Teacher Solution Key — Number Theory & Cryptography Kickoff Worksheet

Use these worked solutions and talking points to connect each warm■up to the cryptography concepts we'll study.

1. Quick Brain Teasers — Solutions & Why They Matter

1) Clock Math: If it's 9 o'clock now, what time will it be in 100 hours?

Solution:

A 12■hour clock is arithmetic modulo 12. Compute 100 mod 12.

$12 \times 8 = 96$, so $100 \equiv 4 \pmod{12}$. Starting at 9 o'clock and moving 4 hours lands on 1 o'clock. Answer: 1 o'clock.

Why this matters:

Modular arithmetic is the backbone of modern public■key cryptography. RSA, Diffie–Hellman, and Elliptic■Curve methods all work with numbers "wrapped around" a modulus, just like hours on a clock.

2) Divisibility Check: Is 123456 divisible by 3? By 9?

Solution:

Sum of digits = 1+2+3+4+5+6 = 21.

• Divisible by 3? Yes, because 21 is divisible by 3.

• Divisible by 9? No, because 21 is not a multiple of 9.

Why this matters:

Digit■sum rules come from $10 \equiv 1 \pmod{9}$ and $10 \equiv 1 \pmod{3}$. These congruences explain check■digit systems (credit cards, barcodes, ISBNs) that detect common errors like a mistyped digit.

3) Remainder Riddle: When 23 is divided by 5, what are the quotient and remainder?

Solution:

$23 = 5 \times 4 + 3$, with $0 \le 3 < 5$. Quotient = 4, remainder = 3.

Why this matters:

This is the Division Algorithm (a.k.a. Euclidean division). It's the entry point to the Euclidean Algorithm for gcds, which powers modular inverses and RSA key operations.

4) Why is 2 a "special" prime?

Solution:

It's the only even prime. Every other even number has 2 as a factor, so it's composite.

Why this matters:

Parity (even/odd) is arithmetic modulo 2 — the mathematics of bits. Many crypto primitives manipulate bits (or numbers mod 2^k), and some theorems apply only to odd primes, so $p = 2$ must be handled separately.

2. Connecting to Cryptography — Solutions & Why They Matter

5) Secret Sharing: You and a friend each pick a prime and multiply them. Why is it hard to recover the primes from the product?

Solution:

For suitably large primes (hundreds or thousands of bits), no efficient algorithm is known that factors their product quickly on classical computers.

Why this matters:

This is the hardness assumption behind RSA. Multiplying is easy; factoring is believed to be hard — a “one■way” function. Keys must be large enough to resist current factoring methods.

6) Check Digits: Append a digit d to 12345 so the result is divisible by 9. What is d?

Solution:

Digit sum of 12345 is 15. We want $15 + d \equiv 0 \pmod 9$. Smallest single digit with this property is $d = 3$ (since $18 \equiv 0 \bmod 9$). New number 123453 is divisible by 9.

Why this matters:

Check■digit schemes use modular arithmetic to catch common entry errors. Real systems use variants like mod■10 (Luhn for cards) or mod■11 (ISBN■10).

7) Randomness Matters: Make a ‘random■looking’ number from a birthday. What’s the catch?

Solution (example to discuss):

Let x = MMDDYYYY. Define $r = (a \cdot x + c) \bmod m$ with public constants (e.g., a=1103515245, c=12345, m=2^31). This quickly makes numbers that look random.

But if an attacker guesses x (the birthday) or sees enough outputs, they can predict future values. That makes it unsuitable for keys or nonces.

Why this matters:

*Cryptography needs *unpredictable* (entropy■rich) randomness from secure generators. Weak or guessable seeds break encryption (e.g., predictable keys, repeated nonces). Use CSPRNGs seeded from high■entropy sources.*

3. Reflection — Sample Talking Points

- Notice how everyday arithmetic becomes powerful when done modulo n (clocks, digit sums).
- Division with remainder leads to gcds → modular inverses → solving congruences.
- Primes are the atoms of integers; picking large ones securely is central to key generation.
- Randomness quality is security■critical; predictable ‘random’ breaks systems.

Use these connections to motivate why we care about proofs, algorithms (like Euclid’s), and careful attention to assumptions (prime sizes, entropy sources).