Oct20

Tuesday, October 20, 2020 9:58 AM

Comments on Project 1 +ε

① Get in the habit of always doing integer division w/ `a//b`.

* even if $b|a$ b/c sage saves $a/b \in \mathbb{Q}$.

② E.E.A.(a,b) to get $au+bv=1$

to get $a^{-1}\equiv u \mod b$

No guarantee $0 \le u < b$

Replace u w/ $u\%b$ when trying to find an inverse.

e.g. getInverse fn.

③ intToText & textToInt should not live inside of our Cryptosystems (i.e. encrypt & decrypt functions).

$$\begin{tikzcd}
\text{Pics} \arrow[dr, "\text{scheme}"] & & \\
\text{Ascii} \arrow[r] & M \arrow[r, "e"] & C \\
\text{Strings} \arrow[ur] & \mathbb{Z}/N\mathbb{Z} \arrow[u, phantom, sloped, "\subseteq"] &
\end{tikzcd}$$

Recall:

Defn An integer a is a quadratic residue modulo a prime p if $p \nmid a$ & a has a square root mod p.

The Legendre Symbol is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a qr} \\ -1 & a \text{ is a nr} \\ 0 & \text{if } p \mid a. \end{cases}$$

Prop This has nice properties

* $$\underline{\left(\frac{a}{p}\right)} = a^{p-1/2} \bmod p \underset{\substack{\uparrow \\ \text{HW6} \\ p\nmid a.\ g\in\mathbb{F}_p \\ \text{prim root}}}{=} \boxed{(-1)^{\log_g a}}$$

* Multiplicative & only depends on class of a mod p.

Remark

* Legendre symbol is easy to compute

* Discrete log hard to compute

* But... since $\left(\frac{a}{p}\right) = \underline{(-1)}^{\log_g a}$ ← easy to compute whether $\log_g a$ is even or odd.

$$\rightsquigarrow \log_g a = \begin{cases} \text{even} & \text{if } \underset{\leftarrow}{a}^{\frac{p-1}{2}} \equiv 1 \mod p \\ \text{odd} & \text{if } a^{\frac{p-1}{2}} \equiv -1 \mod p \end{cases}$$

Slogan

The last bit of the discrete log is insecure.

(HW)

Generalize this to the last k bits of discrete log are insecure if

$$p-1 = 2^k \cdot m$$

Rmk

Comes back to philosophy of "Security of p related to the factors of $p-1$"

What if base of Legendre is not prime?

Defn Let b^* be an odd positive int. Then the Jacobi Symbol is:

$*\; b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_t}\right)^{\alpha_t}$$

Legendre symbols defined in terms of quad residues.

This is multiplicative in a & b and only depends on residue of a mod b.

Theorem (Quad Reciprocity).

a, b odd & positive.

$$\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & a \text{ or } b \equiv 1 \bmod 4 \\ -\left(\frac{b}{a}\right) & a \ \& \ b \equiv 3 \bmod 4. \end{cases}$$

useful computational tool.

Questions

$*\; \left(\frac{a}{b}\right) \equiv a^{b-1/2} \bmod b$? NO!

* $\left(\frac{a}{b}\right) = 1$ is a a square mod b? NO! (if b not prime)

Case $b = pq$ $\quad p \neq q$

$$1 = \left(\frac{a}{b}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right)$$

HW5 #9

Both $= 1$ (CRT $\vee$ a is square mod b)

Both $= -1$ (a not a square mod b)

Exercise

$b = p^2$ $\quad (a, b) = 1$

$\Rightarrow \left(\frac{a}{b}\right) = 1$

Example $p = 3$ $\quad q = 5$.

$$* \left(\frac{4}{15}\right) = \left(\frac{4}{3}\right) \cdot \left(\frac{4}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{4}{5}\right)$$
$$= 1 \cdot 1$$

$4 = 2^2$ mod 15

$$* \underline{\left(\frac{2}{15}\right)} = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = \underline{1}$$

Squares mod $15 = \underline{\{1, 4, 9, 10, 6\}} \not\ni 2$

Lemma: $b = pq$

$\left(\frac{a}{b}\right)=1$ a square mod b

$$\Longleftrightarrow \underline{\left(\frac{a}{p}\right)} = \underline{\left(\frac{a}{q}\right)} = 1$$

Proof Above ✓

Problem:

① Easy to compute $\left(\frac{a}{pq}\right)$ (even if you don't know p, q).

e.g. $\left(\frac{a}{pq}\right) = \pm\left(\frac{pq}{a}\right) \xrightarrow{\text{reduce}} \ldots$

② Hard to tell if a is a square modulo pq.

③ Easy to tell if you know p & q.

Goldwater-Micali Cryptosystem

Goal: Send messages from small message spaces $\mathcal{M}$.

For us $\mathcal{M}=\{0,1\}$.

Setup/Ex

Alice send Bob a 0 or a 1.

(Eve knows this).

Alice sends c to Bob.

Eve encrypts $c_0 = e(0)$

$c_1 = e(1)$

If $c_0 = c$ Eve knows $m = 0$

" $c_1 = c$ " " $m = 1$.

Goldwater & Micali introduce probabilistic encryption to solve this proble. Idea: Introduce Noise

Abstract Formulation

Alice chooses m = message.

r = random #.

$e(m,r)$ ← vary randomly as r does.

idea $m_1 \neq m_2$

$S_1 = \{e(m_1, r)\ \ r \text{ varies}\}$

$S_2 = \{e(m_2, r)\ \ r \text{ varies}\}$

look indistinguishable

Implementation ($\mathcal{M} = \{0,1\}$)

Hard Problem

p, q secret primes. $N = pq$. For a given a, determine if a is a square mod N

Trap Door

Knowing p, q, compute $\left(\frac{a}{p}\right)$ & $\left(\frac{a}{q}\right)$

If both $=1$ then QS

Eve's Challenge

She can compute $\left(\frac{a}{N}\right) = 1$. Doesn't help.

(rmk, if $\left(\frac{a}{N}\right) = -1$ then a not a square).

Bob

Key Creation

secret primes p, q. Choose a

w/ $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$

Publishes

$(N = pq, a)$

Eve

Alice

message.

Encryption $m = 0, 1$

Choose random $1 < r < N$.

$\sqrt{N}$

Computes

$$c = \begin{cases} r^2 \bmod N & m=0 \\ ar^2 \bmod N & m=1 \end{cases}$$

$$\left(\frac{c}{N}\right) = \left(\frac{r^2}{N}\right) \overset{?}{=} \left(\frac{a}{N}\right)$$

1 or $1 \cdot 1$

Decryption

$$m = \begin{cases} 0 & \left(\frac{c}{p}\right) = 1 \\ 1 & \left(\frac{c}{p}\right) = -1 \end{cases}$$

Proof of Correctness

If $c = r^2 \implies \left(\frac{c}{p}\right) = \left(\frac{r^2}{p}\right) = 1$

If $c = ar^2 \Rightarrow \left(\frac{c}{p}\right) = \left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{r^2}{p}\right) = -1$

Eve's Challenge

$m = 0$ ciphers = { squares mod N }

$m = 1$ ciphers = { nonsquares c w/ $\left(\frac{c}{N}\right) = 1$ }

*① Factor N gives alg to check.

HARD

*② Make the lists.

HARD.

*③ **Attack:** Check if c is a square in $\mathbb{Z}$.

$1, 4, 9, 16, 25, \ldots < N$.

Alice must choose $r \geq \sqrt{N}$.

If $r^2 =$ one of these, find a new r.

Example

$p = 3, q = 5. \quad a = 8.$

Bob publish

$(N = 15, a = 8)$

Bob Decrypts

$\left(\frac{10}{3}\right) = \left(\frac{1}{3}\right) = 1 \rightsquigarrow m = 0$

Alice chooses

$r = 5$

$m = 0 \rightsquigarrow c = r^2 = 25 \equiv 10$

$m = 1 \rightsquigarrow c = 8 \cdot r^2 \equiv 5 \mod 15$

$\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$

$\boxed{m = 1}$

Remark:

- Each bit of plaintexts must be encrypted w/ N of cryptographic size ($N \sim 2^{1000}$)
- k bit plaintext ⇝ $1000k$ bit cipher.

"Message scales by 1000"

HW Implement this system.

Digital Signatures

↑ verify senders, verify documents are approved by sender & not forged.

setup

Samantha the signers.

Victor the verifyer.

Goal

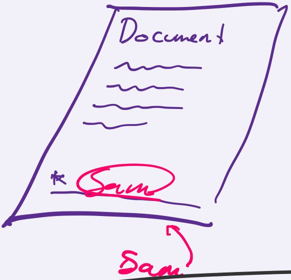
Document: D.

Samantha creates a "signed document" D^{sig} shows that she approves of D.

Victors confirms D^{sig} is D signed by Samantha.

Example D = Paper document

D^{sig} = Signed Document.



verify that this Document was indeed signed by Sam.

Formalism

Signing

* K^{priv} = Private signing key.

↑ private

* SIGN = Algorithm:

Input	output
D - document	D^{sig} - signed document.
K^{priv} - signature	

Verification

* K^{pub} - Public verification key (associated to K^{priv}).

* VERIFY = Alg:

Input $\dashrightarrow$ **Output**

D - document

D^{sig} - signature

K^{pub} - verify key

TRUE if D signed by K^{prv} is D^{sig}

FALSE otherwise.

Example (BAD).

- Make K^{prv} public then Victor can check if $K^{prv}: D = D^{sig}$ by just doing it.
- Bad b/c then anyone can sign as samantha.

Considerations

- Given K^{pub} an attacker cannot determine K^{prv} & also cannot determine any signing mechanism giving same signatures.
- Give K^{pub}, $D_1, \ldots, D_n$ & $D_1^{sig}, \ldots, D_n^{sig}$ I cannot determine D^{sig} from any other D.