Solutions

4 I LOVE MATH = L ORYH PDWK. Just move three letters toward the end of the alphabet to encode, wrapping to the beginning of the alphabet as needed.

5 Here are the solutions using keys of 3, 6, and 9 to encode:

- HELLO: KHOOR, NKRRU, QNUUX
- GO KNIGHTS: JR NQLJKWV, MU QTOMNZY, PX TWRPQCB
- TO INFINITY AND BEYOND: WR LQILQLWB DQG EHBRRQG, CX RWORWRCH JWM KN-HXWM, ZU OTLOTOZE GTJ HKEUTJ,

6 CORRECT, YOU GOT IT, ITISGOOD, HARDER WITHOUT KEY (e = 9)

7 subtract 3, 7, or 9. That is, move in the reverse direction through the alphabet by the amount specified by the key.

8 For a key of e we can decode by adding 26 − e since this is the same thing (mod 26) as subtracting e.

9 A and N are both coded as A (0), B and O are both coded as C (2). This means that when we see, for example, the letter C in the encoded message, we can’t tell if the original message had a B or an O.

10 Multiplying each number from 0–25 by 3 we get a different number each time. This means it is at theoretically possible to recover the original message without any guesswork.

11 e = 4 has the same problems that e = 2 had.

12 The encoding key cannot share any divisors (factors) with 26 = 2 × 13. So the encoding key may not be even, or 13. Other encoding keys will work.

13 Q DANANA, FVYC OQZEC SZMAF, MF FI DZIFM, KIHFYHYGAFYQN ZQGEC

14 DECODE WITH NINE (use d = 9)

15 5 · 21 = 105 ≡ 1 (mod 26), so 21 is the decoding key.

16 2^5 = 32 ≡ 32 (mod 65), 3^5 = 243 ≡ 48 (mod 65), 4^5 = 1024 ≡ 49 (mod 65), 10^5 = 100000 ≡ 30 (mod 65),

17 30^{25} means multiply 30 × 30 × 30 · · · × 30. (That’s twenty-five 30’s multiplied together.) We can do this in five groups of 5 30’s:

\[
30^{25} = (30 \times 30 \times 30 \times 30 \times 30) \times (30 \times 30 \times 30 \times 30 \times 30) \times (30 \times 30 \times 30 \times 30 \times 30) \\
\times (30 \times 30 \times 30 \times 30 \times 30) \times (30 \times 30 \times 30 \times 30 \times 30) \\
= 30^5 \times 30^5 \times 30^5 \times 30^5 \\
= (30^5)^5
\]

18 71

19 17