Your Name:Steven Hayden

For each multiple-choice question and each answer choice, write 3-5 sentences explaining why that answer choice either is, or is not, correct

Question 1- to 15 (each is 5 points):

Q1: Answer (A or B or C or D or E)

Explain Other Choices:

Q2: Answer (A or B or C or D or E)

In Q2, the diagram is to help you explain the operation. The diagrams are already in the online videos.

After drawing the diagram, you add the sentences that explain the mode itself

Q3: Answer (A or B or C or D or E)

Explain Other Choices:

Q4: Answer (A or B or C or D or E)

Explain Other Choices:

Q5: Answer (A or B or C or D or E)

Explain Other Choices:

Q6: Answer (A or B or C or D or E)

Explain Other Choices: E is the correct answer.

A:The preimage resistant is correct because it should be hard for an attacker to map a hash to an element.

B:given an element the attacker should be able to find a collision

C:Collions is very similar to the second preimage, the attacker picks inputs to find a collision

D:A, B, and C are correct, so D is not.

Q7: Answer (A or B or C or D or E)

Explain Other Choices:

A is the correct answer. Hacker comes from roughly cutting into things, like a secure computer.

B Identity thief is someone is looking for specifically one thing. This could include being a hacker but is too specific.

C Intruder could be a potential answer if it specifically relates to computer.

D A cyber-terrorist can be a hacker, but the specifically hold damaging information

Q8: Answer (A or B or C or D or E)

Explain Other Choices:

A:Companies can monitor their employees emails. There are laws against this, but there are loop holes in in them.

B: Companies can gain access to software and use beyond the agreed upon users. This is essential robbing the software company of sales.

C: This helps protect other work so they can get compensated. There are laws but are week against other countries stealing the property.

D is the correct answer for all the reasons above.

E is incorrect

Q9: Answer (A or B or C or D or E)

Explain Other Choices:

A: pseudorandom number generator use an algorithm, so It can generate number faster than a true random number generator.

B: A psedo random number generator should not be backward predictable even though technically it can be, because it is an algorithm.

C: A psedo random number generator can be used for a shared Initialization Vector, but not to create a psedo random number. A truly random number should be used to initialize a psedo random number generator. Or a seed to duplicate results.

D: is incorrect as there is only one right answer.

E: is incorrect as there is a right answer above

Q10: Answer (A or B or C or D or E)

Explain:

A: Hash function can hide a message, but most of the time there is a digital signature passed through the hash function.

B: The user uses their private key to decrypt a message that was encrypted using their public key. They do not know where the message came from.

C: This is the correct answer. Symmetric key is shared between Allice and Bob, and only they know. This helps protect their info, and only they can communicate with each other.

D: Not all are true

E: Not all are false

Q11: Answer (A or B or C or D or E)

Explain:

Q12: Answer (A or B or C or D or E)

Explain:

Q13: Answer (A or B or C or D or E)

Explain:

Q14: Answer (A or B or C or D or E)

Explain:

Q15: Answer (A or B or C or D or E)

Explain:

Q16 (6 points)

The birthday paradox is the phenomenon that in a group of people, the odds of two people having the same birthday are higher than you think. For example; a random group of 23 people, there is about a 50 percent chance that two people have the same birthday.

Whoever is trying to gain access just has to keep trying until they get a collision or the same hash value. They can keep storing the collisions until they can use statistic to identify values, and ultimately break the function.

|  |  |  |
| --- | --- | --- |
| **its** | **Possible outputs (H)** | **Desired probability of random collision** |
|
| **50%** |
| 16 | 216 (~6.5 x 104) | 300 |
| 32 | 232 (~4.3 × 109) | 77,000 |
| 64 | 264 (~1.8 × 1019) | 5,100,000,000 |
| 128 | 2128 (~3.4 × 1038) | 2.2E+19 |
| 256 | 2256 (~1.2 × 1077) | 4E+38 |
| 512 | 2512 (~1.3 × 10154) | 1.4E+77 |

Q17 (7 points)

In Q17, for each layer (5 layers), pick one protocol. Then summarize the main tasks and features of that protocol. Therefore, you describe 5 different protocols.

Q18 (6 points)

Q19 (6 points)