Interactive quiz for Week 3

Quick-fire true or false around the class.

1. The hash function SHA-256 takes an input of any size, and produces an output of size 256 bits.

2. There are no collisions for SHA-256 (that is, there are no bitstrings x and y with $x \neq y$ and SHA-256(x) = SHA-256(y)).

3. There exists a bitstring z of size 256 bits such that, for all bitstrings x, we have SHA-256(x) $\neq z$.

4. A cryptographic hash function is hard to invert, and collision resistant.

5. Suppose x and y of length 256 bits differ by one bit. Then SHA-256(x) and SHA-256(y) probably differ by about 128 bits.

6. Suppose x and y of length 256 bits differ by 128 bits. Then SHA-256(x) and SHA-256(y) probably differ by about 128 bits.

7. If x and y of length 256 bits differ by 256 bits, then x XOR $y = 111\ldots1$ (which may be written as 1^{256}).

8. If x and y of length 256 bits differ by 256 bits, then x XOR $1^{256} = y$.

9. Suppose x and y of length 256 bits differ by 256 bits. Then SHA-256(x) and SHA-256(y) probably differ by about 128 bits.

10. Suppose SHA-256(x) and SHA-256(y) differ by only 5 bits. Then x and y also differ by only about 5 bits.

11. To play paper-scisors-stone by WhatsApp, Alice and Bob can proceed as follows:

(a) Alice chooses $x \in \{$“paper”, “scissors”, “stone”$\}$, and sends $\mathrm{H}(x)$ to Bob.

(b) Bob chooses $y \in \{$“paper”, “scissors”, “stone”$\}$, and sends y to Alice.

(c) Then Alice sends x to Bob. Bob verifies that her x matches the hash that she previously sent.

(d) Since they have exchanged their choices x and y, they can see who won.

12. SHA-1 is secure.

13. SHA-2 is secure.

14. SHA-3 is secure.

15. SHA-256 provides about 128 bits of security.

16. Suppose Alice and Bob share a key k, and Alice wants to send a message m to Bob. She encrypts the message using AES in CTR mode, with the key k, and sends it on an untrusted network. If an adversary interferes with the message during transmission, Bob will be able to detect that, and reject the message.

17. Suppose Alice and Bob share a key k, and Alice wants to send a message m to Bob. She computes a HMAC of the message with the key k, and sends the message and the HMAC on an untrusted network. If an adversary interferes with the message and/or HMAC during transmission, Bob will be able to detect that, and reject the message.

18. A MAC is secure if there’s no way for an attacker (who doesn’t have the MAC key) to compute the MAC of any message.

19. In the MAC game, the adversary tries to make a MAC on a message of the challenger’s choice.

20. In the MAC game, the adversary has the MAC key.

21. In the MAC game, the adversary (who does not have the key) tries to make a MAC on a message of their own choice.

22. A MAC is secure if no attacker can win the MAC game with non-negligible probability.

23. HMAC is secure.

24. AES in CTR mode provides protection of confidentiality and integrity.

25. Let $\mathrm{Dec}_k(x)$ mean the decryption of x with k using AES-128 as a single block (this means that x is exactly one AES block, i.e., 128 bits). There exists a key k of length 128 bits and a bitstring x of length 128 bits such that attempting $\mathrm{Dec}_k(x)$ will fail (the decryption cannot be done).

26. Let $\mathrm{Dec}_k(x)$ mean the decryption of x with k using AES-128 in CTR mode. There exists a key k of length 128 bits and a bitstring x of length 256 bits such that attempting $\mathrm{Dec}_k(x)$ will fail (the decryption cannot be done).

27. In authenticated encryption, a decryption attempt will fail if the ciphertext is corrupted.

28. Authenticated encryption means that any attempt by an adversary to modify a ciphertext will cause the decryption to fail.

29. In the authenticated encryption game, the adversary tries to produce a ciphertext such that the decryption will not fail. In this game, the adversary is allowed to use valid ciphertexts, and tries to come up with a new ciphertext that will successfully decrypt.

30. CTR mode and CBC mode provide authenticated encryption.

31. GCM mode provides authenticated encryption.

32. Encrypt-then-MAC provides authenticated encryption.

33. Authenticated encryption is always better than regular encryption. There are no use cases where it is better to use CTR mode than GCM mode.

34. Encrypt-then-MAC means we encrypt the plaintext and take a MAC of the ciphertext. The result of the operation is the encryption and the MAC, taken together.

35. Encrypt-and-MAC means we encrypt the plaintext and take a MAC of the plaintext. The result of the operation is the encryption and the MAC, taken together.

36. Encrypt-and-MAC is secure.

37. If you are writing a program and you find you need encryption, you should use AES.

38. If you are writing a program and you decide you need AES, you should write your own implementation rather than use a library.