Math 451

~~Q's~~ revolution.csv

Group

A = [0 0 1 1 0 0 0;
0 0 1 1 0 1 1;
0 0 1 0 0 0 0;
0 0 1 0 0 1 0;
1 0 0 0 0 0 0;
0 0 0 0 0 0 1;
0 0 0 0 0 0 1;
⋮
];

People

p_1 ← (c:?) — p_2

PeoplePeople = A * A'

Note: Costs?

Report

proj 7

proj7.pdf ← only uploaded by group leader

everyone: text field

grading: Your sub-group = person1, person2, ...

sub-group leader = person

group leader = person → ex A b/c ...

you = you → ex D b/c (....)

Summary & desc

RSA

p, q are primes

let $n = pq$ $\quad m = (p-1)(q-1)$

pick e such that $\boxed{\gcd(e, m) = 1}$

so e has an inv. under mod m

find $d = e^{-1}$ inv. mod m

total numbers: p, q, n, m, e, d

encryption: $\boxed{c = p^e \bmod n}$ $\quad$ use powermod

$\boxed{p = c^d \bmod n}$

$x^y \bmod z = \text{powermod}(x, y, z)$

Alice: (RSA/Coded/ public key crypto)

① give (e, n) to everyone

② use (e, n) to encrypt their message before sending it.

typically "Mark was here"

block out pairs "Mar" "kwa" "s " "her" "ewa"

for this class → use "blocks" of chr

ex) 3 digits for each char

$$p = p + 68$$

---

block sizes $\quad \boxed{s_1 s_2} s_3 \ldots s_n$

p

$|s_1|^2$ = total number of books to make

Next Mon @ 7am Hand in exam 4 (8 probs)
take home final (4 probs)

$$\begin{array}{r} (1,0,2,1)_3 \\ (1,1,0)_3 \\ \hline (1,2,0,1)_3 \end{array}$$