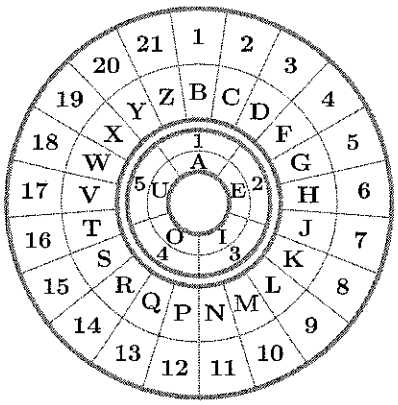
Practice Exam 2

Name: Key



1. (a) Convert "**practice exam**" into numbers.

p r a c t i c e

12, 14, 1, 2, 16, 3, 2, 2

e x a m

2, 19, 1, 10

(b) What vowel goes with the number 3?

I

(c) What consonant goes with the number 3?

D

(d) What vowel goes with the number 48?

48 - 45 = 3

I

$48 \equiv 48-21 = 27 \equiv 27-21 = 6$

(e) What consonant goes with the number 48?

H

(f) What vowel goes with the number -3? $-3 \equiv -3+5 = 2$, E

(g) What ~~vowel~~ consonant goes with the number -3? $-3 \equiv -3+21 = 18$, W

2. Give the **standard represenative** of each number.

$2+3 \pmod{21}$

5

$2 \times 3 \pmod{21}$

6

$20+30 \pmod{21}$

$-1+9 = 8$

$20 \times 30 \pmod{21}$

$-1 \times 9 = -9 \equiv -9+21 = 12$

$6 \times 3 \pmod{5}$

$1 \times 3 = 3$

$18 \equiv 18-5-5-5 = 3$

$22 \times 17 \pmod{21}$

$1 \times 17 = 17$

$181+212 \pmod{10}$

$1+2 = 3$

$181+212 \pmod{100}$

$81+12 = 93$

$181 \times 212 \pmod{10}$

$1 \times 2 = 2$

$181 \times 212 \pmod{20}$

$180 \quad 200$

$1 \times 12 = 12$

$10^2 \pmod{31}$

$100-31-31-31 = 7$

$10^4 = (10^2) \times (10^2) \pmod{31}$

$7 \times 7 = 49 \equiv 49-31 = 18$

$2^5 \pmod{31}$

$32 \bmod 31 = 1$

$10^6 = (10^4) \times (10^2) \pmod{31}$

$18 \times 7 = 126 - 4(31) = 2$

Bonus: $2^{53} = 2^5 \times \cdots \times 2^5 \times 2^3 \pmod{31}$

$1 \times \cdots \times 1 \times 8 = 8$

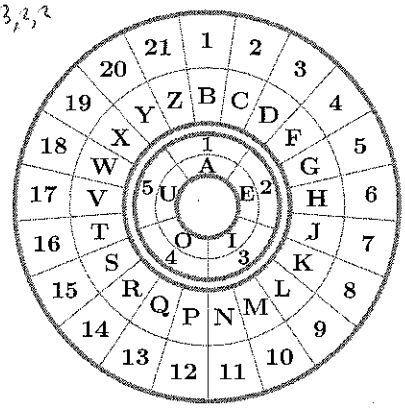
3. (a) Encrypt: Where does the shift by 5 cipher take **practice exam**?

p r a c t i c e e x a m

+5: 17,19,6,7,21,8,7,7 7,24,6,15

= 1 3 2 2 3 1

VX AJZIJE EDAS



(b) Decrypt: What was shifted by 5 to get **VXAJZIJE EDAS**?

(Just subtract 5 instead)

A = 1, -5: -4 = 1 A

D = 3, -5: -2 = 19, X

(c) Find the key: What shift turns **practice exam** into **XZILCULO OGIV**?

P 12 19 X — looks like +7, check vowels

a 1 3 I

1+7=8=3 mod 5 so it does work

(d) Find the key: What shift turns **practice exam** into **WYIKBUKO OFIT**?

P 12 18 W — looks like +6,

a 1 3 I — not 6! need +2 (mod 5)

Consonants also work with +6, +27, +48,

+27 = 2 (mod 5)

(e) Somebody claims a shift cipher turned **practice exam** into **VA DIG TIV**. What shift was used or why is "somebody" wrong?

They are wrong. Practice exam is two words but VA DIG TIV is 3. Also the number of letters doesn't match.

(f) Codebreak: What does this say? (It is an English sentence encrypted with a shift cipher.)

DRU TUJ DE DRU UHOW AC DE CDINJ

If you get stuck: how many words are there? which consonant is most common in the ciphertext versus English? which vowel?

8 words

D vs T

U vs E

same word

D 3 16 T — +13

U 5 2 E — +2

DRU TUJ DE DRU UHOW AC

3 14 5 16 5 7 3 2 5 6 4 18 1 2

16 27 2 29 2 20 4 64 2 19 6 3 1 3 15

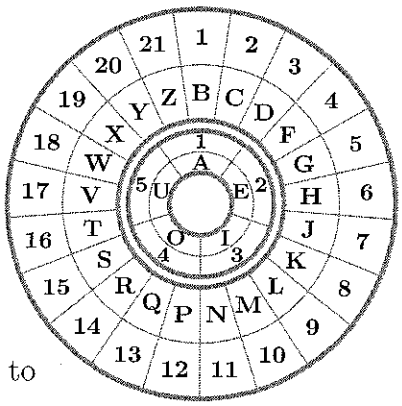
THE KEY TO THE EXAM IS

(Homework)

4. (a) Encrypt: Where does the multiplication by 4 cipher take the word **boy**?

b o y
1 4 20
4 16 80 − 21 = 59, −21 = 38, −21 = 17
4 1 17
F A V

FAV



(b) ~~Decrypt:~~ What does the multiplication by 4 cipher take to **HROKBEKI IQOX**?

H R O K B E K I I Q O X
6 14 4 8 1 2 8 3 13 4 19
+21,5? 48 56 4 8 64 12 8 8 76 4 40
÷4 12 14 1 2 16 3 2 2 19 1 10
P R A C T I C E E X A M

(c) Bad key: Why is multiplication by 3 a bad cipher? What goes wrong? Hint: Give three different English word decryptions of **PAHH**.

P A H H
12 1 6 6
+5
÷3 2
F C C
N L L
W P P

FELL, WELL (oops that's all)

12 ≡ 33 ≡ 54 ≡ 75
÷3 ↓ ↓ ↓ ↓
4, 11, 18, 25≡4, 11, 18, ...
F, N, W

6 ≡ 27 ≡ 48
↓ ↓ ↓
2 9 12
C L P

(d) Key Exchange: You do Diffie-Hellman key exchange with $(b = 3, N = 31)$. You choose $A = 9$ and compute $3^A \pmod{31}$ in order to tell your partner. Your partner tells you their answer was 10. What is the secret number the two of you would say together in the last step?

$10^A = 10^9 = 10^8 \times 10^1 = 16$

$10^4 \times 10^4 \times 10^1$

$18 \times 18 \times 10 \pmod{31}$

$14 \times 10 = 140 - 31 - 31 - 31 - 31$

$= 16$ ←

18 × 18 = 144, 18 = 324, −310 = 14 mod 31