Interactive quiz for Week 1

Quick-fire true or false around the class.

1. ✓ In symmetric-key crypto, the decryption key is the same as the encryption key.
2. ✗ In public-key crypto, the decryption key and the encryption key are completely different and independent of each other.
3. ✗ In a one-time pad, the length of the key must be at least half the length of the message.
4. ✗ The one-time pad is vulnerable to frequency analysis (e.g., exploiting the fact that E is the most common letter in English).
5. ✓ DES has 16 rounds.
6. ✓ If you made a version of DES with only 10 rounds, it would be faster.
7. ✓ But it would be less secure.
8. ✓ If you made a version of DES with 20 rounds, it would be slower.
9. ✓ But it would be more secure.
10. ✓ Encryption with DES involves computing the DES Feistel function in each round.
11. ✗ Decryption with DES involves computing the inverse of the DES Feistel function in each round.
12. ✓ The 16 subkeys K_1 to K_{16} of DES are each of length 48.

✗ 13. The 16 subkeys K_1 to K_{16} of DES are mathematically independent of each other.

✓ 14. You could decrypt a DES ciphertext by trying each of the $2^{56} \approx 10^{17}$ keys in turn.

✓ 15. But this would take longer than the lifetime of the universe on any computer known to humankind.

✗ 16. The S-boxes in DES are not needed. You could create a version of DES without the S-boxes and it would be just as secure.

✗ 17. If the key is 000...0 (i.e., all zeros) then DES encryption does nothing. In other words, $\mathrm{Enc}_{000\ldots0}(m) = m$ for all messages m.

✓ 18. $\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$ for all keys k and messages m.

✓ 19. $\mathrm{Enc}_k(\mathrm{Dec}_k(m)) = m$ for all keys k and messages m.

✗ 20. $\mathrm{Enc3DES}_{k_1,k_2,k_3}(m) = \mathrm{Enc}_{k_1}(\mathrm{Enc}_{k_2}(\mathrm{Enc}_{k_3}(m)))$.

✓ 21. $\mathrm{Enc3DES}_{k_1,k_2,k_3}(m) = \mathrm{Enc}_{k_1}(\mathrm{Dec}_{k_2}(\mathrm{Enc}_{k_3}(m)))$.

✗ 22. DES is more secure than 3DES.

✓ 23. AES is more secure than DES.

✓ 24. AES is more secure than 3DES.

✓ 25. AES is faster than 3DES.

✓ 26. No-one uses DES anymore.

✗ 27. No-one uses AES anymore.