \quad M_r = \frac{M}{m_r}$$

consider $M_1 = \frac{M}{m_1} = m_2 \cdots m_r$ $= m_1 \cdots m_r$

$\gcd(M_1, m_1) = 1$ $\quad (\mathbb{Z}_n^*)$, $i \in \mathbb{Z}_n^*$

$N_1 M_1 \equiv 1 \pmod{m_1}$

inverse

$i = 1$

m_i missing

$$M_i = \frac{M}{m_i} = m_1 \cdots m_{i-1}\, m_{i+1} \cdots m_r$$

$\gcd(M_i, m_i) = 1$

$N_i M_i \equiv 1 \pmod{m_i}$ $\quad (\mathbb{Z}_n^*)$

$2 \leftrightarrow 3, 5$

$2 \leftrightarrow 15$

$$v = \sum_{i=1}^{r} a_i M_i N_i$$

$M_i N_i \equiv 1 \pmod{m_i}$

$M_j N_j = 0 \pmod{m_i}$ $\quad j \neq i$

$j \neq i$

m_i

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_r \pmod{m_r}$

$v \pmod{m_i} = a_i \pmod{m_i}$ $\quad 1 \le i \le r$

$i = 1$

$a_1 M_1 N_1 + \cdots + a_r M_r N_r \pmod{m_1}$

$a_1 \equiv a_1$

0

$M_j = M / m_j$ (multiple m_i ($i \neq j$))

$i = 1, i = 2, \dots$

Ex:

$m_1=2 \quad m_2=3 \quad m_3=5 \quad M=30 = 2\times3\times5$

$x \equiv 1 \pmod 2$

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$M_1 = \frac{M}{2} = 15 \quad M_2 = \frac{M}{3} = 10 \quad M_3 = \frac{M}{5} = 6$

$N_1 = 1 \quad N_2 = 1 \quad N_3 = 1$

$M_1N_1 \equiv 1 \pmod 2 \quad M_2N_2 \equiv 1 \pmod 3 \quad M_3N_3 \equiv 1 \pmod 5$

$$v = \sum_{i=1}^{3} a_i M_i N_i$$

$= 1\cdot(15) + 10(2) + 6(2)$

$= 15 + 20 + 12$

$= 47$

$47 \equiv 1 \pmod 2 \quad 47 \equiv 2 \pmod 3 \quad 47 \equiv 2 \pmod 5$

Example

$m_1 = p \quad m_2 = q$ two primes

$M = pq \quad \phi(M) = (p-1)(q-1)$ (2)

RSA $\phi(M) \neq |Z_M|$

$M \nmid a \quad \phi(M)$

$a^{\phi(M)} \equiv a^{(p-1)(q-1)} \pmod p$ $\quad p \nmid a$

$= (a^{p-1})^{(q-1)} \pmod p$

$= 1 \quad (a^{p-1} \equiv 1 \pmod p$ FLT

Similarly $a^{\overbrace{(p-1)(q-1)}^{\Phi(M)}} \equiv 1 \pmod{q}$

switch roles of p, q

$a^{(p-1)(q-1)} \equiv 1 \pmod{p}$

$a^{(p-1)(q-1)} \equiv 1 \pmod{q}$

$\Phi(\overbrace{pq}^{M}) \equiv 1 \pmod{\underbrace{M}_{pq}}$

a

CRT

$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$

$\Phi(M) \equiv M$

$a^{\Phi(M)}$

Public-Key cryptography

- so far: $Enc_k(\cdot)$ $Dec_k(\cdot)$

use same key (symmetric key)

Public key

pk - key for encryption

$\neq$

sk - key for decryption

asymmetric key

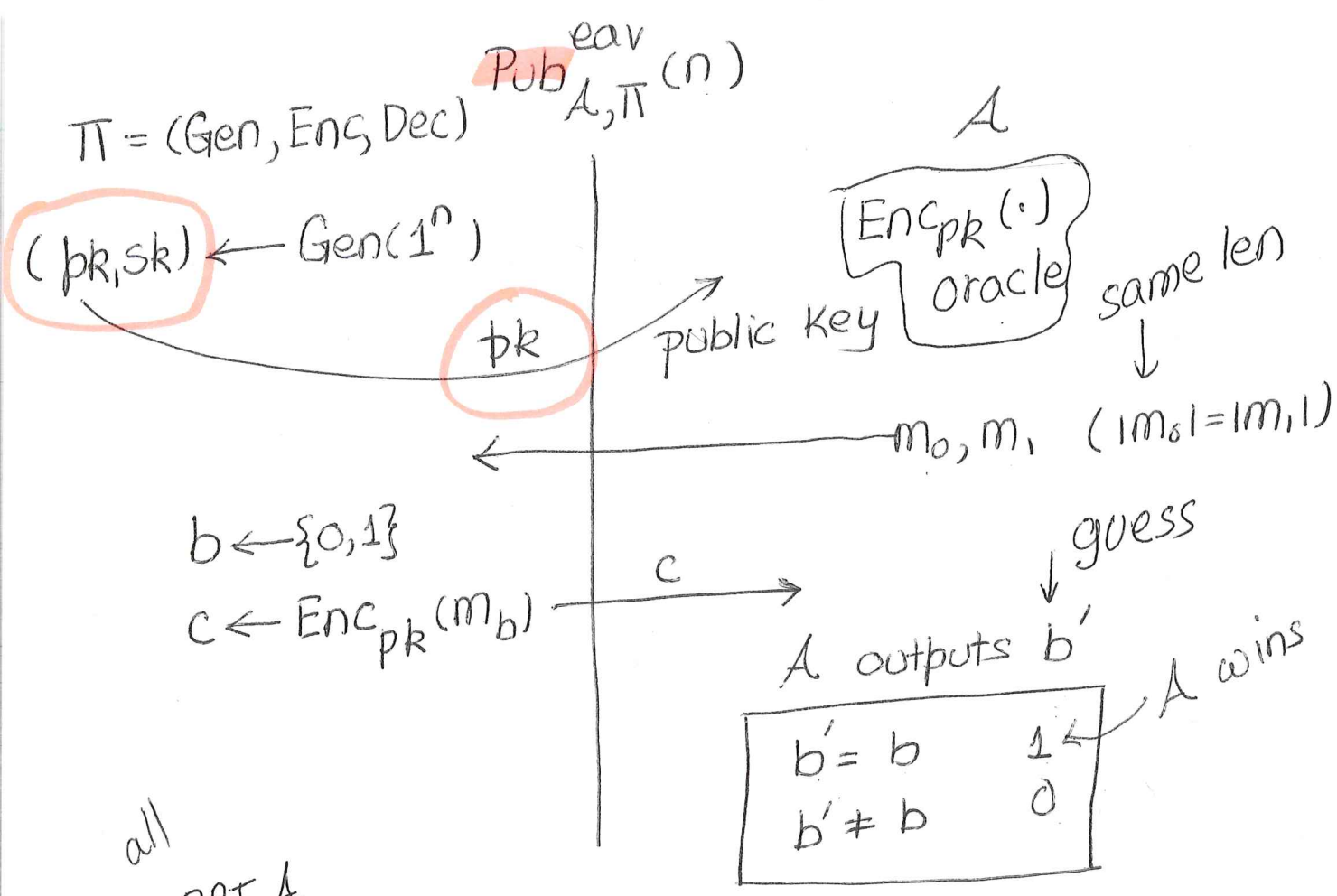
pk → directory → can be published.

(Gen, Enc, Dec)

- $(pk, sk) \leftarrow Gen(1^n)$ — 1^n: sec param
  - pk: public key
  - sk: secret key
  - Len of pk, sk depend on n
  - Len of pk, sk atleast n ($\geq n$)
- Enc: $c \leftarrow Enc_{pk}(m)$ <uses public key>
  - use randomness.
- Dec: $m := Dec_{sk}(c)$ <uses secret key>

$Dec_{sk}(Enc_{pk}(m)) = m$ ✓ Sanity check

Security definition ✓



For all PPT $\mathcal{A}$

$$\Pr\left[\text{Pub}^{eav}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \text{negl}(n)$$

- Giving pk to $\mathcal{A}$, Like giving encryption oracle.
- Remember CPA-security

* No deterministic scheme can be secure according to the definition based on $\text{Pub}^{eav}_{\mathcal{A},\Pi}(n)$