Interactive quiz for Week 2

Quick-fire true or false around the class.

1. You should always use a block mode for symmetric key encryption, even if your plaintext fits into a single block.
2. You can use any block mode (e.g., ECB, CBC, CTR) with any symmetric cipher (e.g., DES, 3DES, AES).
3. ECB is a bad choice of block mode for symmetric key encryption.
4. If you encrypt a JPG file (for example, a picture of a penguin) with ECB block mode, someone who views the encrypted file with a JPG browser will be able to see the outline of the original image.
5. In CBC block mode, the IV should be kept secret.
6. In CTR block mode, you use a different nonce for each block.
7. CBC and CTR are compatible with each other: if you encrypt using CBC, you can decrypt using CTR.
8. Because the plaintext never passes through the encryption function in CTR (rather, the nonce and counter pass through the encryption function), it would be OK if an adversary captured the input-output of the encryption function.
9. ECB, CBC and CTR are all parallisable.
10. If you change one bit in an AES-ECB ciphertext and then decrypt it, there will be one bit wrong in the plaintext.
11. If you change one bit in an AES-CTR ciphertext and decrypt it, there will be one bit wrong in the plaintext.

12. If you change too many bits of an AES-CBC ciphertext, it will be corrupted and it won't decrypt to anything.

13. Suppose an attacker knows what encryption system is being used, and has a ciphertext, but doesn't have the key. If the encryption system is good, there is no way that the attacker can get the plaintext.

14. In IND-CPA, the attacker chooses the plaintexts that get encrypted.

15. In IND-CPA, the attacker is trying to get the challenger to perform a decryption.

16. In IND-CPA, the attacker chooses a bit b at random, and then later guesses whether another bit b' is equal to b.

17. In IND-CPA, the attacker is limited to performing *polynomially-many* operations.

18. DES in CTR mode satisfies IND-CPA.

19. AES in CBC mode satisfies IND-CPA.

20. In a realistic attack scenario, an attacker is always presented with a ciphertext and two plaintexts, and has to guess which of the plaintexts is in the ciphertext.

21. In a good cipher, there are polynomially-many different keys.

22. In IND-CPA, the challenger can perform *exponentially-many* operations.

23. In AES-128, we perform 10 rounds, each round consisting of *substitution*, *byte permutation*, column manipulation, and *XOR with a round key*.

24. If you are using AES, you don't have to use a block mode.

25. There are known attacks against AES and it shouldn't be used.

26. In AES, the operation $\oplus$ is defined using polynomials.

27. The definition of AES makes special use of the polynomial $x^8+x^4+x^3+1$, which lives in a space of polynomials whose coefficients are either 0 or 1.

28. The coefficient of x^6 in that polynomial is 0.

29. You need to understand polynomials if you want to use an AES library in your program.

30. You should always program your own version of AES, rather than use libraries.