The in-class part of the Final Exam is scheduled as follows:
Thursday, May 7th at 10:15 a.m. in Walker 222.

The best way to study for the in class part of the final is to do the following

1. Study new material Section 8.1, 8.2, 8.3, 8.5, 8.7, 8.8, 8.10, 8.12, 8.13
   Note the final will have a heavier emphasis on the new material.
2. Study Test 1 and Test 2.
   In particular, know how to encrypt and decrypt messages using shift cipher, affine ciphers, the Vigenere cipher, and how to break a Vigenere cipher using signatures and scrawls.

Take Home Part: D2L RSA Discussion (Worth 10 points)
Due by 5:00 p.m., Thursday, May 7th

Good Questions to Study from Old Tests: Test 1: # 4, 5, 6
Test 2 # 1, 5, 6, 7, 8, 11.

Things you will given on Final
MOD 26 alphabet assignment
MOD 26 Inverse Table
Vigenere Cipher Square
Formulas for Index of Coin and keyword length
Give Ascii Code Table
Formulas for Fermat Factorization process: $y^2 = x^2 - m$
$p = x + y$, $q = x - y$

Note: Bring some type of computer MOD program

Ex: Find s and t where $sa + tb = \gcd(a,b)$

Never Solve For a Quotient!
Leave Quotients in Numerical Form

$a = 3001, \quad b = 541$

want $\gcd(a,b)$ and where $sa + tb = \gcd(a,b)$

Find s, t

$$\begin{array}{r} 5 \\ 541 \overline{)3001} \\ -2705 \\ \hline 296 \end{array}$$

quot, rem

Never Shift Quotients!

Run Euclid $a = 3001 > b = 541$

Solve for remainders

a = quot $\cdot$ b + rem

$3001 = \underline{5} \cdot 541 + \underline{296} \Rightarrow 296 = 3001 - 5 \cdot 541 = a - 5b$

$541 = \underline{1} \cdot 296 + \underline{245} \Rightarrow 245 = 541 - 1 \cdot 296 = b - 1\cdot(a - 5b) = b - a + 5b = -a + 6b$

$296 = \underline{1} \cdot 245 + \underline{51} \Rightarrow 51 = 296 - 1 \cdot 245 = (a - 5b) - 1\cdot(-a + 6b) = a - 5b + a - 6b = 2a - 11b$

$245 = \underline{4} \cdot 51 + \underline{41} \Rightarrow 41 = 245 - 4 \cdot 51 = (-a + 6b) - 4(2a - 11b) = -a + 6b - 8a + 44b$
$= -9a + 50b$

$51 = \underline{1} \cdot 41 + \underline{10} \Rightarrow 10 = 51 - 1 \cdot 41 = (2a - 11b) - 1\cdot(-9a + 50b) = 2a - 11b + 9a - 50b$
$= 11a - 61b$

$41 = \underline{4} \cdot 10 + \underline{1} \Rightarrow 1 = 41 - 4 \cdot 10 = (-9a + 50b) - 4(11a - 61b)$
$= -9a + 50b - 44a + 244b = -53a + 294b$

gcd

$10 = \underline{10} \cdot 1 + \underline{0}$

$\gcd(3001, 541) = 1$

Thus
$-53a + 294b = 1 = \gcd(a,b)$
$(-53)a + (294)b = 1 = \gcd(a,b)$

$\boxed{s = -53, \quad t = 294}$

check

$sa + tb = (-53)(3001) + (294)(541) = 1 = \gcd(a,b)$

Ex

Find $25^{-1} \pmod{89}$ $\qquad e^{-1} \pmod{f}$

$e = 25 \qquad f = 89$

want to solve

$sf + te = \gcd(e,f)$

Run Euclid Alg on $f = 89 > e = 25$

$$25 \overline{)89}^{\,3 \leftarrow q}, \quad -75, \quad 14 \leftarrow r$$

Euclid Alg

solve for remainders

$sf + te = \gcd(e,f)$

f quot e rem

$89 = 3 \cdot 25 + 14 \Rightarrow 14 = 89 - 3 \cdot 25 = f - 3e$

$25 = 1 \cdot 14 + 11 \Rightarrow 11 = 25 - 1 \cdot 14 = e - 1 \cdot (f - 3e) = e - f + 3e = -f + 4e$

$14 = 1 \cdot 11 + 3 \Rightarrow 3 = 14 - 1 \cdot 11 = (f - 3e) - 1 \cdot (-f + 4e) = f - 3e + f - 4e$

$= 2f - 7e$

$11 = 3 \cdot 3 + 2 \Rightarrow 2 = 11 - 3 \cdot 3 = (-f + 4e) - 3(2f - 7e) = -f + 4e - 6f + 21e$

$= -7f + 25e$

$3 = 1 \cdot 2 + 1 \Rightarrow 1 = 3 - 1 \cdot 2 = (2f - 7e) - 1(-7f + 25e)$

gcd

$= 2f - 7e + 7f - 25e = 9f - 32e$

$2 = 2 \cdot 1 + 0$

$\gcd(89, 25) = 1$
inverse exist

Thus

$9f - 32e = 1 = \gcd(e,f)$

$(9)f + (-32)e = 1 = \gcd(e,f)$

$s = 9 \qquad t = -32$

we are interested in $t = -32$

Note $t = -32 < 0$ convert to a positive representation

$t = -32 \bmod 89 = 57$ $\quad \left(\begin{array}{l}\text{Take} \\ -32 + 89 = 57\end{array}\right)$

can use MOD program

$$\boxed{\text{Hence } 25^{-1} \bmod 89 = 57}$$

e^{-1}

check $(e \cdot e^{-1}) \bmod f = 1$

$(25 \cdot 57) \bmod 89 = 1425 \bmod 89 = 1$ ✓

~~WRONG! $5^{60} \bmod 71 \approx 8.67 \times 10^{41} \bmod 71 = C$~~

RSA

Ex) Use method of successive squares to compute

$$5^{60} \bmod 71$$

1.) Take exponent 60 and write it as a sum of powers of 2, start with 2^0. Start by computing powers of 2 less than 60.

$2^0 = 1$ $2^3 = 8$ ✓ $2^6 = 64 > 60$ stop

$2^1 = 2$ $2^4 = 16$ ✓

$2^2 = 4$ ✓ $2^5 = 32$ ✓

write 60 as a sum of powers of 2 from largest to smallest

$$\begin{aligned} 60 &= 32 + 28 \\ &= 32 + 16 + 12 \\ &= 32 + 16 + 8 + 4 \end{aligned}$$

$$\begin{aligned} 5^{60} \bmod 71 &= 5^{32+16+8+4} \bmod 71 \\ &= (5^{32} \cdot 5^{16} \cdot 5^{8} \cdot 5^{4}) \bmod 71 \\ &= (\underbrace{25 \cdot 5}_{} \cdot \underbrace{54 \cdot 57}_{}) \bmod 71 \\ &= (\underset{\bmod 71}{125} \cdot \underset{\bmod 71}{3078}) \bmod 71 \\ &= (54 \cdot 25) \bmod 71 = 1350 \bmod 71 \boxed{= 1} \end{aligned}$$

Recall

$a^{k+l} = a^k \cdot a^l$

← Look Below

Note $3078 \bmod 71 = 25$

$125 \bmod 71 = 54$

Final answer

Double exponent each time

Final answer

6

$5^1 \bmod 71 = 5$

$5^2 \bmod 71 = 25 \bmod 71 = 25$

✓ $5^4 \bmod 71 = (5^2)^2 \bmod 71 = (25)^2 \bmod 71 = 57$

✓ $5^8 \bmod 71 = (5^4)^2 \bmod 71 = (57)^2 \bmod 71 = 54$

✓ $5^{16} \bmod 71 = (5^8)^2 \bmod 71 = (54)^2 \bmod 71 = 5$

✓ $5^{32} \bmod 71 = (5^{16})^2 \bmod 71 = (5)^2 \bmod 71 = 25$

Go back above and finish

Ex) Suppose we want create an RSA scheme for enciphering and deciphering messages. Suppose we choose the primes $p = 3$ and $q = 11$ and use an enciphering exponent of $e = 7$.

a.) Find m and f

$$m = p \cdot q = 3 \cdot 11 \boxed{= 33}$$

$$f = (p-1)(q-1) = (3-1)(11-1) = 2 \cdot 10 \boxed{= 20}$$

b.) Find the deciphering exponent d

$e = 7$ Recall $d = e^{-1} \bmod f = 7^{-1} \bmod 20$

we know $(e \cdot d) \bmod f = 1$

$$(7 \cdot d) \bmod 20 = 1$$

answer $d = 3$ since $(7 \cdot 3) \bmod 20 = 21 \bmod 20 = 1$

c.) Using a MOD 26 alphabet assignment, encipher the message PAUL in blocks of 1 letter each

Basic Computation is enciphering is $x^e \bmod m$, plaintext # is

MOD 26 alphabet assign

$P \Rightarrow 15 \Rightarrow 15^e \bmod m = 15^7 \bmod 33 = 170859375 \bmod 33 = 27$

$A \Rightarrow 0 \Rightarrow 0^e \bmod m = 0^7 \bmod 33 = 0$

$U \Rightarrow 20 \Rightarrow 20^e \bmod m = 20^7 \bmod 33 = 1280000000 \bmod 33 = 26$

$L \Rightarrow 11 \Rightarrow 11^e \bmod m = 11^7 \bmod 33 = 19487171 \bmod 33 = 11$

Ciphertext 27 0 26 11

d.) Decipher the message 15 20 28 7 $m=33$

Basic computation to decipher $y^d \bmod m$ $d=3$

ciphertext plaintext MOD 26 alphabet

$15 \Rightarrow 15^d \bmod m = 15^3 \bmod 33 = 3375 \bmod 33 = 9 \Rightarrow J$

$20 \Rightarrow 20^d \bmod m = 20^3 \bmod 33 = 14 \Rightarrow O$

$28 \Rightarrow 28^d \bmod m = 28^3 \bmod 33 = 7 \Rightarrow H$

$7 \Rightarrow 7^d \bmod m = 7^3 \bmod 33 = 13 \Rightarrow N$

plaintext is "JOHN"

Ex] Given the affine cipher

$$y = 11x + 17 \bmod 26$$

ciphertext # (at y) plaintext # (at x)

a.) Encipher the message R U

plaintext mod 26 alph

$R \Rightarrow x = 17 \Rightarrow y = (11(17) + 17) \bmod 26 = 204 \bmod 26$
$= 22 \Rightarrow W$

$U \Rightarrow x = 20 \Rightarrow y = (11(20) + 17) \bmod 26 = 237 \bmod 26$
$= 3 \Rightarrow D$

$\boxed{\text{ciphertext is "W D"}}$

b.) Find the decipherment formula

encipherment formula: $y = (11x + 17) \bmod 26$

Solve for x

$$11x + 17 = y \bmod 26$$

$$11x = (y - 17) \bmod 26$$

Note
$-17 \bmod 26 = 9$

$$11x = (y + 9) \bmod 26$$

$$\cancel{11^{-1} 11}\, x = 11^{-1}(y + 9) \bmod 26$$

$$\boxed{x = 19(y+9) \bmod 26}$$

From Inverse Table

$11^{-1} \bmod 26 = 19$

c.) Use the decipherment formula to decipher "ZJ"

ciphertext $x = 19(y+9) \bmod 26$

mod 26 alphabet

$Z \Rightarrow y = 25 \Rightarrow x = 19(25+9) \bmod 26 = 19(34) \bmod 26$

$= 646 \bmod 26$

$= 22 \xrightarrow{} W$

mod 26

$J \Rightarrow y = 9 \Rightarrow x = 19(9+9) \bmod 26 = 19(18) \bmod 26$

$= 342 \bmod 26$

$= 4 \Rightarrow E$

$\boxed{\text{plaintext is "WE"}}$

$y = (ax+b) \bmod 26$

$\underline{\gcd(a, 26) = 1}$

d.) What's wrong with the affine cipher

$y = (4x+3) \bmod 26$

$a = 4 \qquad \gcd(4, 26) = 2 \neq 1$

$4^{-1} \bmod 26$ Does not exist!

Ex) Suppose that for an affine cipher it is known that the plaintext letter E enciphers as the ciphertext letter P and the plaintext letter T enciphers as X. Find the affine cipher formula that was used?

want to find a and b

$$y = (ax + b) \bmod 26$$

ciphertext #   plaintext #

ciphertext P $\Longleftrightarrow$ plaintext E

$y = 15$ $x = 4$

gives

$$15 = (a(4) + b) \bmod 26$$

$$4a + b = 15 \bmod 26 \quad *$$

$$y = (ax + b) \bmod 26$$

ciphertext X $\Longleftrightarrow$ plaintext T

$y = 23$ $x = 19$

$$23 = (a(19) + b) \bmod 26$$

$$19a + b = 23 \bmod 26 \quad **$$

put * and ** together Find a and b

$$\begin{aligned} &4a + \cancel{b} = 15 \bmod 26 \quad (1) \\ -\ &19a + \cancel{b} = 23 \bmod 26 \quad (2) \end{aligned}$$

subtract eqn 1 & 2

$$-15a = -8 \quad 26$$

Note

$-15 \bmod 26 = 11$

$-8 \bmod 26 = 18$

$$11a = 18 \bmod 26$$

$$\cancel{11^{-1} \cdot 11}\, a = (11^{-1} \cdot 18) \bmod 26$$

Note

$11^{-1} \bmod 26 = 19$

inverse table

$$a = (19 \cdot 18) \bmod 26$$

$$a = 342 \bmod 26$$

$$\underline{\underline{a = 4}}$$

Find b: Sub $a = 4$ back into eqn 1

$$4a + b = 15 \bmod 26$$

$$4(4) + b = 15 \bmod 26$$

$$16 + b = 15 \bmod 26$$

$$b = (15 - 16) \bmod 26$$

$$b = -1 \bmod 26$$
$$b = 25$$

answer: $a = 4$, $b = 25$

formula: $y = (4x + 25) \bmod 26$

Ex] $3^{57} \bmod 73$ — use successive squares to compute

Exponent: 57 write as a sum of powers of 2

$2^0 = 1$ $2^2 = 4$ ✓ $2^4 = 16$ $2^6 = 64 \not> 57$

$2^1 = 2$ ✓ $2^3 = 8$ ✓ $2^5 = 32$

$$57 = 32 + 25$$
$$= 32 + 16 + 9$$
$$= 32 + 16 + 8 + 1$$

$$3^{57} \bmod 73 = 3^{32+16+8+1} \bmod 73$$
$$= (3^{32} \cdot 3^{16} \cdot 3^{8} \cdot 3^{1}) \bmod 73$$
$$= (\underbrace{64 \cdot 8}_{} \cdot \underbrace{64 \cdot 3}_{}) \bmod 73 \quad \text{(See below!)}$$
$$(512 \bmod 73 \cdot 192 \bmod 73) \bmod 73$$

Answer!

$= (1 \cdot 46) \bmod 73 = 46 \bmod 73 \boxed{= 46}$

Double exponent to square previous result

✓ $3^1 \bmod 73 = 3$

$3^2 \bmod 73 = 9$

$3^4 \bmod 73 = (3^2)^2 \bmod 73 = (9)^2 \bmod 73 = 8$

✓ $3^8 \bmod 73 = (3^4)^2 \bmod 73 = (8)^2 \bmod 73 = 64$

✓ $3^{16} \bmod 73 = (3^8)^2 \bmod 73 = (64)^2 \bmod 73 = 8$

✓ $3^{32} \bmod 73 = (3^{16})^2 \bmod 73 = (8)^2 \bmod 73 = 64$

Ex] Find $29^{-1} \bmod 83 = e^{-1} \bmod f$

$e = 29 \quad f = 83$

$$\begin{array}{r} 2.86 \\ 29\overline{)83} \\ \underline{58} \\ 25 \leftarrow r \end{array}$$

Find $\gcd(e,f) = \gcd(29,83)$ STOP at gcd

by Euclid Alg $a > b$

Solve for remainders to find s, t where $sf + te = \gcd(e,f) = 1$

Never sub for quotients!

$$\overset{f}{83} = \overset{q}{\underline{2}} \cdot \overset{e}{29} + \overset{r}{\underline{25}} \Rightarrow 25 = \overset{f}{83} - 2 \cdot \overset{e}{29} = f - 2e$$

$$29 = \underline{1} \cdot 25 + \underline{4} \Rightarrow 4 = 29 - 1 \cdot 25 = e - 1 \cdot (f - 2e) = e - f + 2e = -f + 3e$$

$$25 = \underline{6} \cdot 4 + \underset{\gcd}{\underline{1}} \Rightarrow 1 = 25 - 6 \cdot 4 = (f - 2e) - 6(-f + 3e) = f - 2e + 6f - 18e = 7f - 20e$$

$$4 = \underline{4} \cdot 1 + \underline{0}$$

STOP at gcd!

$\gcd(83, 29) = 1$ Thus $7f - 20e = 1 = \gcd(e,f)$

$$(7)f + (-20)e = \gcd(e,f)$$

$s = 7 \qquad \underline{\underline{t = -20}}$

To get inverse of $e = 29 \bmod f = 83$, need t

However, $t = -20 < 0$. Convert t to positive form

$$t = t \bmod f = -20 \bmod 83 = \underline{\underline{63}}$$

$$\boxed{\text{Hence } e^{-1} \bmod f = 29^{-1} \bmod 83 = 63}$$

Check:

$$(e \cdot e^{-1}) \bmod f = 1$$

$$(29 \cdot 63) \bmod 83 \stackrel{?}{=} 1$$

$$1827 \bmod 83 = 1$$

$$1 = 1 \checkmark$$

4 Written HW

13 9 8 16

RSA Scheme: $p = 5,\ q = 7$

Hence: $m = p \cdot q = 5 \cdot 7 = 35$

$f = (p-1)(q-1) = (5-1)(7-1) = 4 \cdot 6 = \underline{\underline{24}}$

encryption exponent: $e = 5$

$d = e^{-1} \bmod f = 5^{-1} \bmod 24$

$(e \cdot d) \bmod f = 1$

$(5 \cdot d) \bmod 24 = 1$

$d = 5 \Rightarrow$ since $(5 \cdot d) \bmod f = (5 \cdot 5) \bmod 24 = 25 \bmod 24 = 1$

cipher text: 13 9 8 16

plaintext + map 26 alphabet

$13 \Rightarrow 13^d \bmod m = 13^5 \bmod 35 = 371293 \bmod 35 = 13 \Rightarrow N$

$9 \Rightarrow 9^d \bmod m = 9^5 \bmod 35 = 59049 \bmod 35 = 4 \Rightarrow E$

$8 \Rightarrow 8^d \bmod m = 8^5 \bmod 35 = 32768 \bmod 35 = 8 \Rightarrow I$

$16 \Rightarrow 16^d \bmod m = 16^5 \bmod 35 = 1048576 \bmod 35 = 11 \Rightarrow L$

plaintext is : NEIL

1f) Is 1559 prime

$\sqrt{1559} \approx 39.4$ (Test prime divisors less than 39.4, last to test is 37)

Test

$\frac{1559}{2}$ NO

$\frac{1559}{3}$ NO

$\frac{1559}{5}$ NO

$\frac{1559}{7} \approx 222.7$ NO

$\frac{1559}{11}$ NO

$\frac{1559}{13}$ NO

$\frac{1559}{17}$ NO

$\frac{1559}{19}$ NO

$\frac{1559}{23}$ NO

$\frac{1559}{29}$ NO

$\frac{1559}{31}$ NO

$\frac{1559}{37}$ NO

STOP!

$\boxed{\text{1559 is prime}}$

Ex] Use the Fermat factorization method to factor $m = 4412609$

Take $\sqrt{m} = \sqrt{4412609} \approx 2100.62$

nearest integer greater is 2101

Let $x = 2101$

$y^2 = x^2 - m$

$y^2 = (2101)^2 - 4412609$

$y^2 = 1592$

$y = \sqrt{1592} \approx 39.9$ (not an integer)

Increase x by ~~up~~ by 1: $x = 2102$

$y^2 = x^2 - m$

$y^2 = (2102)^2 - 4412609$

$y^2 = 5795$

$y = \sqrt{5795} \approx 76.1$ (not an integer)

Increase x by 1: $x = 2103$

$y^2 = x^2 - m$

$y^2 = (2103)^2 - 4412609$

$$y^2 = 10000$$

$$y^2 = \sqrt{10000} = 100$$ is a perfect square!

$$x = 2103, \quad y = 100$$

primes: $$p = x + y = 2103 + 100 = 2203$$

$$q = x - y = 2103 - 100 = 2003$$

Answer: $p = 2203, \quad q = 2003$

Check: $4412609 = m = p \cdot q = 2203 \cdot 2003 = 4412609$

Fermat's Little Thm says If p is prime, $a^{p-1} \equiv 1 \mod p$, $p \nmid a$

2b.) $\underset{p-1}{3^{22606}} \equiv 3955 \mod 22607$

$\not\equiv 1 \mod \underset{p}{22607} \Rightarrow$ $\boxed{\text{modulus } 22607 \text{ is not prime!}}$

2a $2^{6600} \equiv 1 \bmod 6601$

~~says nothing~~
test is inconclusive for showing whether 6601 is prime or not!

---

p. 325 1a 1573

Test primes $\sqrt{1573} \approx 39.66$ (Test all primes less than 39.66)

$\frac{1573}{2}$ NO $\sqrt{143} \approx 11.95$ (Test primes less than this)

$\frac{1573}{3}$ NO $\frac{1573}{7}$ NO $\frac{143}{11} = 13$

$\frac{1573}{5}$ NO $\frac{1573}{11} = 143$

Factor tree

1573

$11 \cdot 143$

$11 \cdot 13$

$$\boxed{1573 = 11 \cdot 11 \cdot 13 = 11^2 \cdot 13}$$