Number Theory:

RSA

02/24

Prof. Forest

Warm up

① Discuss with your neighbors, are cupcakes better than cookies?

② $6^{10} \mod 11 = ?$

1

$6 \equiv 6 \mod 11$

$6^2 \equiv 6^2 \mod 11$

Midterm Exam

Topics

1. Sets, Functions
2. Logic (Propositional, Predicate)
3. Number theory

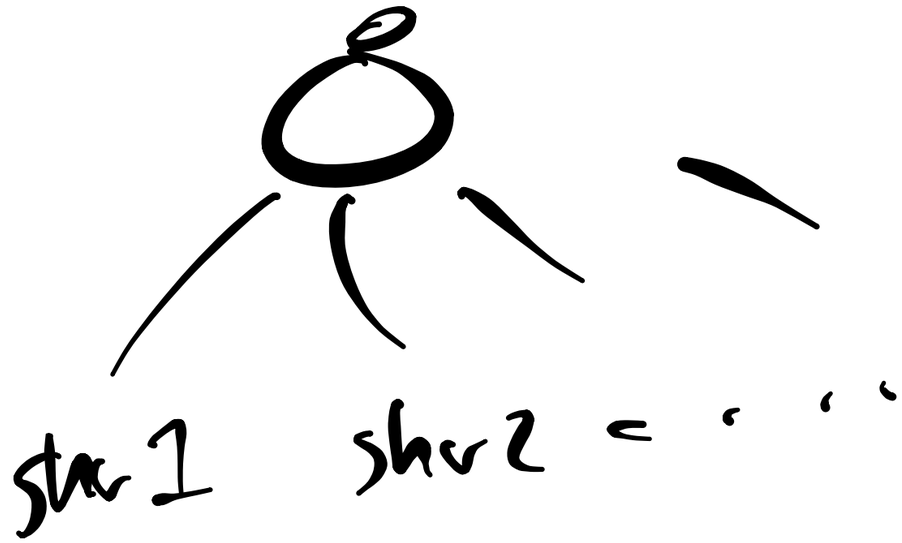
Skill

Basic proof
1. direct
2. contrapositive
3. Cases
4. contradiction

~3 questions covering key parts of each topic and evaluating your proof skills

RSA

SSS



RSA

$p = 5 \quad q = 11$

public key

private key

$n = p \cdot q = 55$

$(p-1)(q-1) = (4)(10) = 40$

$\gcd(e, 40) = 1$

$e = 7$

$d = e^{-1} \quad \mathbb{Z}_{40}$

$d \cdot e \equiv 1 \mod 40$

$d = 23$

private : $\langle 23, 55 \rangle$

$\langle d, n \rangle$

public : $\langle e, n \rangle$

: $\langle 7, 55 \rangle$

private : $(23, 55)$ public key : $(7, 55)$

$m = 13$

$$c = m^e \bmod n$$
$$= 13^7 \bmod 55$$
$$= 7$$

$$m' = 7^{23} \bmod 55 = 13$$
$$c^d \bmod n$$

① Pair up w/ someone

② take 2 notecards

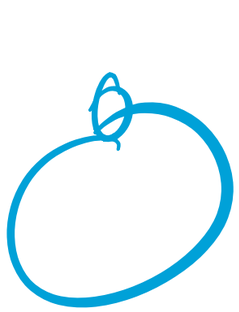
③ create a public and private key

④ write private key on one and public key on another card

⑤ Hide your secret work

⑥ Exchange public keys w/ another group

⑦ communicate a message securely to one another



public key

m → c →

private key

m

The Chinese Remainder Theorem (Sunzi's Theorem)

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers (i.e. $\gcd(m_i, m_j) = 1$ for all i, j $i \neq j$) greater than 1 and $a_1, a_2, \ldots, a_n$ be arbitrary integers. Then the system has a unique solution modulo $m = m_1 m_2 \cdots m_n$

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

Fermat's Little Theorem (or the French Remainder Theorem)

If p is prime and a is an integer not divisible by p. Then

$$a^{p-1} \equiv 1 \pmod{p}$$

Lemma 1

$$a \bmod b \equiv (a \bmod bc) \bmod b$$

Lemma 2

$$a^b \bmod k = (a \bmod k)^b \bmod k$$

Lemma 3

$$ab \bmod k = (a \bmod k \quad b \bmod k) \bmod k$$

Corollary 1

Let m_1, m_2 be relatively prime and $m_1 \neq m_2$. If $b \equiv x \pmod{m_1}$ and $b \equiv x \pmod{m_2}$ Then $b \equiv x \pmod{m_1 m_2}$

$m' \equiv m \bmod n$

$m' \equiv m \bmod p$

$m' \equiv m \bmod a$

then $m' \equiv m \bmod p$

Lemma 4: Let p be a prime number. For any $a, k \in \mathbb{Z}$, $p \mid ak$ if and only if $p \mid a$

$a = 6$ $p = 3$
$k = 2$
$3 \mid 2 \cdot 6$ and $3 \mid 6$

$a = 8$ $p = 3$
$k = 2$
$3 \nmid 8$ so $3 \nmid 8 \cdot 2$

p q

/

$n = p \cdot q$

n

p has more
200 digits

takes more time to factor n
into p and q than the
life of any human.

Theorem: RSA correctness

Let there be a public key $\langle e, n \rangle$ and a private key $\langle d, n \rangle$. For any integer message m

$$m \equiv \underbrace{(m^e \bmod n)}_{\text{encrypt}}^{d} \bmod n$$

decrypt

That is, you can decrypt (using your private key) accurately any message encrypted w/ your public key

Proof of RSA Correctness

Goal: show $m' \equiv m \mod n$ where $m' = (m^e \bmod n)^d \bmod n$.

Let's first show $m' \equiv m \mod p$.

Goal: show $m' \mod p = m \mod p$.

$$m' \bmod p = \left[(m^e \bmod n)^d \bmod n \right] \bmod p$$

$$= (m^{ed} \bmod n) \bmod p \quad \text{by Lemma 2}$$

$$= [m^{ed} \bmod pq] \bmod p \quad \text{by definition of } n$$

$$= m^{ed} \bmod p \quad \text{by Lemma 1}$$

$$= m^{k(p-1)(q-1)+1} \bmod p \quad \text{by def of } e$$

$$= m \cdot m^{k(p-1)(q-1)} \bmod p \quad \text{by laws of exponents}$$

$$= [m \bmod p \cdot m^{k(p-1)(q-1)} \bmod p] \bmod p \quad \text{by Lemma 3}$$

$$= [m \bmod p \cdot (m^{k(q-1)} \bmod p)^{(p-1)} \bmod p] \bmod p \quad \text{by Lemma 2}$$

$(m^{k(q-1)} \bmod p)^{p-1} \bmod p$ looks like $a^{p-1} \bmod p$

this opens up 2 cases.

Case 1. $m^{k(q-1)} \bmod p \not\equiv 0 \pmod p$ meaning $p \nmid m^{k(q-1)} \bmod p$ so Fermat's Theorem holds. therefore

$$m' = [m \bmod p \cdot 1] \bmod p$$

$$= m \bmod p$$

Case 2. $m^{k(q-1)} \bmod p \equiv 0 \pmod p$ so $p \mid m^{k(q-1)} \bmod p$ which means Fermat's Little Theorem does not hold.

In this case though by Lemma 4 $p \mid m$ so

$$m \equiv 0 \bmod p$$

and

$$\begin{aligned} m' &= [\, m \bmod p \cdot 0 \,] \bmod p \\ &= 0 \bmod p \\ &\geq 0 \end{aligned}$$

$$m' \equiv m \bmod p$$

therefore $m' \equiv m \bmod p$. Similarly (left as an exercise)

$m' \equiv m \bmod q$.

therefore by Corollary 1

$$m' \equiv m \bmod pq$$

or

$$m' \equiv m \bmod n$$

□