Interactive quiz for Day 1

Quick-fire true or false around the class.

1. Compute $53 \times 120 \bmod 256$.

2. Compute $(x^2 + 3x + 1)(x^3 - 1)$

3. Ox3F $\oplus$ 0xFF.

4. I toss a fair coin three times. What is the probability that I get *at least one head*?

5. I toss a fair coin n times. What is the probability that I get *exactly one head*?

6. Compute gcd(21,35).

7. Simplify $x^{-k} \cdot (xy)^k \cdot y$.

8. How may years is 2^{64} seconds?

9. You want to store some secret documents **on your computer**, so that even if your computer gets stolen, no-one could read them. What are good tools for this purpose? (Hint: what format are the documents in? what is the adversary's budget?)

10. You want to store some secret documents **in the cloud**, so that even if your password is compromised, no-one could read them. What are good tools for this purpose? (Hint: is encryption necessary? Who is the adversary? Does MFA help?)

11. You want to send secret messages to your friend, so that no-one except your friend could read them. What are good tools for this purpose? (Hint: What are the *attacker capabilities*? Access to your phone? Access to messaging service? Software authorship (e.g., OS or another app)? Hardware manufacturer?)