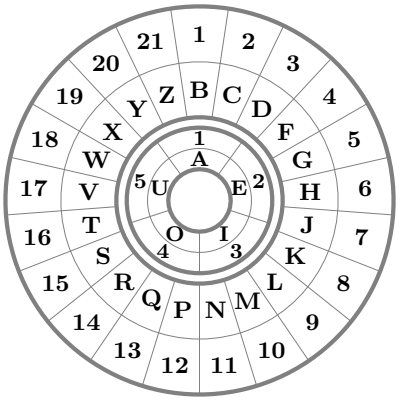
Practice Exam 2 Name: _____

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



(b) What vowel goes with the number 3?

(c) What consonant goes with the number 3?

(d) What vowel goes with the number 48?

(e) What consonant goes with the number 48?

(f) What vowel goes with the number -3?

(g) What consonant goes with the number -3?

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

$2 + 3 \pmod{21}$ $2 \times 3 \pmod{21}$

$20 + 30 \pmod{21}$ $20 \times 30 \pmod{21}$

$6 \times 3 \pmod{5}$ $22 \times 17 \pmod{21}$

$181 + 212 \pmod{10}$ $181 + 212 \pmod{100}$

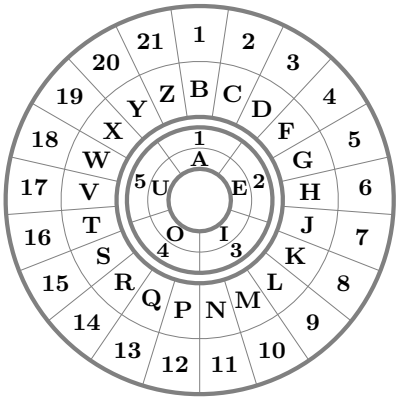
$181 \times 212 \pmod{10}$ $181 \times 212 \pmod{20}$

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

$2^5 \pmod{31}$ $10^6 = (10^4) \times (10^2) \pmod{31}$

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

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



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

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

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

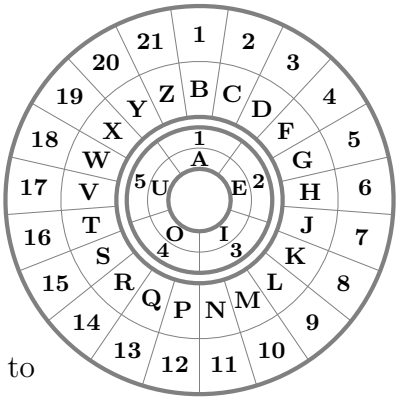
(e) Somebody claims a shift cipher turned **practice exam** into **VA DIG TIV**. What shift was used or why is "somebody" wrong?

(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?

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



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

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

(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?