1)

CRYPTO — Lecture # 7 — 2 Feb 2016 — mb + VG

- NOTE: Today's NYT article on BANK THEFTS by Tellers.
- For today's lecture, WIKI on YAO's MILLIONAIRES PROBLEM is EXCELLENT.

- Some comments: Generation of primes: EASY. Integer factorization: HARD.
  - Wolfram alpha finds nextprime[randominteger(10^{250})] ← a 250 integer #. in a fraction of a sec on iphone 6.
  - FACTORING 100 digit nos, product of 2 randomly chosen 50-digit numbers is possible but hugely expensive (6 mos on 100,000 work stations In 2000)
  - NSA ← National Security Agency suggests using a product of 2 500 digit primes.
  - YAO's MILLIONAIRES PROBLEM. (see Wiki): {How can A + B determine which of them is richer w/o disclosing their wealth? HONEST but CURIOUS Model.

- OT (oblivious transfer):

① A selects at random two n-digit primes P_1, P_2 & sets $N = P_1 \cdot P_2$.
← n large eg n = 100 decimal digits

② A → B: N

③ B selects $x \in_u \mathbb{Z}_N^*$ (for typical unfactorizable N, $x \in_u \mathbb{Z}_N$ i.e. $1 \le x < N$ ← uniformly chosen at random, will have $x \in \mathbb{Z}_N^*$)

Computes $x^2 \bmod N$

④ B → A: $x^2 \bmod N$

Known to A but not to B — How?

⑤ A computes $\underbrace{\sqrt{x^2} \bmod P_1}_{= \pm x_1}$ & $\underbrace{\sqrt{x^2} \bmod P_2}_{= \pm x_2}$ to get $\pm x \bmod P_1$ and $\pm x \bmod P_2$

$\pm x_1$ $\pm x_2$ in CRF {Chinese Remainder Form

Now A has $\sqrt{x^2} \bmod N = \langle \pm x_1, \pm x_2 \rangle$

Set $x = \langle +x_1, +x_2 \rangle$, $y = \langle +x_1, -x_2 \rangle$

Then $\sqrt{x^2} \bmod N = \pm x, \pm y$. {These are all the possibilities. Why?

B chose either $\pm x$ or $\pm y$. {A knows this, but has no way to decide which one B chose. Why?

⑥ A → B: One of $\pm x, \pm y$ chosen at random by A.

If B gets $\pm x$ (having chosen x initially), he gets nothing from A (that he doesn't already have.

If B gets $\pm y$, he can factor N. Why?

This is because $(x \pm y, N) = P_1$ or P_2.

because $x+y = \langle x, x \rangle + \langle x, -x \rangle = \langle 2x, 0 \rangle$, Say.

$\therefore P_2 \mid x+y$. But $P_1 \nmid x+y$ because $0 < x_y < N$

$P_1 \mid x+y \Rightarrow P_1 \mid 2x \Rightarrow N \mid 2x \Rightarrow N \mid x$ →← ($x+y = \langle 2x, 0 \rangle$; $P_1, P_2 > 2$; $1 \le x < N$)

$\therefore \gcd(x+y, N) = P_2$.

2)

How to compute $\sqrt{\ }$ mod P in the case that $P \equiv 3 \bmod 4$

If $P \equiv 3 \bmod 4$

Then $\sqrt{x} \bmod P = ?$

Use $x^P \bmod P = x$ for all x

$\therefore \quad x^{P+1} \bmod P = x^2$

P is odd $\therefore \quad x^{\frac{P+1}{4}} \bmod P = \pm\sqrt{x}$

$\leftarrow P \equiv 3 \bmod 4 \therefore 4 \mid P+1$

If $P \not\equiv 3 \bmod 4$

Can always compute sqrts mod P, but especially easy if $P \equiv 3 \bmod 4$.

Harder if $P \equiv 3 \bmod 8$

Randomizing algs if $P \equiv 1 \bmod 8$

EXAMPLE:

$N = P_1 \cdot P_2 = 3 \cdot 11 = 33$

$x = 17$

$x^2 \bmod N = 25 \qquad \therefore \quad x = \pm 17 = \pm 16, \ \pm 5$

$\qquad\qquad\qquad\qquad = \pm(1, 5) \qquad\qquad = \pm(2, 5)$

$17 \pm 5 = 22, \ 12$

$(22, 33) = 11 \quad ; \quad (12, 33) = 3$

Let $\quad x = \langle x \bmod P_1, \ x \bmod P_2 \rangle$

$\qquad x^2 = \langle x^2 \bmod P_1, \ x^2 \bmod P_2 \rangle$

$x^2 \pmod N$ has 4 sq roots: $\langle \pm \underbrace{x \bmod P_1}_{x_1}, \ \pm \underbrace{x \bmod P_2}_{x_2} \rangle$

If $\quad x = \langle x_1, x_2 \rangle \quad \& \quad y = \langle x_1, -x_2 \rangle$

Then $\quad x^2 = y^2 \bmod N$

$\qquad x + y = \langle \overset{\neq 0}{2x_1}, 0 \rangle. \qquad \gcd(x+y, N) = P_2.$

$\qquad x - y = \langle 0, 2x_2 \rangle \qquad (x-y, N) = P_1.$

3) Assume FACTORING is hard ~~&~~ virtually impossible.

<u>Standard OT</u>: A has secret P_1, P_2 s.t. $N = P_1 \cdot P_2$

B gets secret w. probab $= 50\%$ (not $\approx 50\%$ under the assumption That Factoring N is virtually impossible.)

A does not know if B got secret.

<u>1 of 2 OT</u>:

A has 2 secrets.

B gets 1 or the other.

A does not know which he got.

Initially, B has no choice which secret to get.

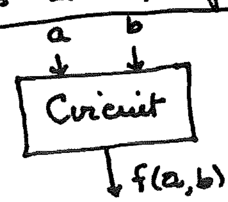
Later, B <u>will</u> be able to choose

For example, if B knows That 1 secret is odd and The other secret is even, B will be able to get The odd one, say, wo letting on to A that he wants odd.

↑ For This, we assume existence of a 1-way fnctn f. This f is for B to prove to A when he got neither secret. → If he got neither, he proves it by showing he had sent $f(x \cdot r)$ to A.

In this case The process repeats.

<u>SOLUTION TO YAO's PROBLEM using The 1 of 2 OT</u>:



a is A's secret info, a single bit

b is B's secret info, a single bit

for the special case where each has either \$1M (denoted by 1) or \$2M (denoted by 0).

A → B: <u>$f(a,0)$</u>, and <u>$f(a,1)$</u>, in such a way That B can access just one.

The correct answer if $b=0$. — if $b=1$.

In The honest but curious model, B accesses $f(a, b)$: ← B's bit

This is done as follows:

A → B: 1 of 2 OT (k_s, k_t). B gets one of <u>k_s</u>, <u>k_t</u>. A doesn't know which.

B → A: Which of <u>$f(a,0)$</u>, <u>$f(a,1)$</u> should go into box locked w. k_s.

A puts <u>$f(a,0)$</u> in box locked with <u>k_s</u>, <u>say</u>

" " <u>$f(a,1)$</u> " " " <u>k_t</u>. } as requested by B.

A doesn't know which of <u>$f(a,0)$</u>, <u>$f(a,1)$</u> B got.

<u>NEXT UP</u>: Implementation of the <u>1 of 2 OT</u>.

4)

- Assume FACTORING is IMPOSSIBLY HARD. (This will fail when Quantum Computing exists)

<u>Standard OT:</u> ① A has a secret, namely the primes P_1, P_2 s.t. $N = P_1 \cdot P_2$.

B gets the secret with probability $= 50\%$.

Under the assumption that factoring N is impossibly hard, this is not $\approx$: it is $=$.

A does not know if B got the secret.

<u>1?2 OT</u> ② A more powerful (1?2) OT is one where A has 2 secrets, ~~and~~ B gets 1 or the other, A does not know which one he got (& B has no choice in which one he gets).

For this, I assume $\exists$ 1-way functn f.

OT: ① A selects 3 primes P_1, P_2, P_3 {independently & uniformly at random from the set of n-digit primes. Set $N = P_1 \cdot P_2 \cdot P_3$.

② $A \to B$: N

③ B selects $x \in_u \{1, 2, \ldots, N-1\}$ at random & computes $x^2 \bmod N$ and $f(x \circ r)$ for some random r.

④ $B \to A$: $x^2 \bmod N$ and $f(x \circ r)$

⑤ A computes $\pm w, \pm x, \pm y, \pm z$ s.t. $x^2 \bmod N = \underbrace{w^2 = x^2 = y^2 = z^2}$.

A knows the 8 square roots of $x^2 \bmod N$, but does not know r & $\therefore$ cannot determine which root B chose.

⑥ $A \to B$: one of w, x, y, z.

⑦ B: If B gets x, he reveals r and the process restarts at ③. Else

⑧ B gets $w, y,$ or z. Together with x, B can use this to compute exactly <u>one</u> of P_1, P_2, P_3.

A does not know if B got $\underline{P_1, P_2}$ or $\underline{P_3}$. Only that he got just one.

The primes P_1, P_2, P_3 can be made keys to locked boxes

(A generates random primes Q_1, Q_2, Q_3. Then

A sets $N_1 = P_1 \cdot Q_1$, $N_2 = P_2 \cdot Q_2$, $N_3 = P_3 \cdot Q_3$.

A encrypts messages M_i under N_i for $i = 1, 2, 3$.

B will get one of M_1, M_2, M_3 & A won't know which.

5) All congruent to 3 mod 4 to make it easy to compute sq roots

$N = 3 \cdot 7 \cdot 11 = \underline{231}$

$x = 53 \qquad x^2 \bmod N = 37$

$37 = \langle 37 \bmod 3,\ 37 \bmod 7,\ 37 \bmod 11 \rangle = \langle 1, 2, 4 \rangle$

$\sqrt{x^2 \bmod P} = 37^{\frac{P+1}{4}} \bmod P = \langle 1,\ 2^{\frac{7+1}{4}} \bmod 7,\ 4^{\frac{11+1}{4}} \bmod 11 \rangle = \langle 1, 4, 9 \rangle$

Check: $\langle 1,4,9 \rangle \cdot \langle 1,4,9 \rangle = \langle 1,2,4 \rangle$ ✓

$\cancel{P \equiv 3 \bmod 4}$

$\cancel{P+1 \equiv 0 \bmod 4}$

$\cancel{x^{\frac{P+1}{2}} = \left(x^{\frac{P+1}{4}}\right)^2}$

$x^P \equiv x \bmod P$

$x^{P+1} \equiv x^2 \bmod P$

$x^{\frac{P+1}{2}} \equiv \pm x \bmod P$

$x^{\frac{P+1}{4}} \equiv \pm\sqrt{x} \bmod P$

Roots of $x^2 \bmod N = 37 = \langle 1,2,4 \rangle$ are $\langle \pm 1, \pm 4, \pm 9 \rangle$

Check: $7 \cdot 11 = 77 = \langle 77 \bmod 3, 0, 0 \rangle = \langle 2, 0, 0 \rangle$

$3 \cdot 11 = 33 = \langle 0, 5, 0 \rangle$

$3 \cdot 7 = 21 = \langle 0, 0, 10 \rangle$

$\therefore \langle 1,0,0 \rangle = 2 \cdot 77 \bmod 231 = 154$

$\langle 0,1,0 \rangle = 3 \cdot 33 = 99 \bmod 231 = 99$

$\langle 0,0,1 \rangle = 10 \cdot 21 = 210 = -21$

$\therefore \langle 1,4,9 \rangle = 154 + 4 \cdot 99 + 9 \cdot (-21) = 361 \bmod 231 = 130$

$\langle 1,-4,9 \rangle = 154 - 4 \cdot 99 + 9(-21) = 31$

$\langle 1,4,-9 \rangle = 46$

$\langle 1,-4,-9 \rangle = 178$

$\therefore (130+31, \overset{231}{N}) = (161, 231) = 7 \qquad (130+46, N) = (176, 231) = 11$

$(130+178, N) = (308, N) = 77 \rightarrow 3, \qquad (31+46, N) = (77, N) = 77 \rightarrow 3$

$(31+178, N) = (209, N) = 11, \qquad (46+178, N) = (224, N) = 7$