Quiz Submissions - Module 5 self-test

Thomas Jun Wei Lim (username: tjwlim)

Attempt 8

Written: Mar 18, 2017 3:12 PM - Mar 18, 2017 3:13 PM

Submission View

Your quiz has been submitted successfully.

Information

Choose the best answer.

Questions

Question 1 **1 / 1 point**

If trying all the keys of a 40-bit cipher takes 1 second on a certain computer network, how long would it take to try all the keys of a 120-bit cipher? You can assume that trying each key takes the same amount of time in each case.

○ 3 seconds

○ 2^3 seconds

○ 80 seconds

● 2^80 seconds

View Feedback

Question 2 **1 / 1 point**

Which of the following statements are true?

1. Using encryption without integrity protection is sufficient to protect against passive adversaries like Eve.
2. One-time pads can be implemented efficiently by using a pseudorandom keystream generator.

○ Neither

● Only statement 1

○ Only statement 2

○ Both statements

View Feedback

Question 3 **1 / 1 point**

About how long would an RSA key have to be in order to have the same cryptographic strength as a 128-bit AES key?

○ 33 bits

○ 128 bits

● 2600 bits

○ 2^128 bits

View Feedback

Question 4

1 / 1 point

If there are 40 people in a room, what is the probability they all have different birthdays (month and day)?

○ 40/365

○ About 1/2

● About 1/10

○ About 1/1000000

View Feedback

Question 5

1 / 1 point

Which statement is true?

● Message Authentication Codes allow for deniable authentication.

○ One makes a digital signature by decrypting a message with a private signature key.

○ The Verify function in a digital signature scheme takes two arguments and outputs a boolean.

○ To hybridize a signature, send a hash of a large message and a signature on that hash.

View Feedback

Question 6

1 / 1 point

Which kinds of cryptography are most appropriate for program security?

○ Keyless encodings, such as base-64 or ASCII armor

○ Symmetric-key encryption and MACs

○ Public-key decryption and signing

● Public-key encryption and signature verification

View Feedback

Question 7

1 / 1 point

Which of these is *not* a flaw in WEP?

○ The IV is too short.

● The IV is not encrypted.

○ The checksum interacts pessimally with the stream cipher.

○ The authentication protocol reveals enough information for an attacker to authenticate herself.

Hide Feedback

Right! The IV in WEP is in fact not encrypted, but that doesn't cause a problem with the protocol.

Question 8 **1 / 1 point**

Encoding IP packets as hostnames and looking them up in DNS is an example of:

○ IPSec

○ A VPN

○ DNS spoofing

◉ Tunelling

› View Feedback

Question 9 **1 / 1 point**

What is the most successful privacy enhancing technology in use today?

◉ SSL / TLS

○ Tor

○ Anonymizer.com

○ Remailers

› View Feedback

Question 10 **1 / 1 point**

A particular store requires you to show photo ID in order to get their loyalty card. Later, using that card along with a cash payment would have what level of nymity?

◉ Verinymity

○ Pseudonymity

○ Linkable anonymity

○ Unlinkable anonymity

› View Feedback

Question 11 **1 / 1 point**

Perfect forward secrecy protects against what attack?

○ An adversary trying every possible decryption key in order to read past messages

◉ An adversary stealing your decryption key in order to read past messages

○ An adversary trying every possible decryption key in order to read future messages

○ An adversary stealing your decryption key in order to read future messages

› View Feedback

Attempt Score: 11 / 1

Overall Grade (last attempt)**:** 11 / 1

Done